EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Vysoká škola báňská – Technická univerzita Ostrava

DISTRIBUOVANÉ SYSTÉMY ŘÍZENÍ

učební text

Jiří Koziorek a kol.

Ostrava 2011

Recenze: Ing. Jaromír Škuta, Ph.D.
RNDr. Miroslav Liška, CSc.

Název: Distribuované systémy řízení
Autor: doc. Ing. Jiří Koziorek, Ph.D., Ing. Jiří Kocián, Ing. Libor Chromčák, Ing. Tomáš Láryš
Vydání: první, 2011
Počet stran: 264
Náklad: 20

Studijní materiály pro studijní obor Měřicí a řídicí technika, Fakulta elektrotechniky a informatiky, VŠB-TU Ostrava.

Jazyková korektura: nebyla provedena.

Určeno pro projekt:
Operační program Vzděláváním pro konkurenceschopnost
Název: Personalizace výuky prostřednictvím e-learningu
Číslo: CZ.1.07/2.2.00/07.0339
Realizace: VŠB – Technická univerzita Ostrava
Projekt je spolufinancován z prostředků ESF a státního rozpočtu ČR

ISBN **978-80-248-2599-1**

POKYNY KE STUDIU

Distribuované systémy řízení

Pro předmět Distribuované řídicí systémy, 1. semestru magisterského oboru Měřicí a řídicí technika jste obdrželi studijní balík obsahující:

- integrované skriptum pro distanční studium obsahující i pokyny ke studiu
- CD-ROM s doplňkovými animacemi vybraných částí kapitol
- harmonogram průběhu semestru a rozvrh prezenční části
- rozdělení studentů do skupin k jednotlivým tutorům a kontakty na tutory
- kontakt na studijní oddělení

Prerekvizity

Pro studium tohoto předmětu je vhodné mít základní znalosti programovatelných automatů Siemens Simatic.

Cílem předmětu

je seznámení se základními způsoby návrhu a programování distribuovaných řídicích systémů. Po prostudování modulu by měl student být schopen určit, zda pro danou aplikaci je distribuovaný řídicí systém vhodný, navrhnout jeho strukturu, vhovný komunikační systém a vytvořit řídicí software.

Pro koho je předmět určen

Modul je zařazen do magisterského studia oborů Měřicí a řídicí technika studijního programu Elektrotechnika, ale může jej studovat i zájemce z kteréhokoliv jiného oboru FEI, VŠB-TU Ostrava.

Skriptum se dělí na části, kapitoly, které odpovídají logickému dělení studované látky, ale nejsou stejně obsáhlé. Předpokládaná doba ke studiu kapitoly se může výrazně lišit, proto jsou velké kapitoly děleny dále na číslované podkapitoly a těm odpovídá níže popsaná struktura.

Na tvorbě studijní opory se podíleli

doc. Ing. Jiří Koziorek, Ph.D. (texty přednášek + podklady do cvičení)

Ing. Jiří Kocián (podklady do cvičení + spolupráce na textech přednášek 7+8)

Ing. Libor Chromčák (podklady do cvičení 11 a12 + spolupráce na textech přednášky 10)

Ing. Tomáš Láryš (podklady do cvičení 13 + spolupráce na textech přednášek 12, 13, 14)

Při studiu každé kapitoly doporučujeme následující postup:

Čas ke studiu: x hodin

Na úvod kapitoly je uveden čas potřebný k prostudování látky. Čas je orientační a může vám sloužit jako hrubé vodítko pro rozvržení studia celého předmětu či kapitoly. Někomu se čas může zdát příliš dlouhý, někomu naopak. Jsou studenti, kteří se s touto problematikou ještě nikdy nesetkali a naopak takoví, kteří již v tomto oboru mají bohaté zkušenosti.

Cíl: Po prostudování tohoto odstavce budete umět

- popsat ...
- definovat ...
- vyřešit ...

Ihned potom jsou uvedeny cíle, kterých máte dosáhnout po prostudování této kapitoly – konkrétní dovednosti, znalosti.

VÝKLAD

Následuje vlastní výklad studované látky, zavedení nových pojmů, jejich vysvětlení, vše doprovázeno obrázky, tabulkami, řešenými příklady, odkazy na animace.

Shrnutí pojmů

Na závěr kapitoly jsou zopakovány hlavní pojmy, které si v ní máte osvojit. Pokud některému z nich ještě nerozumíte, vraťte se k nim ještě jednou.

Otázky

Pro ověření, že jste dobře a úplně látku kapitoly zvládli, máte k dispozici několik teoretických otázek.

Úlohy k řešení

Protože většina teoretických pojmů tohoto předmětu má bezprostřední význam a využití v praxi, jsou Vám nakonec předkládány i praktické úlohy k řešení. Praktické úlohy Vám pomohou aplikovat čerstvě nabyté znalosti při řešení reálných situací.

Použitá literatura a další zdroje

Zde najdete literaturu použitou při tvorbě dané kapitoly a další zdroje o dané problematice.

DVD-ROM

Řešený příklad naleznete na DVD.

Takto je označen odkaz na DVD, kde jsou řešené příklady nebo animace.

Úspěšné a příjemné studium s touto učebnicí Vám přejí autoři výukového materiálu

Jiří Koziorek, Jiří Kocián, Libor Chromčák, Tomáš Láryš

OBSAH

1. DISTRIBUOVANÉ ŘÍDICÍ SYSTÉMY

Čas ke studiu: 2 hodiny

Cíl Po prostudování této kapitoly budete umět:

- Definovat distribuovaný řídicí systém.
- Popsat rozdíly mezi centralizovaným a distribuovaným řídicí systémem.
- Definovat úrovně počítačově řízené výroby a kategorizovat komunikační systémy používané v řídicích systémech.
- V praktické části kapitoly si zopakujete tvorbu jednoduchých aplikací pro programovatelný automat Simatic S7 300.

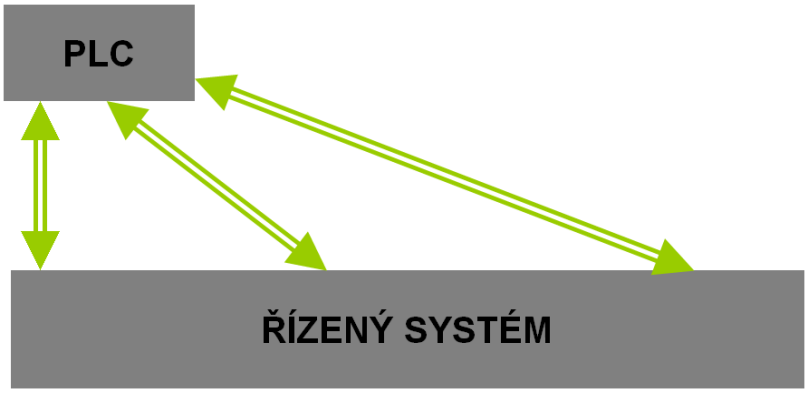
Výklad

V řídicích systémech v průmyslu i jiných technických oblastech lze v současné době pozorovat dva základní přístupy:

- Centralizované řídicí systémy.
- Distribuované řídicí systémy.

1.1. Centralizované řídicí systémy

Centralizovaný řídicí systém se vyznačuje tím, že je zde jeden výkonný řídicí prvek, který zajišťuje všechny řídicí aktivity. K tomuto prvku jsou přivedeny všechny potřebné technologické signály. Bloková struktura takového systému je znázorněna na obr. 1.1. [1]



Obr. 1.1 Struktura centralizovaného řídicího systému.

Výhody:

- Účinný, vhodný, pokud není složitý.
- Jednodušší údržba.
- Jednodušší návrh aplikačních programů.

Nevýhody:

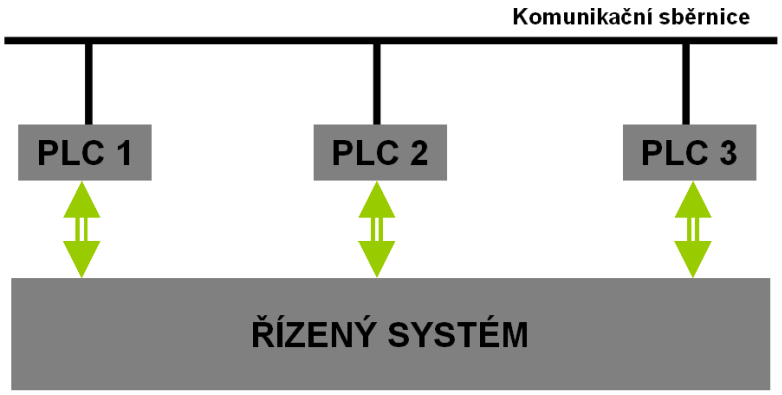
- Omezená kapacita – řídicí jednotku lze rozšiřovat jen do maximálního počtu modulů pro daný typ, je tedy většinou nutné, aby jednotka měla určitou rezervu pro případné rozšíření systému.
- Při poruše havaruje vše.
- Rozsáhlá kabeláž pro přivedení technologických signálů.

1.2. Distribuované řídicí systémy

Distribuovaný řídicí systém je složen z několika dílčích systémů, které jsou mezi sebou propojeny komunikační sběrnicí a které se společně podílejí na řízení. Tento přístup se začal v automatizaci rychle rozvíjet a nasazovat v době, kdy vznikly výkonné a spolehlivé komunikační sběrnice, které bylo možné k tomuto účelu využít a rovněž kdy cena jednotlivých zařízení s procesorem byla čím dál nižší (a nebyl tedy tak výrazný cenový rozdíl, pokud se v řídicím systému použil jeden výkonný prvek nebo několik menších prvků). Komunikace je tedy základním předpokladem pro možnost realizace distribuovaných řídicích systémů [1].

Vzhledem k tomu, že řídicí systém obsahuje několik řídicích prvků, lze se na řídicí aplikaci dívat jako na lokální či globální, podle toho, zda běží pouze na jednom zařízení nebo zda využívá několika zařízení.

Na obr. 1.2 je znázorněna struktura distribuované řídicí aplikace.



Obr. 1.2 Struktura distribuovaného řídicího systému.

Výhody:

- Vyšší výkonnostní možnosti.
- Výstavba složitých systémů.
- Úspora kabeláže pro přivedení technologických signálů.
- Jednodušší odlaďování nové aplikace (jelikož aplikace jako celek je rozdělena mezi několik PLC a může být laděna po částech).
- Postupné rozšiřování – řídicí systém je možné postupně rozšiřovat přidáváním dalších zařízení na komunikační sběrnici.

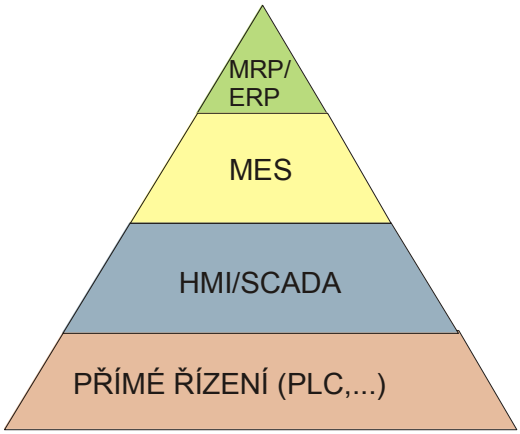
Nevýhody:

- Nepříznivý vliv prostředí – řídicí prvky jsou umísťovány přímo tam, kde je potřeba něco řídit a kde jsou potřebné signály.

- Komunikace mezi zařízeními různých výrobců.
- Vzájemná součinnost.

1.3. Počítačově řízená výroba

Řídicí systémy na bázi mikroprocesoru jsou nejrozšířenějším řídicím prostředkem v současné průmyslové automatizaci. Používají se pro velký rozsah typů úloh – od logického řízení až po komplexní komunikační úlohy. Komunikační funkce hrají podstatnou roli při vytváření distribuovaných řídicích systémů, které se v současné průmyslové praxi velice často používají. Komunikační systémy se uplatňují na všech úrovních počítačově řízené výroby. Počítačově řízená výroba se obvykle znázorňuje jako pyramida se čtyřmi vrstvami (obr. 1.3).



Obr. 1.3 Struktura počítačově řízené výroby.

MRP/ERP – Manufacturing/Enterprice Resource Planning

MES - Manufacturing Execution System

SCADA - Supervisory Control And Data Acquisition

HMI – Human Machine Interface

PLC - Programmable Logic Controller

Na nejnižší úrovni přímého řízení se používají řídicí systémy reálného času, v současné době zejména programovatelné automaty. Cílem této úrovně je přímé řízení technologického systému. Řídicí prvek má na této úrovni přímé spojení s řízeným systémem pomocí technologických vstupně/výstupních signálů.

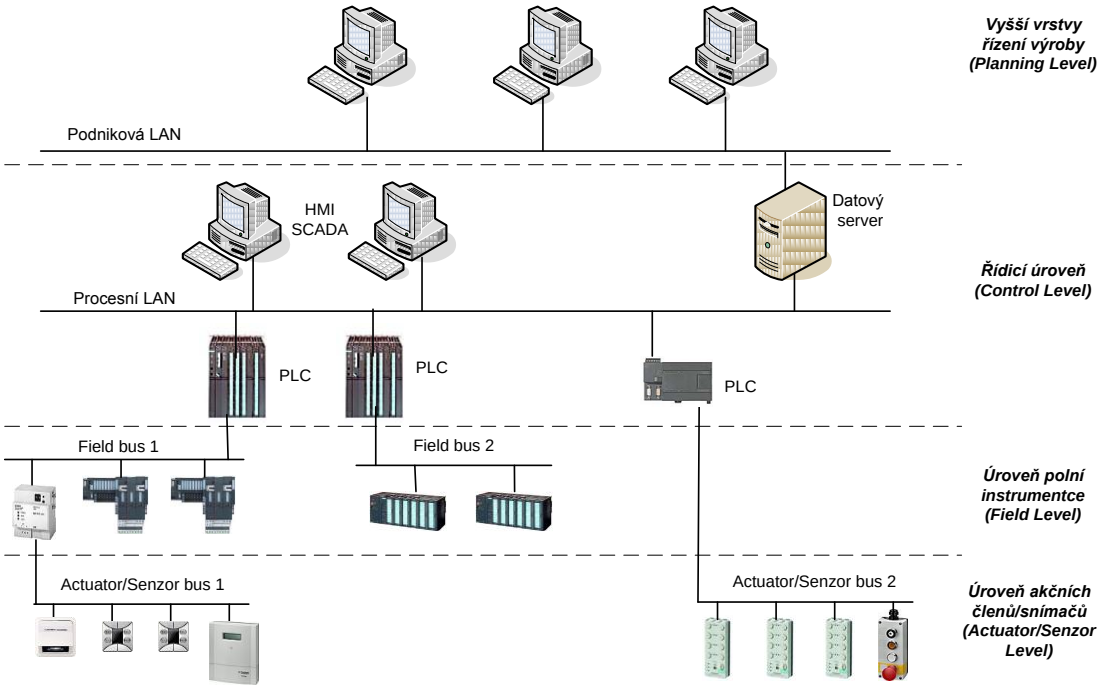
Další úroveň poskytuje uživatelské rozhraní k řídicímu systému. Pod pojmy HMI a SCADA si lze představit celou řadu zařízení, pomocí kterých lze vytvořit tato uživatelská rozhraní. Jedná se zejména o operátorské panely a počítačová vizualizační pracoviště.

Třetí úroveň slouží pro optimalizaci průběhu výroby. Cílem této úrovně je zvyšování efektivity a plynulosti výroby, synchronizaci výrobních aktivit, optimalizaci využití skladových zásob apod. Na této úrovni řízení se používají softwarové nástroje označované jako MES systémy. Zatímco předchozí úrovně se zabývaly řízením jednotlivých dílčích částí výrobního celku, řízením strojů, apod., MES systémy slouží pro jejich vzájemnou koordinaci s cílem dosažení co nejlepší produktivity výroby. MES systémy zajišťují nadřazené řízení výrobního celku.

Nejvyšší úroveň slouží pro řízení výroby podniku. MRP/ERP systémy používané na této úrovni zajišťují vzájemnou součinnost jednotlivých výrobních celků. Jedná se o manažerské informační systémy.

Úrovně přímého řízení a HMI/SCADA zajišťují vlastní řízení určité části výrobního celku nebo stroje. Na těchto dvou úrovních nacházejí uplatnění různé komunikační systémy, které lze opět rozčlenit do následujících základních úrovní (obr. 1.4):

- Úroveň akčních členů/snímačů (Actuator-Senzor Level) – tato úroveň je nejnižší komunikační vrstvou, na které vzájemně komunikují programovatelný automat a akční členy/snímače. Na této vrstvě se obvykle přenáší velice malé objemy dat, komunikační systémy mají poměrně nízké přenosové rychlosti, ale na druhou stranu je vyžadováno striktně časově deterministické chování, jednoduchost a nízká cena. Typickým představitelem komunikačního systému je zde AS Interface, X2X Link apod.
- Úroveň „polní“ instrumentace (Field Level) – na této úrovni obvykle probíhá výměna dat mezi programovatelným automatem a vzdálenými jednotkami vstupů/výstupů. Komunikační systémy používané na této úrovni musí být rovněž deterministické, objemy přenášených dat jsou zde podstatně vyšší a tudíž výkon těchto systémů musí být vyšší než u předchozí úrovně. Typickými přestaviteli komunikačních systémů na této úrovni jsou Profibus DP, Interbus, CAN apod. V současné době se začínají objevovat a používat komunikační systémy na bázi Ethernetu jako Profinet nebo Ethernet Powerlink. Tyto systémy fungují na fyzické vrstvě Ethernetu, přístup ke komunikačnímu médiu je však modifikován tak, aby bylo možné zajistit časově deterministické chování.
- Řídicí úroveň (Control Level) – na této vrstvě dochází ke komunikaci mezi několika programovatelnými automaty nebo komunikaci mezi programovatelnými automaty a HMI/SCADA systémy. Jsou obvykle přenášeny velké objemy dat, a proto jsou potřebné výkonné komunikační systémy. Na druhou stranu už není nezbytné časově deterministické chování. Typický představitelem, který je současné době prakticky výhradně používaný, je Ethernet, resp. průmyslový Ethernet.



Obr. 1.4 Komunikační systémy v průmyslové automatizaci.

Někdy se uvádí mezi polní a řídicí úrovní tzv. úroveň buněk (Cell Level). V této úrovni probíhá komunikace mezi jednotlivými dílčími částmi (buňkami) řízeného systému, tzn. jedná se o komunikaci mezi několika programovatelnými automaty po výkonné komunikační sběrnici. Používají se zde stejné typy sběrnic jako u řídicí úrovně, v dnešní době zejména Ethernet resp. Industrial Ethernet. Jelikož řídicí úroveň a úroveň buněk mají velice podobný význam a používají se zde stejné komunikační systémy, na obr. 1.4 je uvedena pouze řídicí úroveň.

Komunikace na dvou vyšších vrstvách počítačově řízené výroby (MES a MRP/ERP) je obvykle realizována prostřednictvím lokálních sítí LAN, v současnosti zejména komunikačním systémem Ethernet. V odborné literatuře se lze setkat se souhrnným označením pro tyto vrstvy a pro komunikační systémy zde používané - plánovací úroveň (Planning Level). Komunikace na této úrovni nemusí mít časově deterministické chování, neřeší se zde úlohy reálného času a jedná se spíše o kancelářské aplikace.

Programovatelné automaty bývají v současnosti vybaveny celou řadou komunikačních funkcí. Podpora základních komunikačních systémů na úrovních senzorů a akčních členů, polní a řídicí, je standardem, který je u programovatelných automatů vyžadován. Řada výrobců automatů však začíná do svých produktů implementovat podporu dalších, komplexnějších a sofistikovanějších komunikačních systémů, jsko například komunikace přes e-maily, přes protokoly FTP a HTTP apod.

Shrnutí pojmů

Centralizovaný řídicí systém se vyznačuje tím, že je zde jeden výkonný řídicí prvek, který zajišťuje všechny řídicí aktivity. K tomuto prvku jsou přivedeny všechny potřebné technologické signály.

Distribuovaný řídicí systém je složen z několika dílčích systémů, které jsou mezi sebou propojeny komunikační sběrnicí a které se společně podílejí na řízení.

Počítačově řízená výroba se obvykle znázorňuje jako pyramida se čtyřmi vrstvami – **přímé řízení**, **HMI/SCADA**, **MES** a **MRP/ERP**.

Úrovně přímého řízení a HMI/SCADA zajišťují vlastní řízení určité části výrobního celku nebo stroje. Na těchto dvou úrovních nacházejí uplatnění různé komunikační systémy, které lze rozčlenit do následujících základních úrovní - **úroveň akčních členů/snímačů** (Actuator-Senzor Level), **úroveň „polní“ instrumentace** (Field Level), **řídicí úroveň** (Control Level).

Otázky

1. Definujte pojem distribuovaný řídicí systém.
2. Definujte pojem centralizovaný řídicí systém.
3. Jaké jsou výhody a nevýhody distribuovaného řídicího systému.
4. Jaké jsou výhody a nevýhody centralizovaného řídicího systému.
5. Nakreslete strukturu počítačově řízené výroby.
6. Popište jednotlivé vrstvy počítačově řízené výroby.

7. Jak lze rozčlenit komunikační systémy používané v řídicích systémech.
8. Nakreslete příklad struktury řídicího systému a popište jednotlivé úrovně komunikací.

Použitá literatura a další zdroje

1. Kováč F. Distribuované riadiace systémy. Vydavatelstvo STU, Bratislava 1998. ISBN 80-227-1082-2.

Řešená úloha 1.1

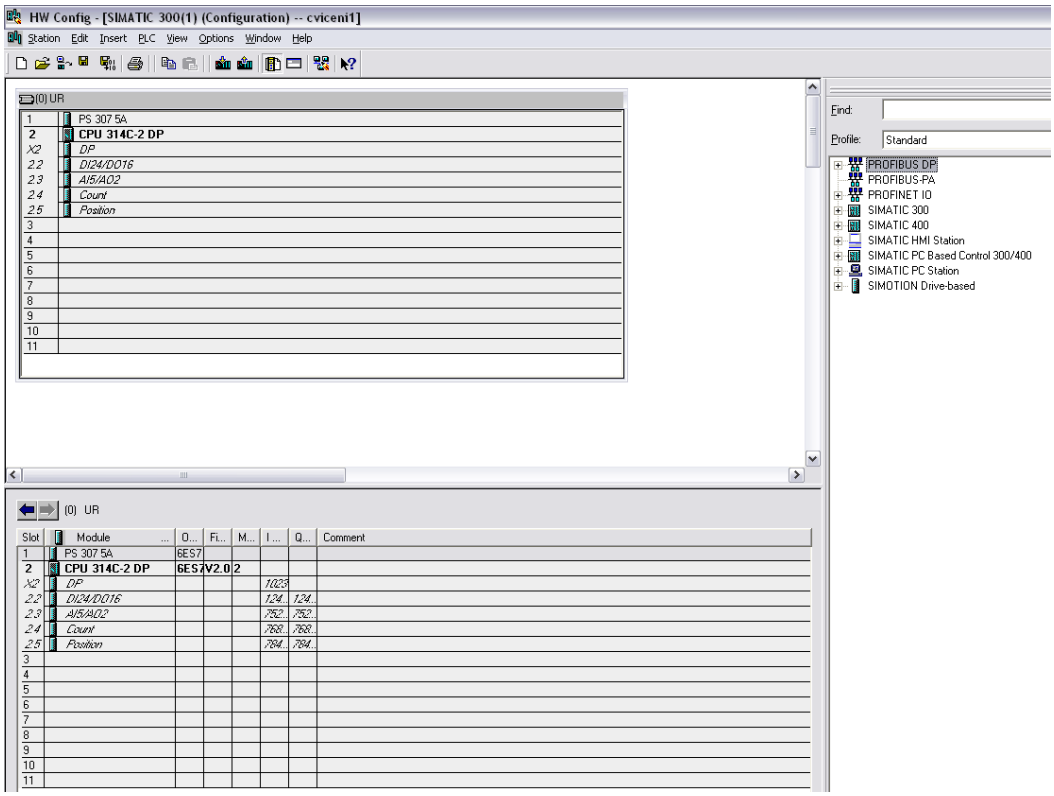
Opakování PLC S7 300.

Zadání: Vytvořte hardwarovou konfiguraci a řídicí program pro automaticky řízená garážová vrata. Použijte PLC Simatic S7 300 CPU 314-2DP s označením 6ES7 314-6CF02-0AB0. Vytvořte a nadefinujte symboly pro vstupy a výstupy systému a naprogramujte řídicí program.

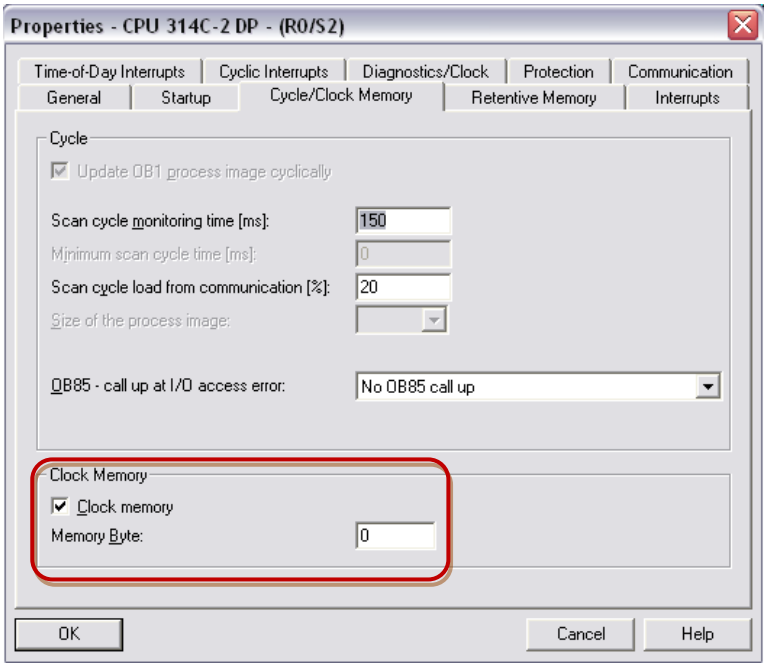
Garážová vrata je možno otevřít buď přiložením čipové karty ke snímači (KONTAKT OTEVŘENÍ POMOCÍ ČIPOVÉ KARTY), nebo dálkovým ovladačem (KONTAKT OTEVŘENÍ POMOC DÁLKOVÉHO OVLADAČE). Po zadání povelu k otevření začne blikat výstražné světlo s frekvencí 1 Hz (VÝSTRAŽNÉ SVĚTLO) a po 5s se vrata začnou otevírat. Vrata jsou otevírána motorem, který je ovládán signály směr a rychlost (SMĚR, RYCHLOST (0-100%)). Motor se uvádí do pohybu postupně, a to tak, že během prvních přibližně 3s nabíhá z nuly na maximální otáčky nejméně v 10 krocích. Po třech sekundách už běží na maximální otáčky a běží tak dlouho, než dojede na doraz (VRATA OTEVŘENA). Po otevření vrat na doraz přestává blikat výstražné světlo. Jsou-li vrata otevřena, je možné je zavřít opět pomocí stejných dvou způsobů (KONTAKT UZAVŘENÍ POMOCÍ ČIPOVÉ KARTY), (KONTAKT UZAVŘENÍ POMOC DÁLKOVÉHO OVLADAČE). Opět začne blikat výstražné světlo (VÝSTRAŽNÉ SVĚTLO) a po 5s se vrata začnou zavírat. Motor se rozbíhá stejným způsobem, jako při otevírání. Pohyb vrat při zavírání je blokován přítomnosti předmětu pod vraty (DETEKTOR-OPTICKÁ ZÁVORA). Pohyb vrat se zastaví při dosažení dorazu zavření (VRATA ZAVŘENA). Po zavření vrat přestává blikat výstražné světlo.

Hardwarová konfigurace je zobrazena na obr. 1.5. Po otevření hardwarové konfigurace je nejprve vložen rack, na první místo v racku je vložen napájecí modul a na druhé místo CPU 314C-2DP.

Pro účely programu je CPU nastaven Clock memory na bajtu MB0 (obr. 1.6).



Obr. 1.5 Hardwarová konfigurace.

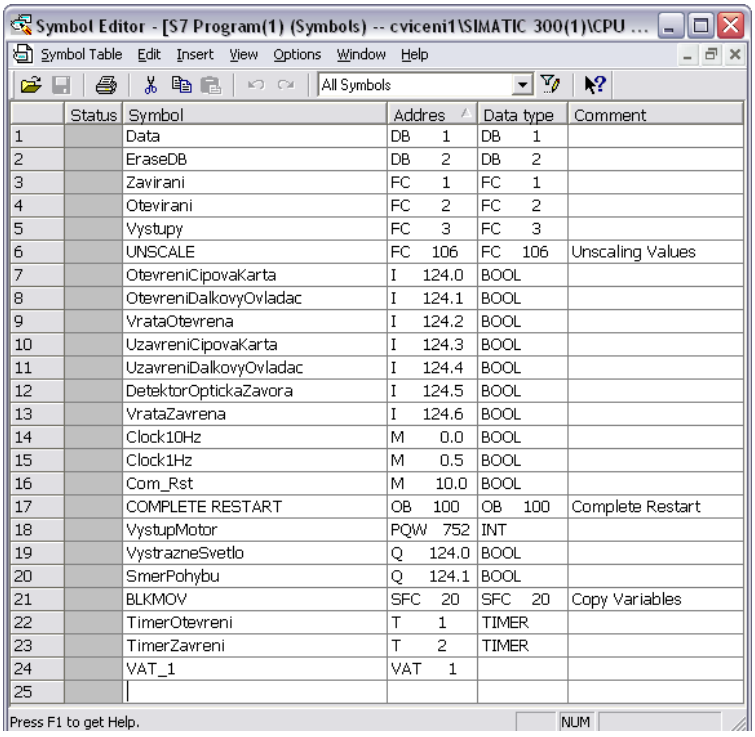


Obr. 1.6 Nastavení Clock memory.

Seznam vstupů a výstupů:

Vstupy		Výstupy	
Kontakt otevření pomocí čipové karty	I124.0	Výstražné světlo	Q124.0
Kontakt otevření pomocí dálkového ovladače	I124.1	Směr	Q124.1
Vrata otevřena	I124.2	Rychlost	PQW752
Kontakt uzavření pomocí čipové karty	I124.3		
Kontakt uzavření pomocí dálkového ovladače	I124.4		
Detektor – optická závora	I124.5		
Vrata zavřena	I124.6		

Vstupy a výstupy z tabulky, názvy funkcí a další proměnné jsou nadefinovány v „Symbol table“ (obr. 1.7).



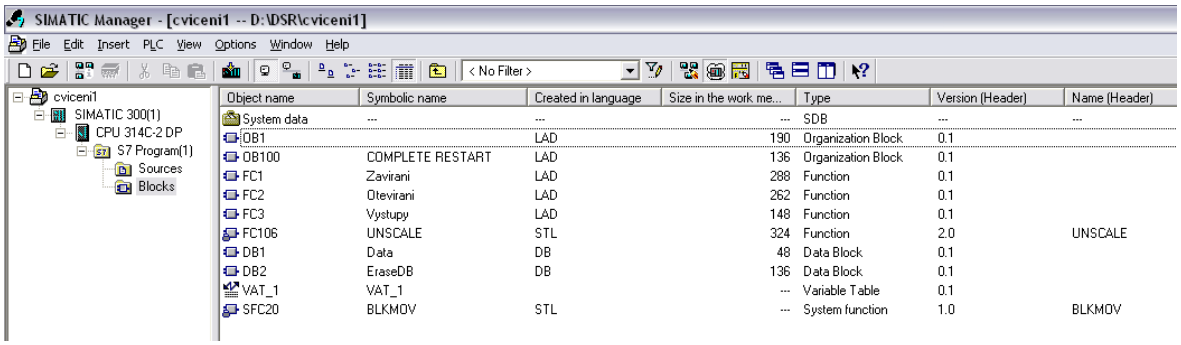
	Status	Symbol	Addres	Data type	Comment
1		Data	DB 1	DB 1	
2		EraseDB	DB 2	DB 2	
3		Zavirani	FC 1	FC 1	
4		Otevirani	FC 2	FC 2	
5		Vystupy	FC 3	FC 3	
6		UNSCALE	FC 106	FC 106	Unscaling Values
7		OtevreniCipovaKarta	I 124.0	BOOL	
8		OtevreniDalkovyOvladac	I 124.1	BOOL	
9		VrataOtevrena	I 124.2	BOOL	
10		UzavreniCipovaKarta	I 124.3	BOOL	
11		UzavreniDalkovyOvladac	I 124.4	BOOL	
12		DetektorOptickaZavora	I 124.5	BOOL	
13		VrataZavrena	I 124.6	BOOL	
14		Clock10Hz	M 0.0	BOOL	
15		Clock1Hz	M 0.5	BOOL	
16		Com_Rst	M 10.0	BOOL	
17		COMPLETE RESTART	OB 100	OB 100	Complete Restart
18		VystupMotor	PQW 752	INT	
19		VystrazneSvetlo	Q 124.0	BOOL	
20		SmerPohybu	Q 124.1	BOOL	
21		BLKMOV	SFC 20	SFC 20	Copy Variables
22		TimerOtevreni	T 1	TIMER	
23		TimerZavreni	T 2	TIMER	
24		VAT_1	VAT 1		
25					

Obr. 1.7 Tabulka symbolů.

Řešení programu v LAD

Program je řešen v OB1. V tomto organizačním bloku jsou volány funkce FC1, FC2 a FC3, které slouží k názornému rozčlenění programu. Funkce FC1 řeší otevírání vrat, funkce FC2 zavírání vrat. Ve funkci FC3 jsou řešeny všechny výstupy programu. Pro prvotní nastavení proměnných po

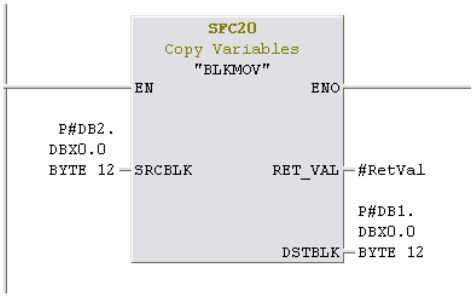
restartu slouží OB100. Detailnější popis částí programu je uveden k jednotlivým Networkům organizačních bloků a funkcí.



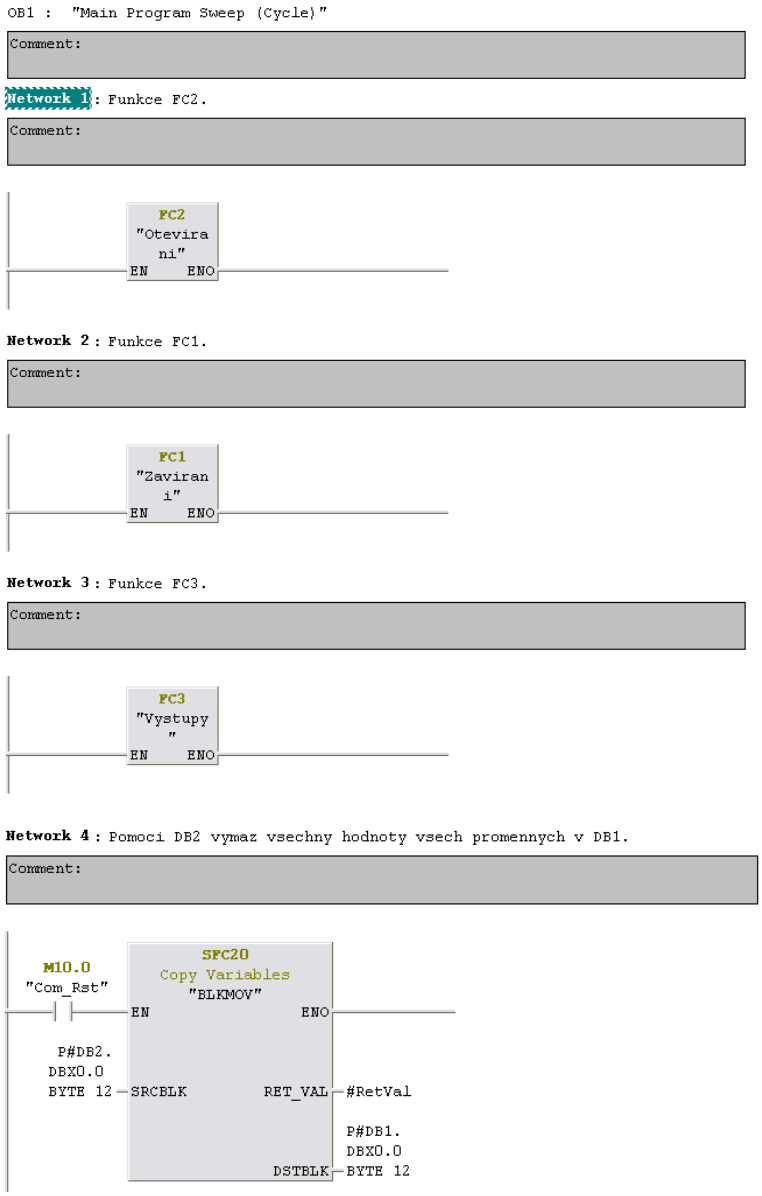
Obr. 1.8 Seznam použitých komponent programu

OB100:

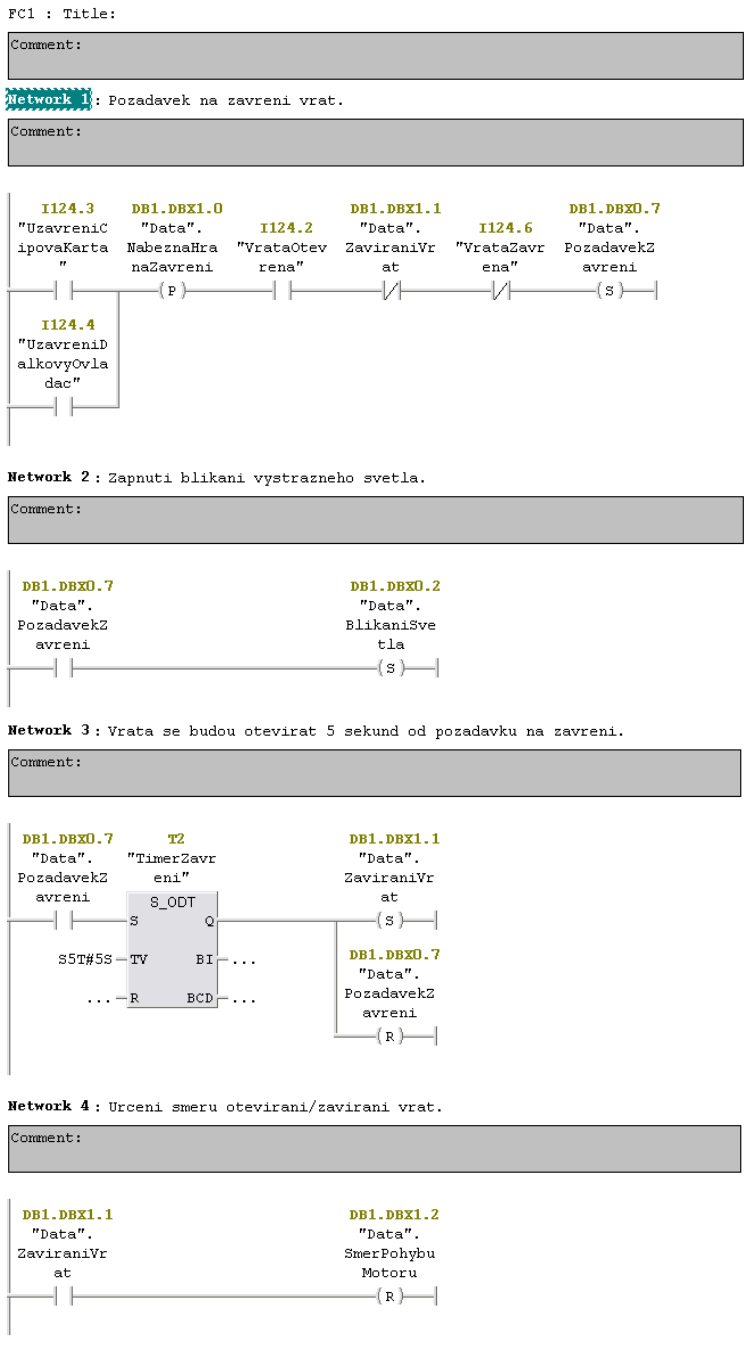
```
OB100 :  "Complete Restart"
Comment:

Network 1: Pomoci DB2 vymaz vsechny hodnoty vsech promennych v DB1.
Comment:
```



OB1:

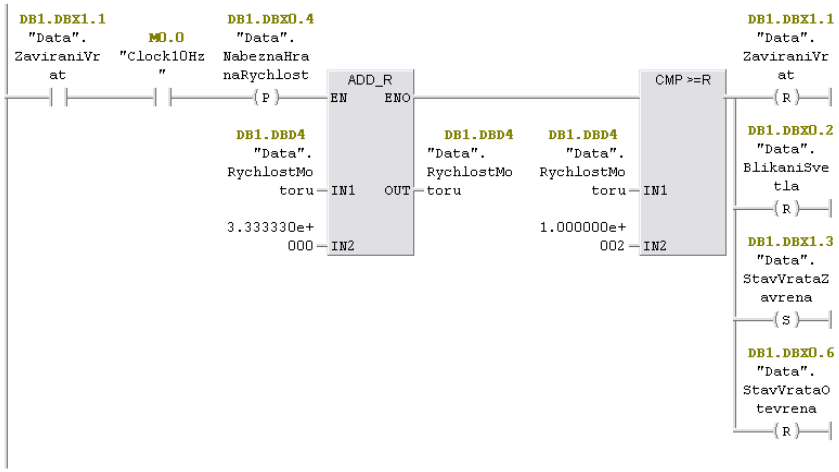

OB1 : "Main Program Sweep (Cycle)"
Comment:
Network 1: Funkce FC2.
Comment:
FC2
"Otevira ni"
EN
ENO
Network 2: Funkce FC1.
Comment:
FC1
"Zaviran i"
EN
ENO
Network 3: Funkce FC3.
Comment:
FC3
"Vystupy "
EN
ENO
Network 4: Pomoci DB2 vymaz vsechny hodnoty vsech promennych v DB1.
Comment:
M10.0
"Com_Rst"
SFC20
Copy Variables
"BLKMOV"
EN
ENO
P#DB2.
DBX0.0
BYTE 12
SRCBLK
RET_VAL
#RetVal
P#DB1.
DBX0.0
DSTBLK
BYTE 12

FC1:


FC1 : Title:
Comment:
Network 1: Pozadavek na zavreni vrat.
Comment:
I124.3
"UzavreniCipovaKarta"
DB1.DBX1.0
"Data".NabeznaHranaZavreni
I124.2
"VrataOtevrena"
DB1.DBX1.1
"Data".ZaviraniVrat
I124.6
"VrataZavrena"
DB1.DBX0.7
"Data".PozadavekZavreni
I124.4
"UzavreniDalkovyOvladac"
Network 2: Zapnuti blikani vystrazneho svetla.
Comment:
DB1.DBX0.7
"Data".PozadavekZavreni
DB1.DBX0.2
"Data".BlikaniSvetla
Network 3: Vrata se budou otevirat 5 sekund od pozadavku na zavreni.
Comment:
DB1.DBX0.7
"Data".PozadavekZavreni
T2
"TimerZavreni"
S_ODT
S
Q
S5T#5S
TV
BI
R
BCD
DB1.DBX1.1
"Data".ZaviraniVrat
DB1.DBX0.7
"Data".PozadavekZavreni
Network 4: Urceni smeru otevirani/zavirani vrat.
Comment:
DB1.DBX1.1
"Data".ZaviraniVrat
DB1.DBX1.2
"Data".SmerPohybuMotoru

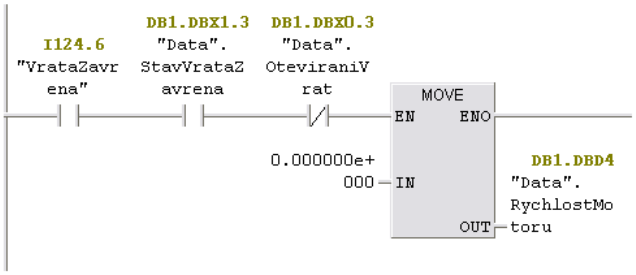
Network 5 : Rychlost zavirani vrat.

Comment:



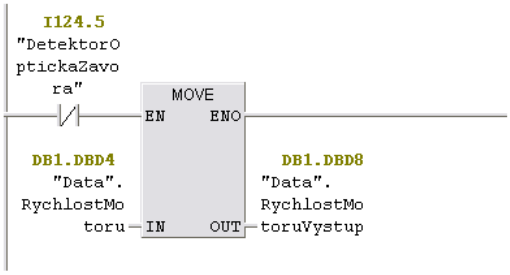
Network 6 : Doraz - vrata zavrena.

Comment:



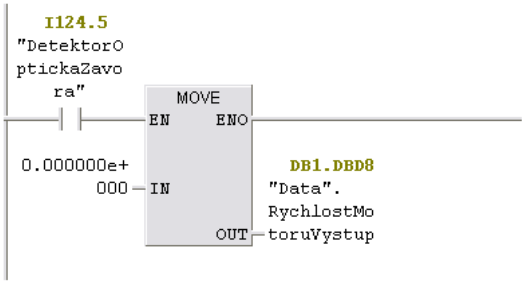
Network 7 : Rychlost motoru.

Comment:



Network 8 : Opticka zavora - zastaveni zavirani.

Comment:



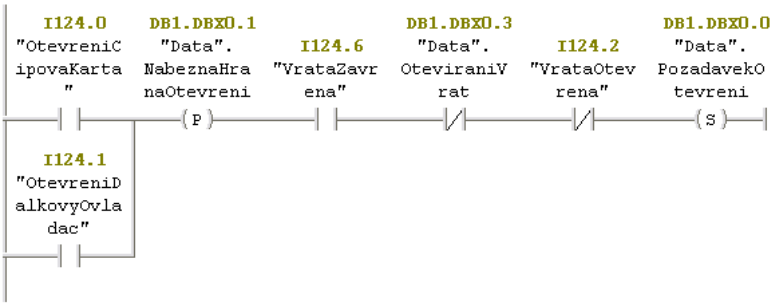
FC2:

FC2 : Title:

Comment:

Network 1: Pozadavek na otevirani.

Comment:

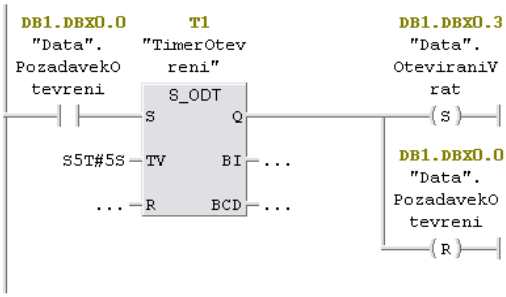


Network 2 : Zapnuti blikani vystrazneho svetla.

Comment:

Network 3 : Vrata se budou otevirat 5 sekund od pozadavku na otevreni.

Comment:

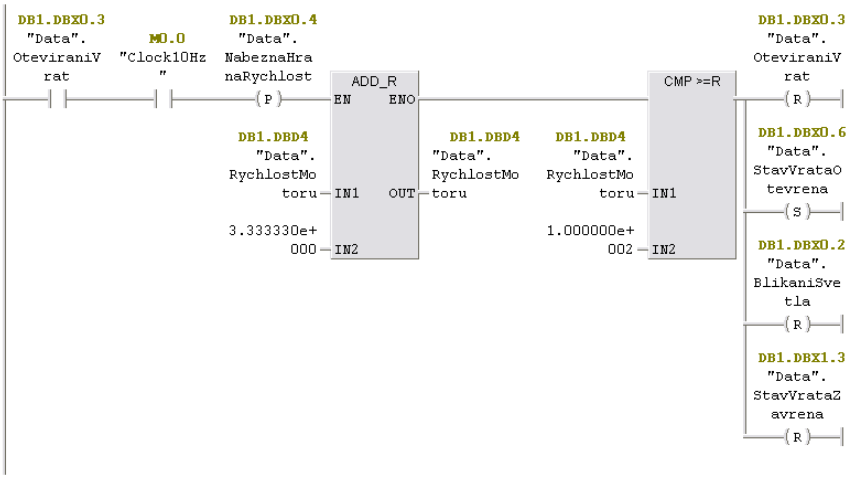


Network 4 : Urceni smeru otevirani/zavirani vrat.

Comment:

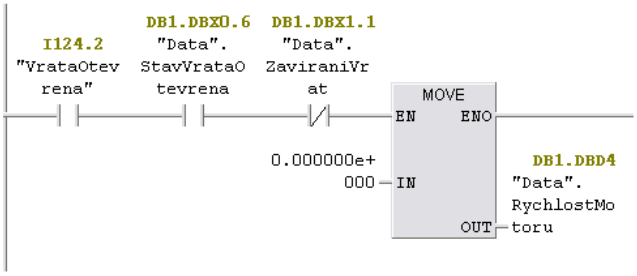
Network 5 : Rychlost otevirani vrat.

Comment:



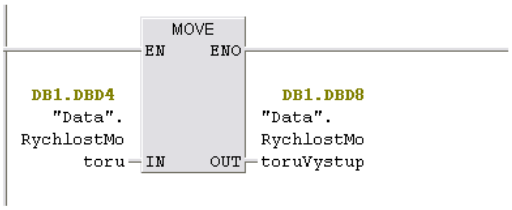
Network 6 : Doraz - vrata otevrena.

Comment:

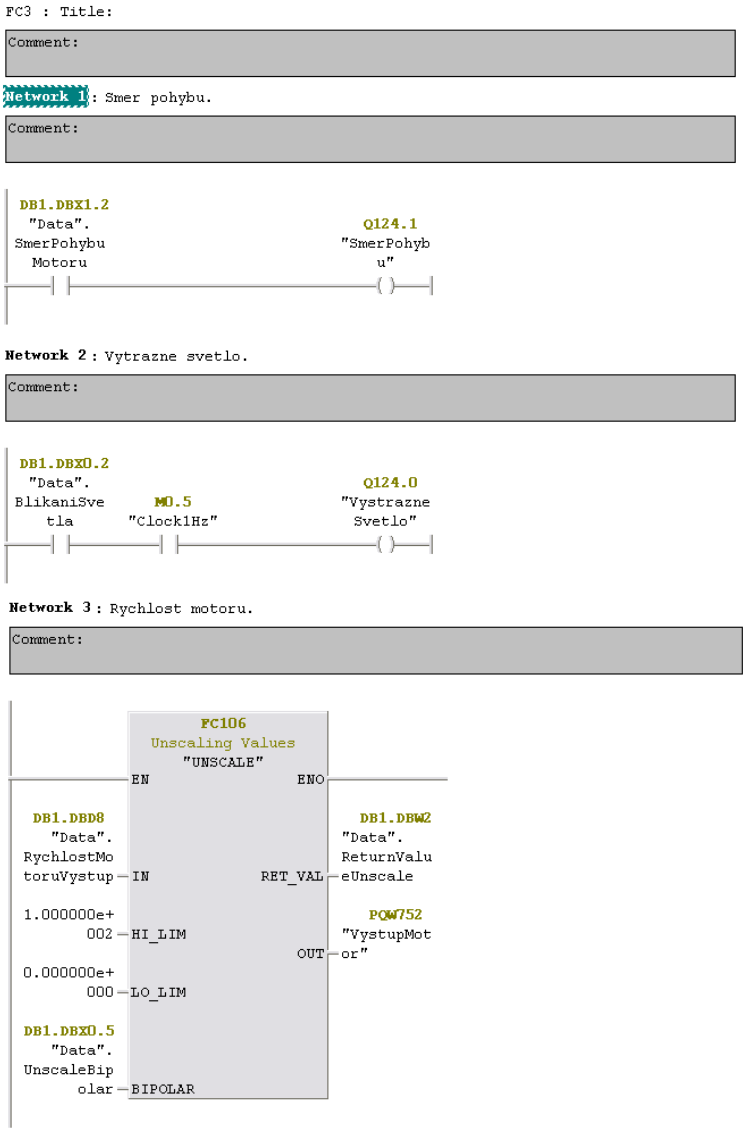


Network 7 : Rychlost motoru.

Comment:



FC3:



DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI1\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI1\

Řešená úloha 1.2

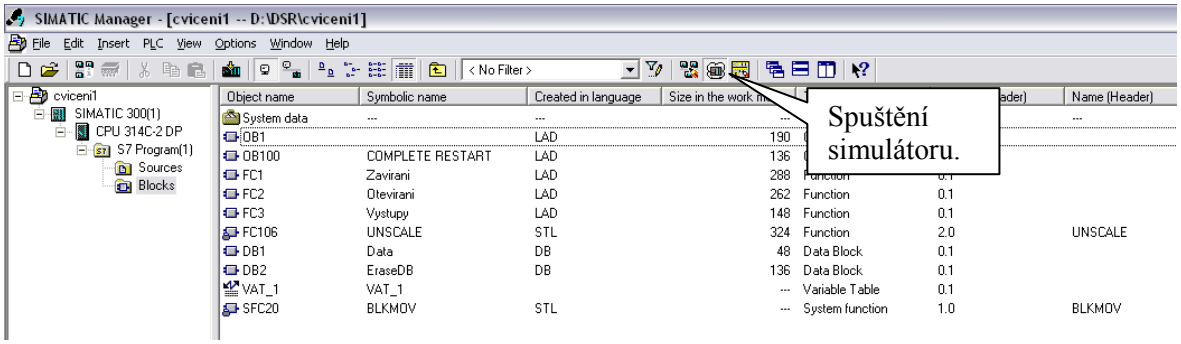
Zadání: Funkci řídicího programu z řešené úlohy 1.1 otestujte v simulátoru.

Řídicí program z řešené úlohy 1.1 je možno otestovat na reálném PLC. Pokud není PLC k dispozici, lze s výhodou využít simulátoru PLC. Simulátor se spouští stiskem Simulator On/Off podle obr. 1.9. Spuštěný simulátor je zobrazen na obr. 1.10.

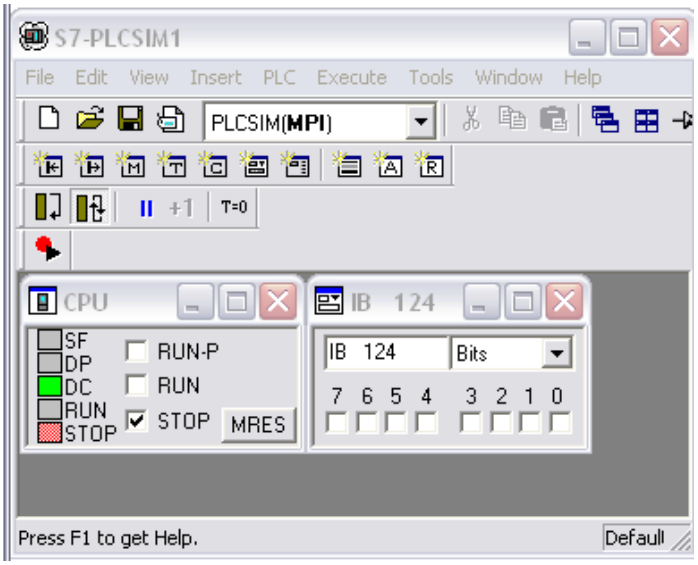
Při spuštěném simulátoru je možno hardwarovou konfiguraci spolu s programem nahrát do simulátoru. Dále PLC v simulátoru přepneme ze „Stop“ do „Run“ či „Run-P“, podle toho, zda chceme za běhu programu do PLC nahrávat bloky či ne (Run-P: Programmable). V okně simulátoru si nadefinujeme potřebné vstupy, výstupy, časovače, čítače nebo paměťové oblasti, které chceme nastavovat a prohlížet.

Pro on-line kontrolu běhu programu je také vhodná „Variable table“ (obr. 1.11), která umožňuje monitoring a nastavování vstupů, výstupů a paměťových oblastí aj.

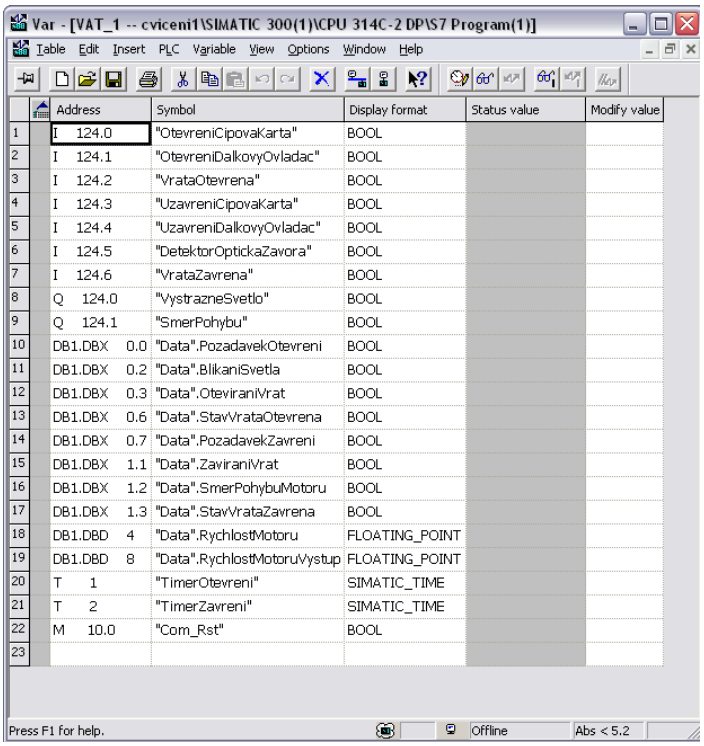
V našem případě jsou v simulátoru nastaveny vstupy IB124 pro zapínání vstupních signálů. Výstupy a další paměťové oblasti jsou pak monitorovány ve „Variable table“.



Obr. 1.9 Zapnutí simulátoru PLC.



Obr. 1.10 Simulátor PLC.



Obr. 1.11 VAT tabulka.

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI1\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI1\

2. ISO-OSI MODEL

Čas ke studiu: 3 hodiny

Cíl Po prostudování této kapitoly budete umět

- Popsat zásady pro propojování otevřených systémů.
- Popsat komunikační model ISO OSI, jeho jednotlivé vrstvy a funkce těchto vrstev.
- Definovat typy služeb, které se v ISO OSI modelu využívají.
- V praktické části se naučíte vytvořit jednoduchou řídicí aplikaci pro programovatelný automat Simatic S7 200 s využitím komunikační sběrnice AS Interface.

Výklad

V současné době již existuje velké množství komunikačních sítí používaných v průmyslové komunikaci, podobně jako v jiných technických podoborech. Již samotná norma IEC 61158 jich definuje 16 základních skupin a některé z nich již dnes existují ve více verzích. A to zdaleka nejsou všechny komunikační sběrnice v dnešní době používané. Existuje celá řada velice rozšířených průmyslových komunikačních sběrnic, které v této normě zahrnuty nejsou. Jedná se např. o velice známou sběrnici AS-i aplikovanou na úroveň akčních členů a snímačů, dále pak sběrnici CAN, jejíž aplikační oblast byla z počátku spatřována spíše v automobilovém průmyslu a mnohé další. Naopak některé ze sběrnic, uvedených v citované normě, se příliš neuchytilo a dnes jsou spíše na ústupu.

Aby se předešlo problémům souvisejícím s používáním velkého množství vzájemně nekompatibilních standardů, mezinárodní organizace ISO (International Organization for Standartization) definovala už v roce 1984 model pro komunikaci otevřených systémů – OSI (Open System Interconection). OSI není komunikačním standardem, ale poskytuje návod jak identifikovat a oddělit koncepčně odlišné části komunikačního procesu. Referenční model ISO OSI (někdy označovaný též RM ISO) tedy nespecifikuje konkrétní komunikační systém, konkrétní komunikační parametry, ale popisuje, jakým způsobem probíhá přenos zprávy mezi komunikačními partnery. Model OSI byl poprvé publikovaný v roce 1984 v souboru dokumentů nazvaných ISO 7498. [1, 2]

2.1. Zásady propojování otevřených systémů

V ISO OSI modelu je definováno 7 funkčních vrstev. Každá vrstva zajišťuje přesně vymezené funkce. Příslušná vrstva komunikuje přímo jen se sousední vrstvou, která leží nad ní nebo pod ní. Služby požaduje od nejbližší nižší vrstvy nebo je poskytuje nejbližší vyšší vrstvě. Důležité je, že komunikační partneři přenosu mezi sebou tvoří na každé úrovni modelu virtuální spoje, zatímco k reálnému přenosu dat dochází pouze ve vrstvě 1 (fyzické), která jako jediná fyzicky propojuje komunikační partnery.

Volání služeb jednotlivých vrstev probíhá tak, že žádající vrstva posílá údaje a parametry do nejbližší nižší vrstvy a očekává odpověď, přičemž se nezabývá podrobnostmi, jak se požadavek vyřizuje. Moduly umístěné ve stejné vrstvě, ale v jiném uzlu sítě, se označují jako peer

(rovnocenné) a navzájem komunikují pomocí protokolu, který definuje formáty zpráv a pravidla pro výměnu dat.

Virtuální spoj znamená, že účastníci komunikující spolu na úrovni vrstvy 7, tj. např. elektronickou poštou, nemají zdání o funkcích vrstev 1 až 6. Každá vrstva má definovány dvě základní skupiny funkcí. První jsou služby dané vrstvy a druhou funkcí je protokol vrstvy jako soubor pravidel, kterými se komunikace mezi účastníky přenosu řídí (tj. určujících, jak lze zahájit přenos, jak ho provést a jak ho ukončit). [1, 2]

2.2. Vrstvy modelu OSI

1. Fyzická vrstva (physical layer)

Je to základní síťová vrstva, která má jako jediná reálné spojení mezi dvěma komunikujícími místy. Jejím úkolem je zajistit přenos jednotlivých bitů mezi příjemcem a odesílatelem prostřednictvím fyzické přenosové cesty. Fyzická vrstva neinterpretuje přenášené bity. Přenosová cesta je realizována elektrickým, optickým, radiofrekvenčním nebo jiným rozhraní. Na této úrovni se realizují všechny detaily týkající se přenosového média, úrovní signálů, frekvencí, kabelů, konektorů apod.

2. Linková vrstva (data link layer)

Tato vrstva má za úkol zajistit přenos celých bloků údajů, označovaných jako rámce, frames mezi dvěma uzly. Linková vrstva má správně rozpoznat začátek a konec rámce a jeho jednotlivé části.

Linková vrstva zajišťuje řízení přístupu ke komunikačnímu médiu, fyzické adresování, realizuje řízení toku a zabezpečení proti chybám. Linková vrstva poskytuje pro vyšší úroveň bezchybnou datovou linku mezi dvěma uzly.

Linková vrstva se označuje také jako spojová vrstva.

3. Síťová vrstva (network layer)

Síťová vrstva u komunikačních systémů, které se vyznačují komplexní topologií sítě. Sítová vrstva sestavuje komunikační cestu pro všechny zprávy a to i v případě, že tato cesta je sestavena z odlišných větví procházející několika uzly. Dohlíží na to, aby pakety došly od zdroje k cíli. Musí zajistit potřebné směrování, routing (volbu vhodné trasy) přenášených rámců a zajistit postupné odevzdávání jednotlivých paketů po této trase od odesílatele k příjemci. Síťová vrstva si tedy musí uvědomovat konkrétní topologii sítě – tzn. způsob vzájemného propojení uzlů mezi sebou.

4. Transportní vrstva (transport layer)

Transportní vrstva řeší koncové řízení komunikace (tj. mezi původním odesílatelem a konečným příjemcem). Je rozhraním mezi aplikačním softwarem a externí sítí. Poskytuje transparentní, spolehlivý přenos dat s požadovanou kvalitou.

Zatímco vrstvy 1-3 jsou „hardwarově orientované“, kdy se starají o vlastní přenos dat, vrstvy 5-7 jsou spíše „softwarově orientované“, kde zajišťují práci s přenášenými daty. Transportní vrstva je tedy určitým rozhraním mezi těmito skupinami vrstev.

Tato vrstva má prostřednictvím nižších vytvořenou iluzi, že každý uzel sítě má přímé spojení s kterýmkoliv uzlem sítě. Díky tomu se už věnuje jenom komunikaci koncových účastníků.

Při odesílání dat vytváří jednotlivé pakety, do kterých rozděluje přenášené údaje a při přijímání je zase skládá do původního tvaru. Dokáže zajistit přenos libovolně velkých zpráv, i když jednotlivé pakety mají jen omezenou velikost.

5. Relační vrstva (session layer)

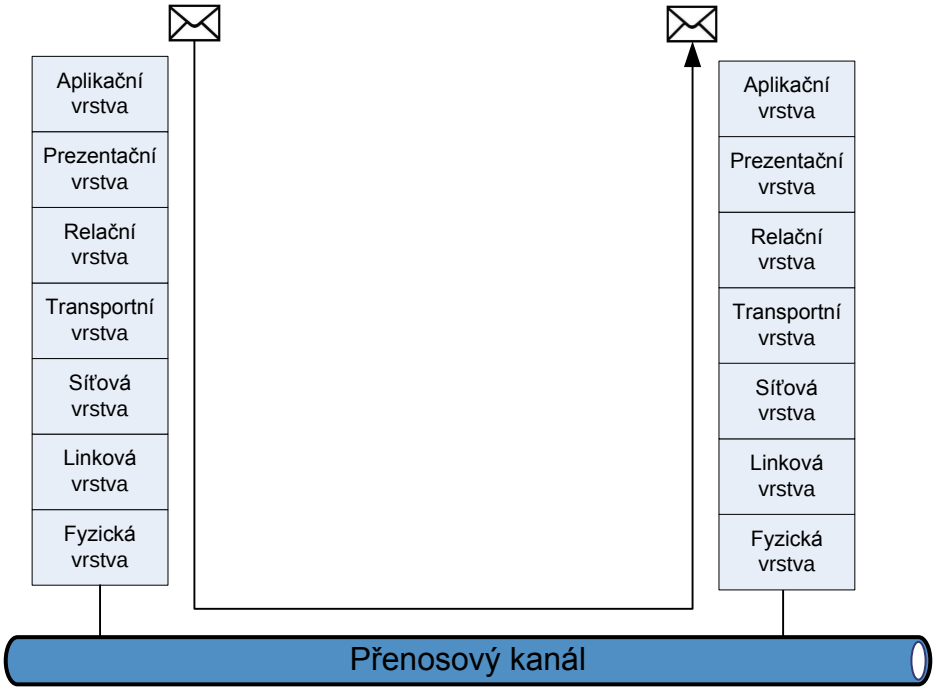
Úlohou relační vrstvy je organizovat a synchronizovat dialog mezi koncovými účastníky a řídit výměnu dat mezi nimi - její úlohou je navazovat, udržovat a rušit relace. Při navazování relace si tato vrstva vyžádá od transportní vrstvy vytvoření spojení, prostřednictvím kterého pak probíhá komunikace mezi oběma účastníky relace. Při ukončení relace má na starosti všechno, co je třeba k ukončení relace a zrušení existujícího spojení.

6. Prezentační vrstva (presentation layer)

Úlohou prezentační vrstvy je převést data do formátu, který používají komunikující partneři. Formát dat se v komunikujících systémech může lišit, a také je někdy nutné upravit formát dat pro účely přenosu. Příkladem činností prezentační vrstvy jsou převody kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů, komprese dat, šifrování apod. Vrstva se zabývá jen strukturou dat, ale ne jejich významem, který je znám jen vrstvě aplikační.

7. Aplikační vrstva (application layer)

Aplikační vrstva představuje rozhraní mezi komunikačním kanálem a koncovou aplikací, která vyžaduje komunikaci. Mohou to být aplikace pro přenos souborů, elektronickou poštu, vzdálené připojování apod. Aplikační vrstva obsahuje části aplikací, které řeší všeobecně použitelné mechanizmy. Například v případě elektronické pošty obsahuje aplikační vrstva část, které zajišťuje předávání zpráv. Uživatelské rozhraní pro práci s elektronickou poštou je pak součástí konkrétní aplikace.

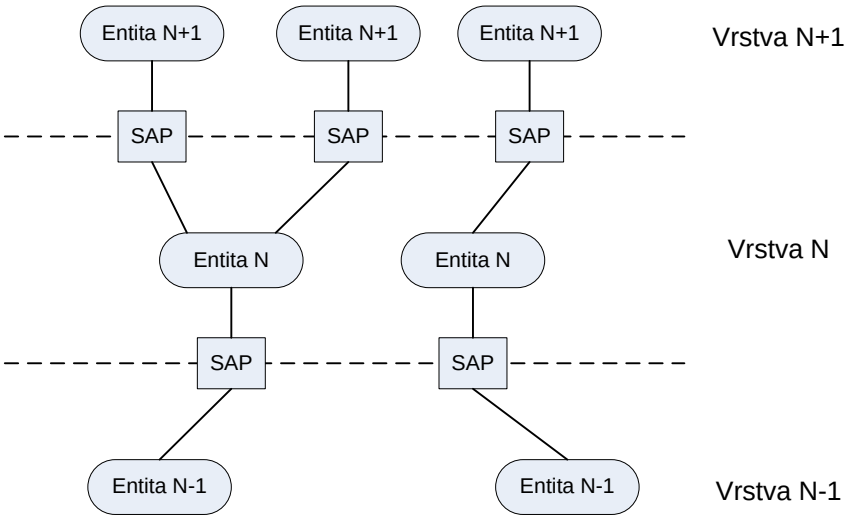


Obr. 2.1 Přenos dat ve vrstvovém modelu ISO OSI.

V předchozím textu byly uvedeny pojmy paket a rámec. Paket (packet) je blok dat vytvářený na úrovni transportní vrstvy. Jedná se o část přenášeného datového souboru, kterou lze přenést najednou. Rámec (frame) je blok data posílány po přenosovém médiu na úrovní linkové vrstvy.

S těmito pojmy souvisí rovněž pojem datagram, což je obecně paket, který není posílán zabezpečeným spojením (tzn. bez předchozího navázání spojení nebo potvrzení o příjmu). Datagramy IP tvoří základní datové bloky internetu. Jeden datagram může být rozdělen a odeslán po částech. Tomuto mechanismu se říká fragmentace a používá se pro úpravu počtu bitů/bajtů (délky) odeslaných dat tak, aby odpovídala maximální délce pro daný typ spojení. Zpráva (message) je pak blok dat na úrovni aplikační vrstvy.

Jakýkoliv prvek, který vykonává činnost v rámci modelu ISO OSI, se označuje jako entita. Může se jednat o objekt softwarové (např. proces) nebo hardwarové povahy (např. řadič). Entita je dána vrstvou, na které se vyskytuje, tzn. mluví se o prezentační entitě, transportní entitě apod. Entity komunikujících zařízení vyskytující se na stejných vrstvách se označují jako rovnocenné entity (peer entity). Entita ve vrstvě N implementuje služby (poskytovatel služby), které jsou poskytovány entitám na úrovni N-1 (uživatel služby). Entity ve vrstvě N-1 jsou zároveň poskytovateli služeb pro entity ve vrstvě N-2 apod. Pro možnost nabízení a využívání služeb entitami je v ISO OSI modelu definován mechanizmus bodů poskytování služby (Service Access Points, SAP), což jsou jednoznačně definovaná místa v rámci rozhraní mezi vrstvami. Tento mechanizmus je znázorněn na obr. 2.2. [1]



Obr. 2.2 Přenos dat mezi vrstvami ISO-OSI modelu.

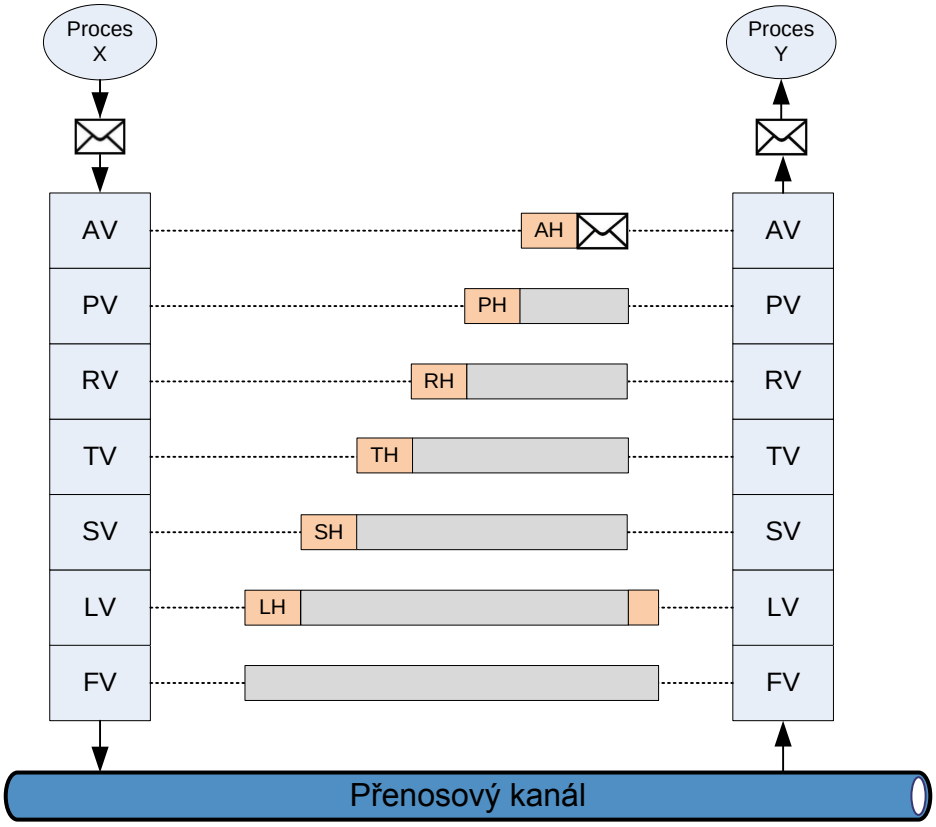
Entita, která chce využívat službu jiné entity, musí znát:

- Příslušný přístupový bod SAP.
- Způsob volání příslušné služby složený z následujících částí:
    - Řídicí informace (Interface Control Information, ICI).
    - Užitečná data (Service Data Unit, SDU).

Informace předávaná přes přístupový bod SAP se označuje jako datová jednotka rozhraní (Interface Data Unit, IDU).

Rovnocenné entity komunikujících zařízení (umístěné na stejných vrstvách) si vzájemně předávají data pomocí komunikačního protokolu. Komunikační protokol je množina pravidel, které určují syntaxi a význam jednotlivých zpráv při komunikaci. Přenos zprávy mezi dvěma zařízeními pomocí komunikačního systému popsaného ISO OSI modelem je znázorněn na obrázku 2.3. Data, která zařízení X vyšle do aplikační vrstvy komunikačního systému, jsou v jednotlivých vrstvách doplněny řídicími informacemi obvykle ve formě hlavičky dané použitým komunikačním protokolem. Data,

která jsou pak na úrovni fyzické vrstvy reálně přenesena, tedy obsahují kromě požadovaných údajů ještě další, řídicí údaje, které slouží pro řízení komunikace. Na straně přijímajícího partnera jsou řídicí údaje zase odebírány, až jsou aplikační vrstvou zařízení Y předána původně odeslaná data.



Obr. 2.3 Přenos zprávy mezi dvěma zařízeními.

2.3. Služby

Na jednotlivých vrstvách ISO OSI modelu jsou entitami poskytovány služby, které mohou mít různý charakter. Služby lze rozdělit na spojované a nespojované:

- Spojované služby (Connection-oriented Services) – tyto služby vyžadují nejprve navázání spojení a poté může probíhat přenos dat. Princip je podobný jako telefonního hovoru – navázání spojení vytočením čísla a zvednutím sluchátka na straně komunikačního partnera, poté může probíhat hovor. Tento princip se používá zejména telekomunikačních systémů, veřejných datových sítí apod. Je výhodnější pro přenos větších objemů dat. Má větší jednorázovou režii pro navazování spojení, menší režii při vlastním přenosu.
- Nespojované služby (Connectionless Services) - zde neprobíhá navázání spojení před přenosem dat. Princip lze přirovnat ke klasické poště. Zpráva je opatřena adresou, přenos může probíhat různými cestami. Tento způsob se používá zejména u lokálních sítí apod. Je výhodnější pro přenos kratších zpráv. Má relativně vyšší režii v průběhu přenosu.

Další způsob rozlišení služeb je na služby spolehlivé a nespolehlivé:

- Spolehlivé (Reliable Services) – při přenosu neztrácí data. Přenos je zajištěn mechanizmem potvrzování. Při přijetí poškozených dat jsou data zaslána znovu.

- Nespolehlivé (Unreliable Services) – neposkytují záruku úspěšnosti přenosu. Nepoužívají mechanismus potvrzování, tzn. nejsou zatíženy režií nutnou pro potvrzování a proto mohou být rychlejší než spolehlivé služby.

Shrnutí pojmů

ISO OSI model je model pro komunikaci otevřených systémů. Definuje **7 funkčních vrstev** a každá vrstva zajišťuje přesně vymezené funkce:

- Fyzická vrstva (physical layer)
- Linková vrstva (data link layer)
- Síťová vrstva (network layer)
- Transportní vrstva (transport layer)
- Relační vrstva (session layer)
- Prezentační vrstva (presentation layer)
- Aplikační vrstva (application layer)

Na jednotlivých vrstvách ISO OSI modelu jsou entitami poskytovány služby, které mohou mít různý charakter. Služby lze rozdělit na **spojované** a **nespojované**, **spolehlivé** a **nespolehlivé**.

Otázky

1. Co je to ISO OSI model a k čemu slouží?
2. Popište jednotlivé vrstvy ISO OSI model.
3. Nakreslete představu přenosu dat ve vrstvovém modelu ISO OSI.
4. Co se v modelu ISO OSI označuje jako entita?
5. Jaký je mechanizmus nabízení a využívání služeb mezi entitami?
6. Jaké entity se označují jako rovnocenné?
7. Co jsou to spojované služby?
8. Co jsou to nespojované služby?
9. Co jsou to spolehlivé služby?
10. Co jsou to nespolehlivé služby?

Další zdroje

1. Kováč F. Distribuované riadiace systémy. Vydavatelstvo STU, Bratislava 1998. ISBN 80-227-1082-2.
2. Zezulka F.; Hynčica O. Průmyslový Ethernet II: Referenční model ISO/OSI. Automa 3/2007. ISSN 1210-9592.

Řešená úloha 2.1

Zadání: Seznamte se s komunikačním procesorem CP 243-2 pro PLC S7 200, který je určený pro komunikaci po sběrnici AS-i.

AS-i je monomaster-multi slave sběrnice (1 master a až 31 slavů), dohromady je tedy na sběrnici připojeno maximálně 32 zařízení.

Na každém slavu mohou být maximálně 4 digitální vstupy a 4 digitální výstupy (4DI/4DO), takže dohromady je na sběrnici maximálně 142 digitálních vstupů a 142 digitálních výstupů. Napájecí zdroj je napojen přímo na dvouvodičové sběrnici, jednotlivé bity přenosu jsou namodulovány na toto napájecí napětí.

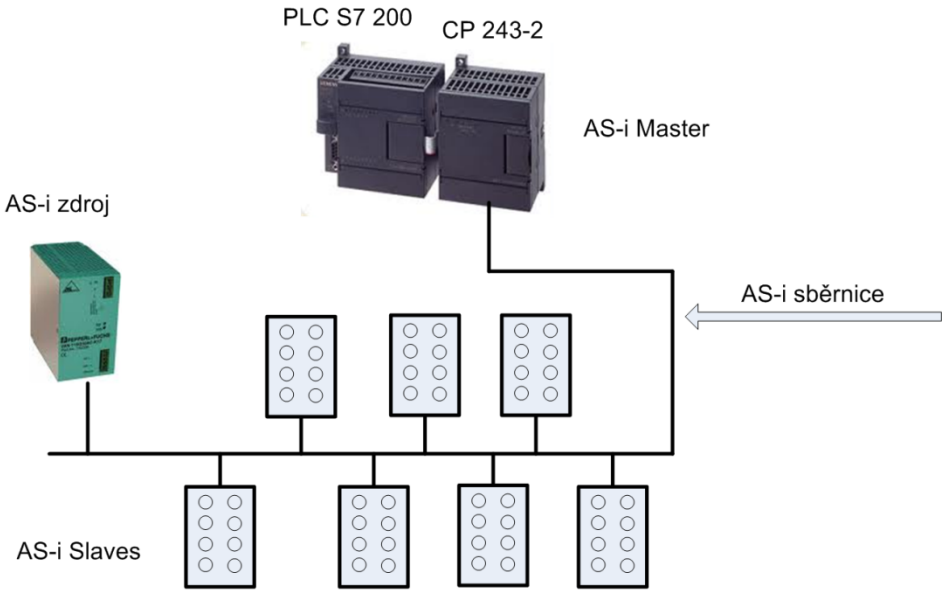
Cyklus AS-i sběrnice je menší než 5ms, což je méně než cyklus programu v PLC. Nedochází tedy k případným nežádoucím reakčním prodlevám programu v závislosti na prodlevách v komunikaci mezi zařízeními.

Komunikace po AS-i sběrnici u PLC firmy Siemens:

- LOGO – může komunikovat po AS-i pomocí komunikačního procesoru CP – jen jako AS-i slave.
- S7 200 – může komunikovat po AS-i pomocí komunikačního procesoru CP 243-2 – jako AS-i master nebo AS-i slave.
- S7 300, S7 400 – může komunikovat po AS-i pomocí DP/AS-i link. DP/AS-i link je brána (rozhraní na všech vrstvách ISO-OSI modelu) mezi sběrnicemi AS-i a Profibus.

CP243-2 pro PLC S7 200

Ukázka použití AS-i sběrnice v v zapojení PLC S7 200 jako AS-i master, dvěma moduly As-i slave, napájením sběrnice (AS-i power supply) je zobrazen na obr. 2.4.

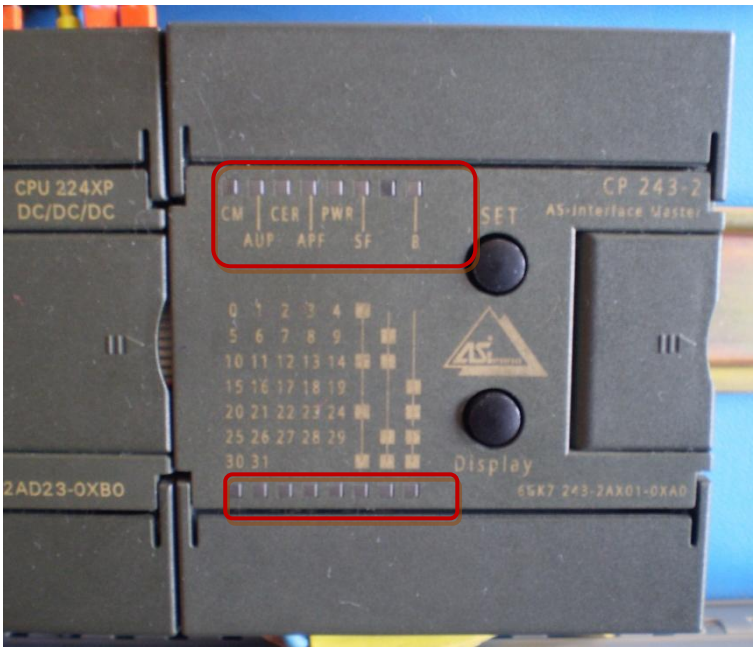


Obr. 2.4 Ukázka použití AS-i sběrnice v zapojení PLC S7 200.

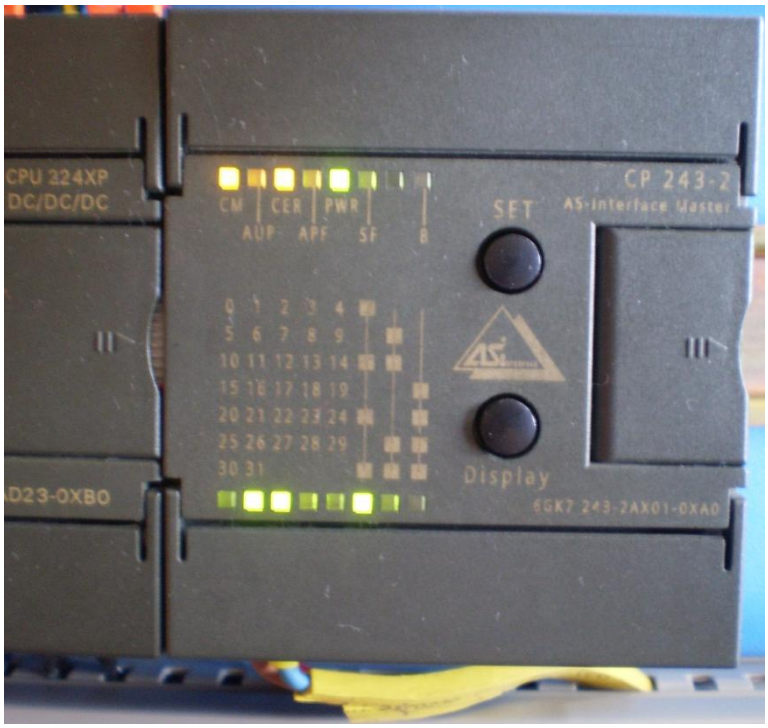
Na obr. 2.5 je zobrazen náhled na čelní panel komunikačního procesoru CP 243-2. Vlevo nahoře na obrázku lze vidět Status display s LED diodami signalizujícími stavy funkcí komunikačního procesoru.

V dolní části předního panelu komunikačního procesoru je slave display s 8 LED diodami rozdělenými do pěti sloupců (Slave display) a tří skupin (Group display). Postupným klikáním na tlačítko „Display“ se zobrazují jednotlivé skupiny připojených slave modulů na sběrnici.

Na obr. 2.6 je zobrazen příklad zapojeného slavu číslo 1 a 2 (svítí 2. a 3. LED dioda sloupce a 1. dioda skupiny).

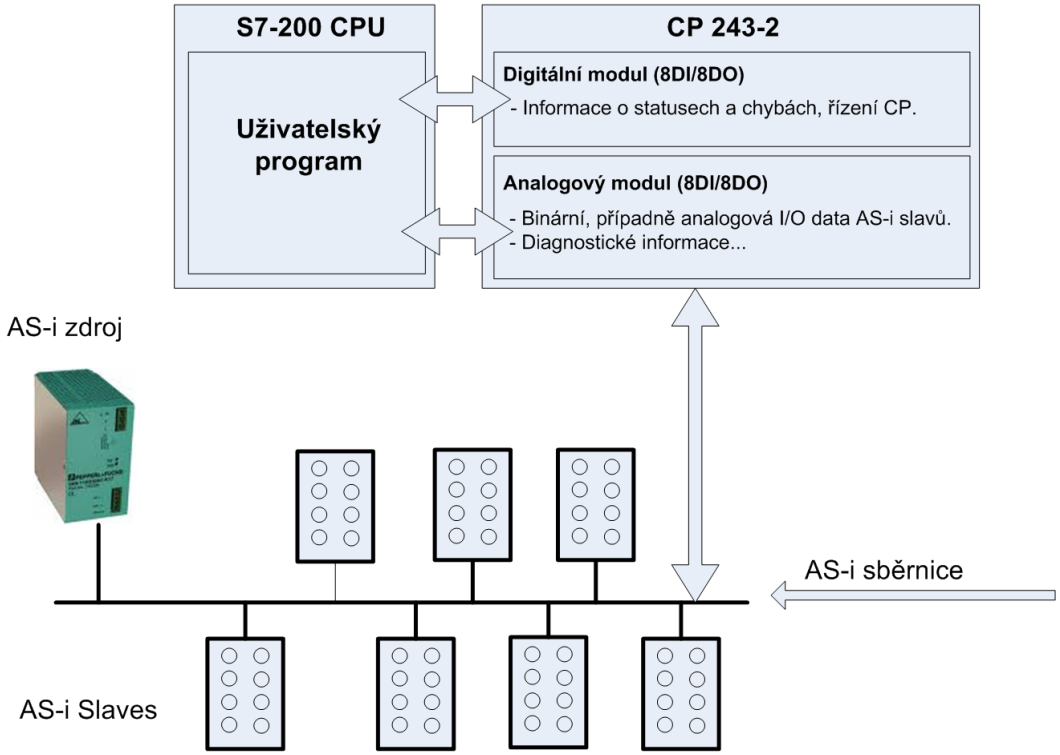


Obr. 2.5 Komunikační modul CP 243-2.



Obr. 2.6 Příklad zapojeného slavu číslo 1 a 2 určeného podle svítících LED diod sloupce a skupiny.

Programovatelný automat S7 200 komunikuje s komunikačním procesorem CP 243-2 prostřednictvím řídicího (control byte) a stavového (status byte) slova digitálního modulu (digital module). Analog modul (Analog module) pak obsahuje binární vstupní/výstupní data AS-i slave modulu (obr. 2.7).



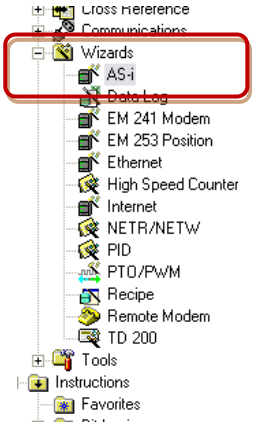
Obr. 2.7 Komunikace mezi PLC S7 200 a CP 243-2.

Řešená úloha 2.2

Zadání: Pomocí dostupného Wizzardu v prostředí MicroWIN pro PLC S7 200 nakonfigurujte komunikaci po sběrnici AS-i.

V laboratoři jsou k AS-i sběrnici připojeny čtyři AS-i slave moduly a adresami 1, 2, 7, 8 (pořadí slave modulů v učebně zleva: 2, 1, 8, 7).

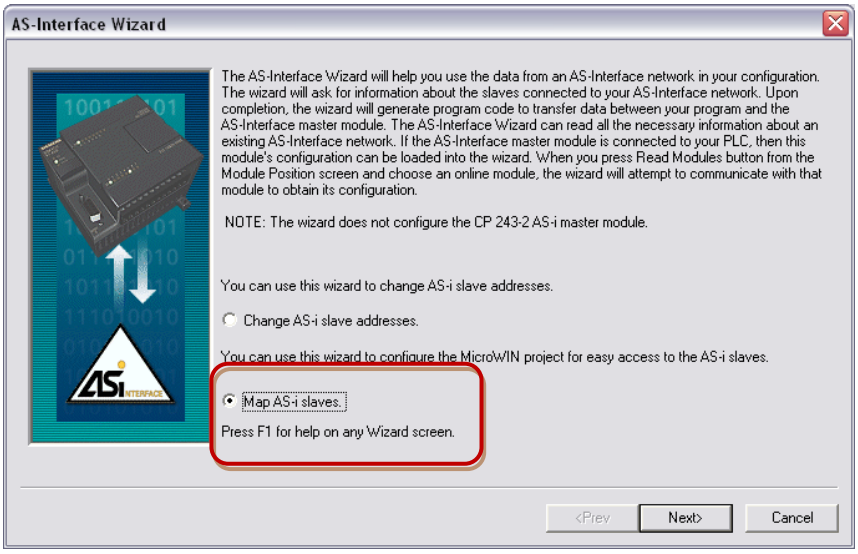
Pro použití AS-i sběrnice u programovatelných automatů S7 200 je v programovacím prostředí MicroWIN průvodce nastavením sběrnice (wizzard – obr. 2.8).



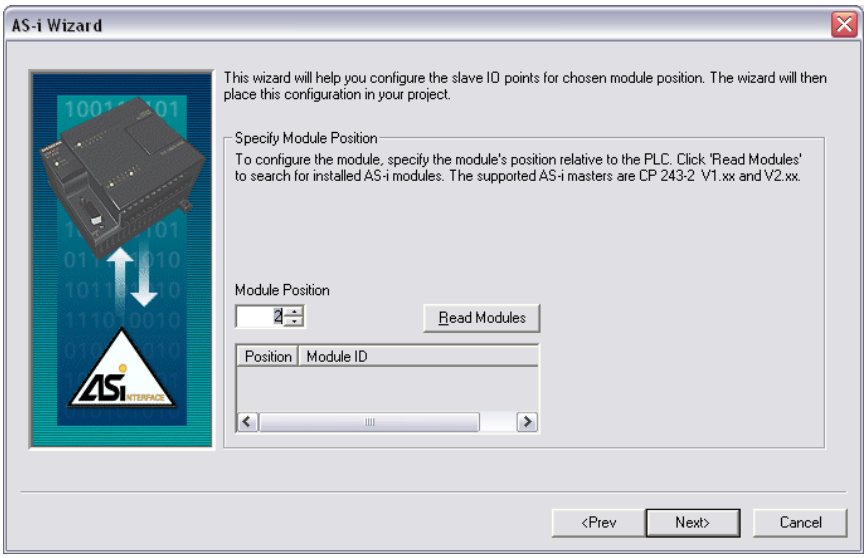
Obr. 2.8 Průvodce nastavením (wizzards) v programovacím prostředí MicroWIN

Wizzard se spustí dvojklikem na položku „AS-i“.

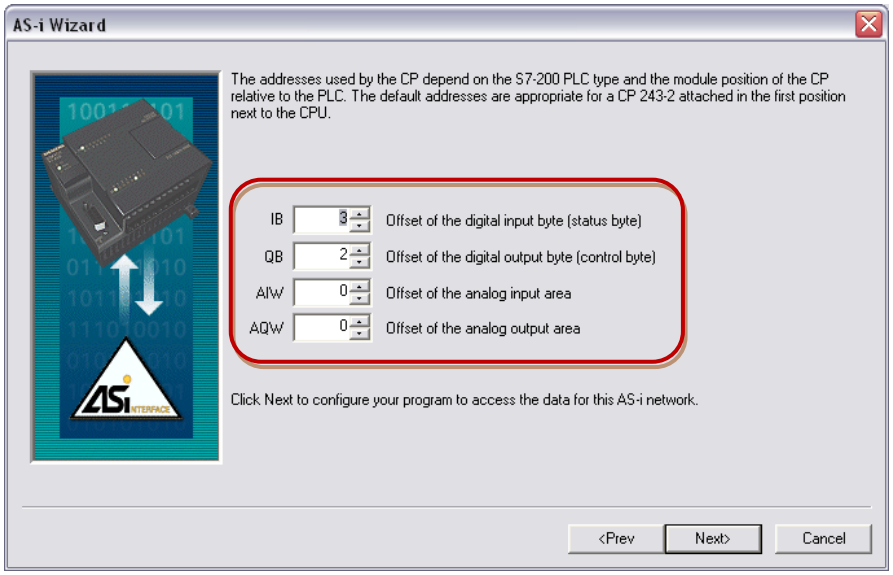
Obrazovka 1: Pokud je AS-i sběrnice fyzicky připojena pomocí komunikačního procesoru k PLC a jsou určeny jednotlivé AS-i slave moduly, je možno zatrhnout „Map AS-i slaves. Pomocí této volby se připojené slave moduly namapují.



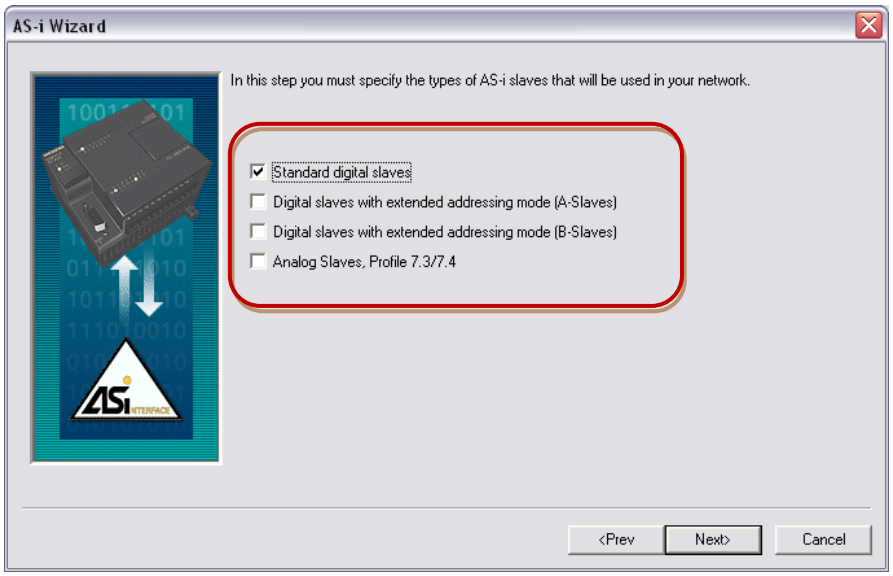
Obrazovka 2: Pozice modulu komunikačního procesoru vzhledem k CPU programovatelného automatu. Je zde možno zadat adresu komunikačního procesoru nebo, pokud existuje online připojení k AS-i sběrnici, pak volbou „Read modules“ se automaticky určí adresa připojeného komunikačního procesoru.



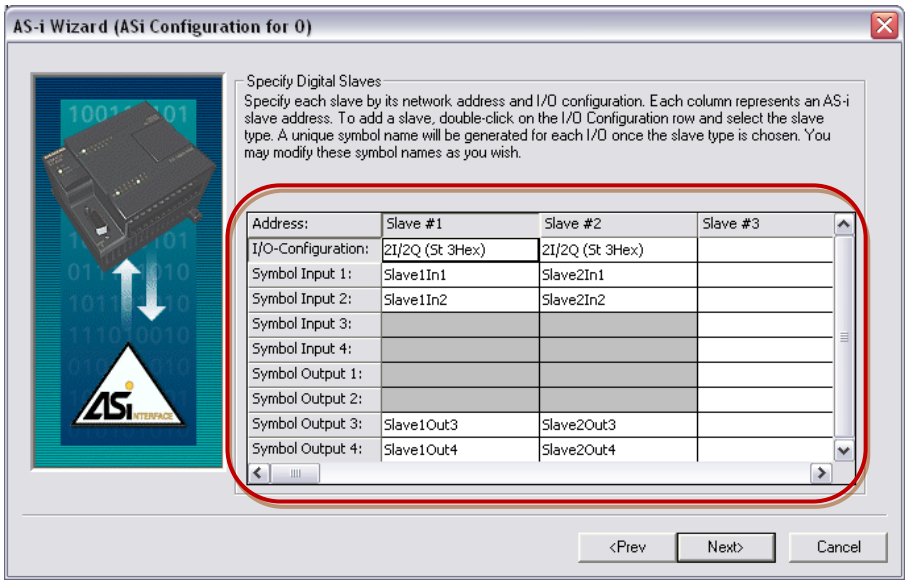
Obrazovka 3: PLC nabídne pozice řídicího slova, stavového slova a analogových vstupních a výstupních datových oblastí obsahujících vstupy a výstupy jednotlivých připojených AS-i slave modulů. Pokud bylo v předchozí obrazovce zvoleno „Read Module“ pak jsou tyto pozice určeny automaticky a nemění se.



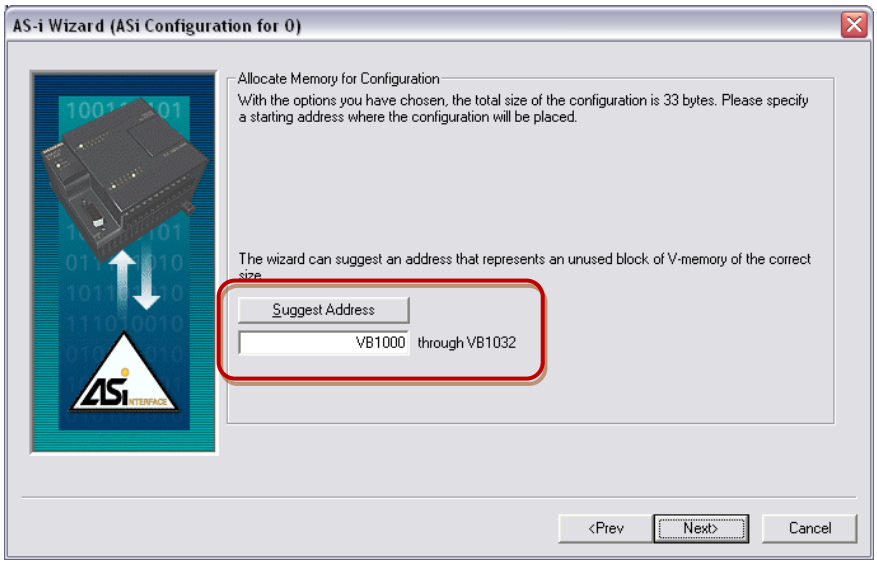
Obrazovka 4: V našem případě se volí „Standard digital slaves“.



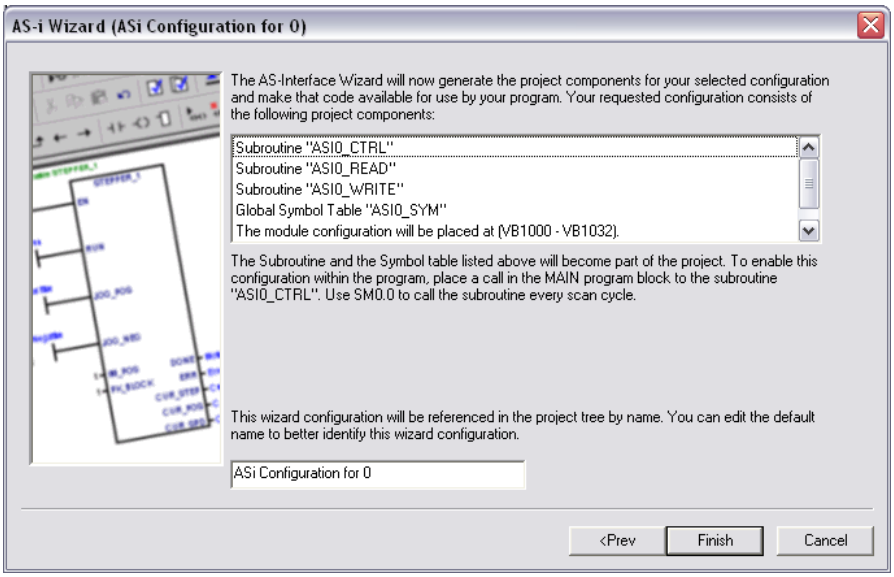
Obrazovka 5: Konfigurace jednotlivých AS-i slave modulů (1 až 31). V našem konkrétním případě jsou ty čtyři AS-i slave moduly, každý se dvěma vstupy a dvěma výstupy a s adresami 1, 2, 7 a 8 (Pozor: vstupy jsou na Symbol Input 1 a Symbol Input 2, ale výstupy jsou na Symbol Output 3 a Symbol Output 4).



Obrazovka 6: Návrh umístění vstupů a výstupů slave modulů v paměti PLC.



Obrazovka 7: Závěrečný přehled. Vygenerování subrutiny crtl, write, read, global symbol table.



DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI2\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI2\

Řešená úloha 2.3

Zadání: Využijte vytvořené konfigurace komunikace po sběrnici AS-i z řešené úlohy 2.2.

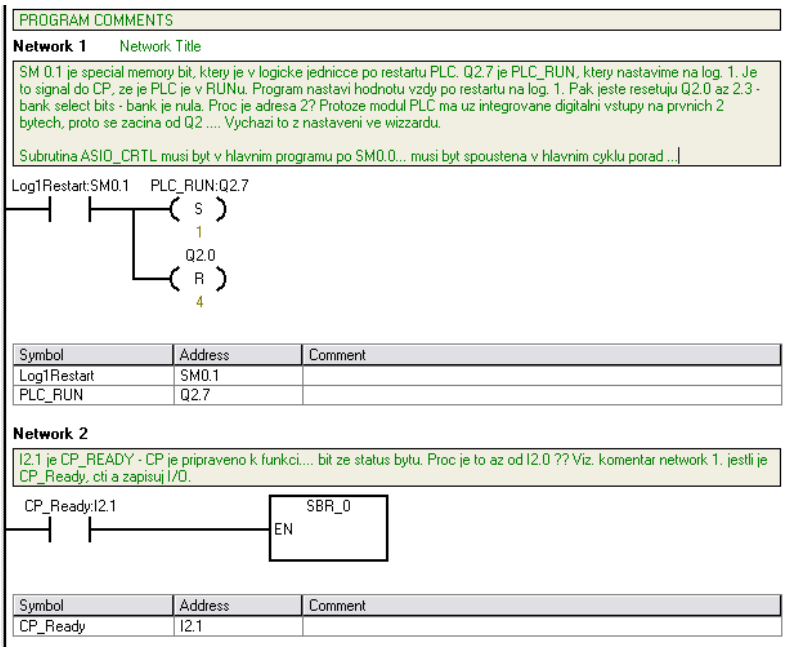
Na společný konektor AS-i slave modulů zapojených v jedné větvi v laboratoři připojte přípravek pro simulaci spínání vstupních signálů. Pro PLC S7 200 napište program tak, aby po přivedení logického signálu na příslušný vstup na AS-i slave modulu se tento signál zapsal na odpovídající digitální výstup na shodném AS-i slave modulu.

K řešení s výhodou využijeme vytvořené konfigurace PLC S7 200 s komunikačním procesorem CP243-2 z řešené úlohy 2.2.

Řešení programu v LAD

Z hlavní funkce Main je volána subrutina SBR_0, která obsahuje logiku programu. Detailnější popis částí programu je uveden k jednotlivým Networkům programu.

Main:

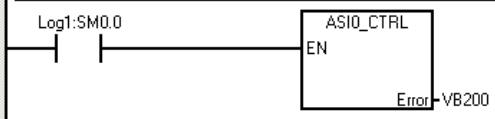


SBR_0:

SUBROUTINE COMMENTS

Network 1 Network Title

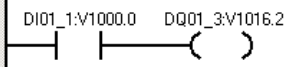
Volani subrutiny ASIO_CTRL.



Symbol	Address	Comment
Log1	SM0.0	

Network 2

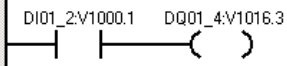
Je-li vstup v logicke jednicce, nastav vystup.



Symbol	Address	Comment
DI01_1	V1000.0	Symbol Input 1:Slave 1 - Digital (2I/2Q (St 3Hex))
DQ01_3	V1016.2	Symbol Output 3:Slave 1 - Digital (2I/2Q (St 3Hex))

Network 3

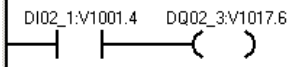
Je-li vstup v logicke jednicce, nastav vystup.



Symbol	Address	Comment
DI01_2	V1000.1	Symbol Input 2:Slave 1 - Digital (2I/2Q (St 3Hex))
DQ01_4	V1016.3	Symbol Output 4:Slave 1 - Digital (2I/2Q (St 3Hex))

Network 4

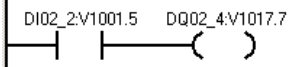
Je-li vstup v logicke jednicce, nastav vystup.



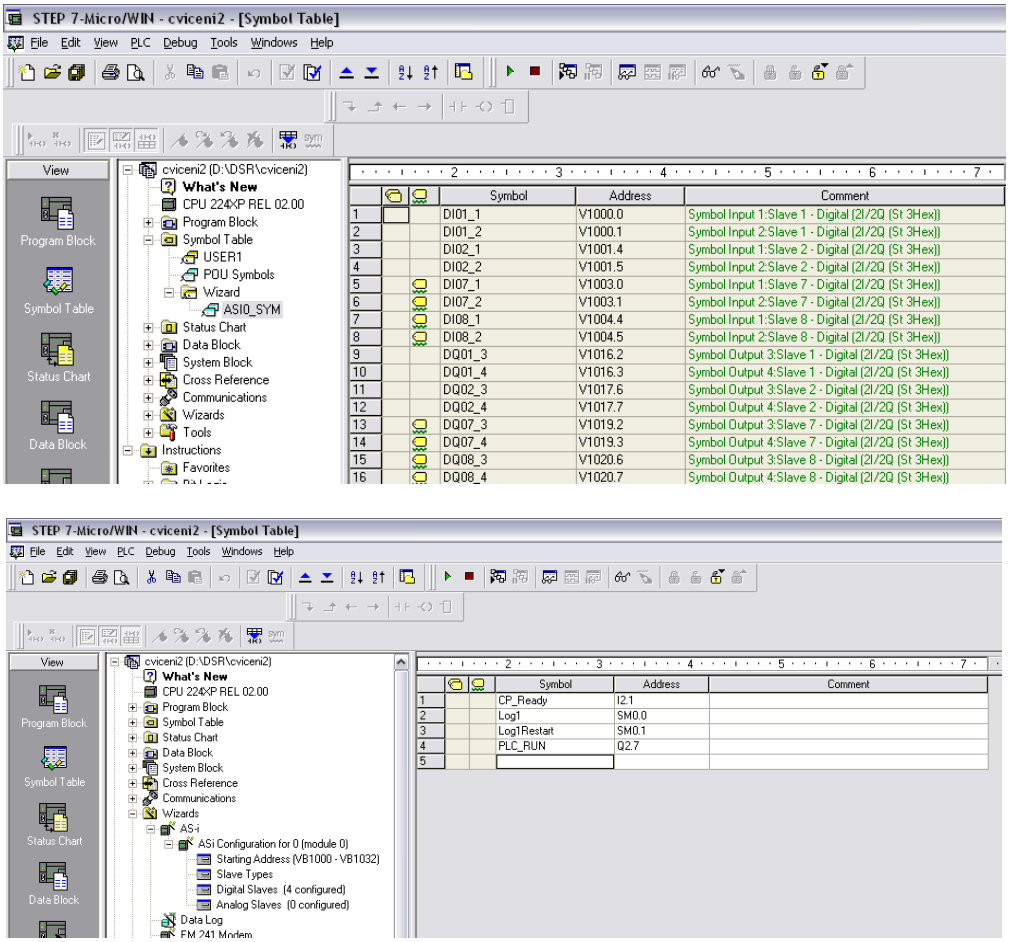
Symbol	Address	Comment
DI02_1	V1001.4	Symbol Input 1:Slave 2 - Digital (2I/2Q (St 3Hex))
DQ02_3	V1017.6	Symbol Output 3:Slave 2 - Digital (2I/2Q (St 3Hex))

Network 5

Je-li vstup v logicke jednicce, nastav vystup.



Symbol	Address	Comment
DI02_2	V1001.5	Symbol Input 2:Slave 2 - Digital (2I/2Q (St 3Hex))
DQ02_4	V1017.7	Symbol Output 4:Slave 2 - Digital (2I/2Q (St 3Hex))



Obr. 2.9 Tabulka symboliky a monitorování proměnných.

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI2\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI2\

3. FYZICKÁ VRSTVA ISO-OSI MODELU

Čas ke studiu: 3 hodiny

Cíl Po prostudování této kapitoly budete umět

- Popsat jednotlivé typy fyzických médií používaných v současných komunikačních systémech.
- Popsat způsoby přenosu dat ve fyzické vrstvě.
- Rozdělit přenosy podle možností šíření signálu.
- Popsat způsoby kódování bitů.
- Popsat příklady nejpoužívanějších standardů fyzických vrstev.
- V praktické části se naučíte vytvořit jednoduchou řídicí aplikaci pro programovatelný automat Simatic S7 300 s využitím komunikační sběrnice AS Interface (DP/ASI Link).

Výklad

Fyzická vrstva je jedinou vrstvou komunikačního systému, která reálně propojuje účastníky přenosu. Jejím úkolem je přenos jednotlivých bitů od vysílače k příjemci. Fyzická vrstva má bezprostřední přístup k přenosovému médiu, přenášené bity nijak neinterpretuje.

V rámci fyzické vrstvy se řeší elektrické, mechanické, funkční a procedurální vlastnosti rozhraní pro připojení různých prostředků pro přenos dat – např. elektrické vlastnosti přenášených signálů, význam, časový průběh, návaznosti signálů, zapojení konektorů apod. [1-9]

3.1. Přenosová média a jejich vlastnosti

V současné době se pro digitální přenos dat používá celá řada přenosových médií [1, 6]. Základní skupiny jsou:

- Metalická přenosová média.
- Optická přenosová média.
- Rádiofrekvenční bezdrátové spoje.
- Optické bezdrátové spoje (infračervené, laserové apod.).
- Ultrazvukové spoje.

U každého přenosového média je možné posoudit jeho vlastnosti ovlivňující přenos signálu. Jedná se zejména o tyto vlastnosti:

- Přenosová rychlost – je rychlost přenosu dat, kterou je možné u média dosáhnout (bit/s). Parametr přenosová rychlost úzce souvisí s parametrem šířka pásma přenosového média.

Jedná se o údaj udávající, jaké frekvence je možné médiem přenášet. Platí, že čím větší je šířka pásma přenosového kanálu, tím větší přenosovou rychlost na něm lze dosáhnout.

- Útlum signálu – jedná se o zeslabení přenášeného signálu průchodem přenosovým médiem. Tato vlastnost ovlivňuje maximální použitelnou délku kabelu. Zeslabení signálu se dá ovlivnit tím, že se mezi uzly připojí zařízení, které signál zesílí (např. opakovače).
- Odolnost proti rušení signálu – parametr, který říká, jak je přenosové médium ovlivnitelné rušivými vlivy okolí, zejména elektromagnetickým rušením. Specifickým typem rušení je tzv. přeslech, vzájemné rušení mezi vodiči, které se objevuje zejména při souběžných vedeních.
- Zkreslení signálu – změna signálu při průchodu komunikačním médiem. Útlumové zkreslení je způsobeno různým zesílením na jednotlivých frekvencích. Fázové zkreslení je nerovnoměrný fázový posun jednotlivých kmitočtových složek. Harmonické (amplitudové) zkreslení vzniká novými harmonickými kmitočty v obvodu, které nebyly na jeho vstupu.
- Mechanické vlastnosti komunikačních médií – odolnost proti ohybu, tahu, tlaku, mechanická pevnost apod.

Metalická přenosová média

Metalické kabely

Jedná se o soustavu dvou nebo několika elektrických vodičů spojených společným pláštěm. Vodiče mohou být plného průřezu nebo lanka. Metalická přenosová média jsou v dnešní době nejpoužívanějšími médiu. Informace je v nich přenášena pomocí elektrických veličin, zejména napětí, případně proudu. Materiálem pro tato média je nejčastěji měď. Pro přenos dat se používají zejména kroucená dvojlinka a koaxiální kabel.

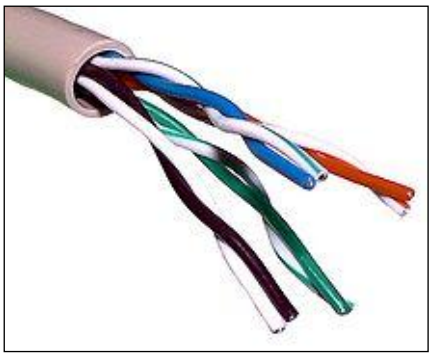
Kroucená dvojlinka (Twisted Pair, TP)

Jedná se o druh kabelu, tvořený párem vodičů, které jsou podélně pravidelně zkrouceny. Někdy se používá označení kroucený pár. V současnosti se často používají kabely (zejména v počítačových sítích), které sdružují několik kroucených párů, které jsou také vzájemně zakrouceny. Šířka pásma je několik stovek MHz a dosahovaná délka až stovky metrů.

Vodiče jsou vzájemně zkrouceny z důvodu zlepšení elektrických vlastností kabelu. Minimalizují se přeslechy, snižuje se vliv okolí na přenášený signál a také vliv vodičů na okolí. Zkroucením se výrazně snižuje vyzařování elektromagnetických vln vodiči do svého okolí. Vlastnosti kroucené dvojlinky lze dále zlepšit stíněním. [1, 3]

Přenášený signál je u kroucené dvojlinky obvykle dán rozdílem potenciálů mezi oběma vodiči.

- V současné době se s použitím kroucené dvojlinky lze setkat velice často v počítačových sítích, ale také v průmyslových komunikačních systémech. U počítačových sítí se používá označení:
- Nestíněná kroucená dvoulinka (Unshielded Twisted Pair, UTP), která nemá žádné stínění (viz. obr. 3.1).
- Stíněná kroucená dvoulinku (Shielded Twisted Pair, STP), která má samostatné stínění každého páru v kabelu.



Obr. 3.1 Kroucená dvojlinka [3].

Koaxiální kabel (Coaxial Cable)

Koaxiální kabel je elektrický kabel s jedním vnitřním vodičem a druhým válcovým vnějším vodičem, které jsou navzájem odděleny dielektrikem. Jedná se o asymetrický kabel, vnitřní vodič je obvykle nazýván jádrem, vnější stíněním. Jádro bývá obvykle vyrobeno z měděného plného drátu nebo lanka, stínění bývá realizováno hliníkovou fólií, či měděným opletem, dielektrikum je obvykle polyetylen, vzduch apod. Průměry kabelů se pohybují od několika milimetrů do desítek centimetrů.

Koaxiální kabelem se přenášení signály o frekvenci zhruba 600kHz až 6000MHz, ale lze jej použít i pro přenos stejnosměrného proudu. Používají se pro rozvody televizních, rádiových signálů, dříve se používaly běžně i u datových přenosů. V současné době se koaxiální kabely začínají znovu objevovat u datových přenosů na velké vzdálenosti často v kombinaci s optickými vlákny. [1, 4, 5]. Příklady koaxiálních kabelů jsou uvedeny na obr. 3.2.

Obr. 3.2 Koaxiální kabely [4].

Optická přenosová média

Optická přenosová média přenášejí data reprezentované světelným paprskem. Jsou obvykle komplikovanější a dražší než elektrická přenosová média [1, 6]. Přenosový systém obsahuje zařízení převádějící data nejčastěji reprezentovaná elektrickým signálem na světelný paprsek, vlastní přenosové médium a přijímací zařízení pro převod světelného paprsku zpět na elektrický signál. Zdrojem světla jsou LED diody nebo laserové diody. Optická přenosová média mají následující výhody:

- Velká šířka pásma – některé typy umožňují dosahovat přenosové vyšší než stovky GHz.
- Nízký útlum – přenos na velké vzdálenosti, podle typu vlákna až stovky kilometrů.
- Odolnost proti elektromagnetické interferenci a přeslechům.

- Elektrické izolační vlastnosti – přenosové médium nevytváří mezi komunikujícími zařízeními galvanické spojení.
- Bezpečnost přenosu (signál nelze jednoduše odposlechnout).
- Dostupný výrobní materiál (křemík).

Optická přenosová média mají následující nevýhody:

- Horší mechanická odolnost než metalická média, složitější spojování.
- Komplikovanější přenosový řetězec.
- Vyšší cena.

Optická vlákna

Mnohovidová optická vlákna (Multimode Optical Fibre, MM)

Mnohovidové optické vlákno je schopné přenášet současně více světelných paprsků. Každy z nich vstupuje do optického vlákna pod trochu jiným úhlem. Jedná se o vlákna se skokovým nebo gradientním indexem lomu. Světlo se v nich šíří odrazem, u vláken s gradientním indexem lomu se světelné paprsky „ohýbají“.

Mnohovidová optická vlákna se používají pro přenosy s rychlostí okolo 10 Mbit/s až 10 Gbit/s na vzdálenosti stovek metrů až jednotek kilometrů. Mají větší průměr (50/125 μm), jako zdroj světla se používají LED diody. Větší průměr jádra umožňuje jednodušší spojování, přenosový řetězec je levnější.

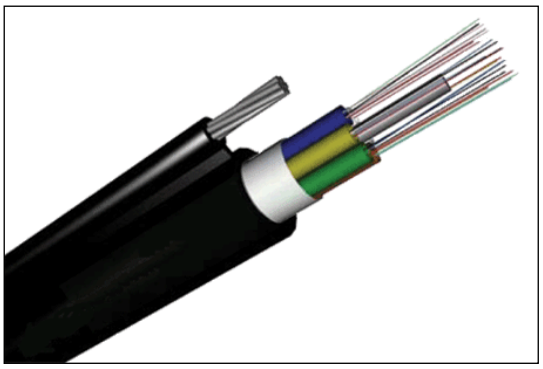
Jednovidová optická vlákna

Jednovidové optické vlákno přenáší jen jeden světelný paprsek, který se vláknem šíří bez odrazů. Jednovidová optická vlákna se používají pro přenosy s rychlostí v Gb/s, šířka pásma je vyšší než stovky GHz, používají se pro přenosy na velké vzdálenosti na desítky až stovky kilometrů. Mají menší průměr než mnohovidová vlákna (obvykle do 10 mikrometrů). Zdrojem světla je laserová dioda. Vzhledem k tomu, že jsou jednovidová vlákna tenčí a křehčí, jsou náročnější na manipulaci. Rovněž jejich cena je vyšší v porovnání s mnohavidovými vlákny.

V současné době se začínají používat rovněž plastová optická vlákna. Ta se odlišují od skleněných zejména mnohem vyšším průměrem (kolem 1000 mikrometrů), vyšší útlumem, ale lepšími mechanickým vlastnostmi a cenou.

Optické kabely

V praxi jsou optická vlákna příliš tenká a křehká, aby se dala používat samostatně. Bývají opatřena ochrannou vrstvou z vhodného materiálu, která zajistí potřebné mechanické vlastnosti. Často se jednotlivá optická vlákna sdružují do jednoho kabelu. Příklad optického kabelu je uveden na obr. 3.3.



Obr. 3.3 Koaxiální kabely [5].

Ostatní přenosová média

Rádiové bezdrátové spoje

Jedná se o přenosy pomocí elektromagnetických vln v rádiové oblasti spektra ($\lambda = 10^{3} – 10^{-1}$ m), případně v oblasti frekvencí nad 100MHz ($\lambda = 10^{-1} – 10^{-4}$ m), která je označována jako mikrovlná oblast. Výhodou těchto přenosových cest je to, že nevyžadují propojení komunikujících zařízení kabelem, nevýhodou je to, mohou být ovlivňovány překážkami na přenosové cestě a atmosférickými vlivy. Zatímco v oblasti rádiových vln (zejména u nižších frekvencí) se signál dokáže některým překážkám vyhnout, „obejít je“, v oblasti mikrovlných spojů je nutná přímá viditelnost. Elekrtomagnetické vlny o vyšších frekvencích se šíří přímočaře, je možné je směřovat na konkrétní cíl. Příkladem komunikačních systémů využívajících tyto přenosové cesty jsou bezdrátové sítě Wi-Fi, Motorola Canopy, Wi-Max) [7].

IR přenosy (infrared, infračervené)

U těchto přenosů se využívá infračervené oblasti spektra ($\lambda = 10^{-4} – 7{,}6 \times 10^{-7}$ m, označované taky jako IR záření nebo tepelné záření). Toto záření není viditelné okem. Obvykle se používají na krátkou vzdálenost při přímé viditelnosti. Typickými aplikacemi jsou v současnosti dálkové ovladače, komunikace mezi notebooky, mobilními telefony apod. Překážky jsou pro toto záření neprostupné a také může být přenos ovlivňován slunečním zářením [7].

Bezdrátové optické spoje (v oblasti viditelného světla)

Zatímco při použití optického vlákna je světlo vedeno přímo vláknem, při bezdrátovém přenosu ve viditelné oblasti spektra ($\lambda = 7{,}6 \times 10^{-7} – 3{,}9 \times 10^{-7}$ m) se světlo šíří vzduchem. Při tomto přenosu jsou překážky rovněž neprostupné, dále může být přenos značně ovlivňován atmosférickými vlivy.

3.2. Přenos dat ve fyzické vrstvě

Zajišťuje přenos jednotlivých bitů mezi příjemcem a odesílatelem prostřednictvím fyzické přenosové cesty, neinterpretuje však přenášené bity. Přenos signálu může být realizován různými způsoby. Podle následujících kritérií lze rozdělit základní formy přenosů [8].

Tab. 3.1 Základní dělení říká, zda jsou bity přenášeny „za sebou“ nebo paralelně.

Sériový přenos	Paralelní přenos
– Bity jsou přenášeny postupně, za sebou jedním vodičem. – Jednotlivé byty jsou pak tvořeny posloupností bitů. – U komunikačních sítí pro distribuované řídicí systémy se používá výhradně tento typ přenosu.	– Několik bitů dat je přenášeno současně. – Obvykle se přenáší celý byte nebo slovo. – Pro každý přenášený bit je nutný jeden vodič. – Přenosové vzdálenosti jsou kratší (obvykle max. jednotky metrů). – Často se používá uvnitř zařízení, počítačů, nebo pro propojení dvou zařízení (počítač-tiskárna). – U komunikačních sítí pro distribuované řídicí systémy se prakticky nepoužívá.

Tab. 3.2 Další dělení specifikuje, zda je přenášený signál synchronizovaný s hodinovým signálem.

Asynchronní přenos	Synchronní přenos
– Znaky jsou přenášeny s libovolnými časovými odstupy. – Pro rozpoznání jednotlivých znaků se používají smluvené příznaky (např. start bit). – Po rozpoznání začátku znaku může příjemce ve správný okamžik detekovat stavy jednotlivých přenášených bitů.	– Synchronní přenos je obvykle založen na přenosu celých bloků dat, nikoliv jednotlivých bytů. – V těchto blocích už nejsou jednotlivé znaky opatřeny start, stop bity. – Na začátku bloku dat se přenáší synchronizační sekvence, které umožní synchronizaci mezi vysílačem a přijímačem. – Obecně lze říci, že bity určené k přenosu generují současně se synchronizačními impulsy. – Synchronizační signál se obvykle nepřenáší samostatným vodičem, častěji bývá sloučen s datovým.

Tab. 3.3 Dělení podle způsobu využití šířky pásma přenosového média.

Přenos v základním pásmu (baseband transmission)	Přenos v přeloženém pásmu (broadband transmission)
– Bity jsou vysílány přímo na komunikační linku. – Je využit konkrétní typ kódování bitů, tzn. způsob reprezentace log.0 a log.1 napětím nebo jinou fyzikální veličinou.	– Jedná se o využití modulace. – Datový signál je reprezentován změnami, modulací nosného signálu. Nosný signál je obvykle harmonický signál. – Základní typy modulací jsou amplitudová modulace (AM), frekvenční modulace (FM), fázová modulace (FM), QAM (Quadratic Amplitude Modulation), aj.

Tab. 3.4 Rozdělení kanálu mezi jednotlivé komunikující zařízení. Cílem takového dělení je rozdělení přenosového kanálu na několik subkanálů. Tomuse říká multiplexování kanálu.

Časový multiplex TDM (Time Division Multiplexing)	Frekvenční multiplex FDM (Frequency Division Multiplexing)
– Kanál je rozdělen na časové úseky. – Každé zařízení vysílá jen v přidělených úsecích. – Každé zařízení má k dispozici celou šířku pásma kanálu po omezenou dobu. – Při tomto způsobu multiplexování lze dosáhnout lepšího využití přenosového kanálu.	– Kanál je rozdělen na frekvenční pásma. – Každému zařízení je přiděleno příslušné pásmo. – Každé zařízení má k dispozici omezenou šířku pásma po celou dobu.

Rozdělení přenosů podle možností šíření signálu:

- **Simplexní přenos** – přenos jedním směrem. Vysílač a přijímač jsou umístěni na opačných koncích kanálu a oba vysílají údaje stále stejným směrem.
- **Poloviční duplex (half-duplex)** – v daném časovém okamžiku disponuje kanálem jen jedna jednotka. Tento způsob odpovídá časovému multiplexování. Umožňuje obousměrný provoz, ale ne současně.
- **Plný duplex (full duplex)** – obě jednotky komunikují po celou dobu v obou směrech, proto se jedná o současný obousměrný provoz. Plný duplex se realizuje buď pomocí frekvenčního multiplexu, přičemž každá strana má přidělená vlastní kanál anebo tak, že pro každý směr je vyhrazen jeden fyzický kanál.

3.3. Způsoby kódování bitů ve fyzické vrstvě

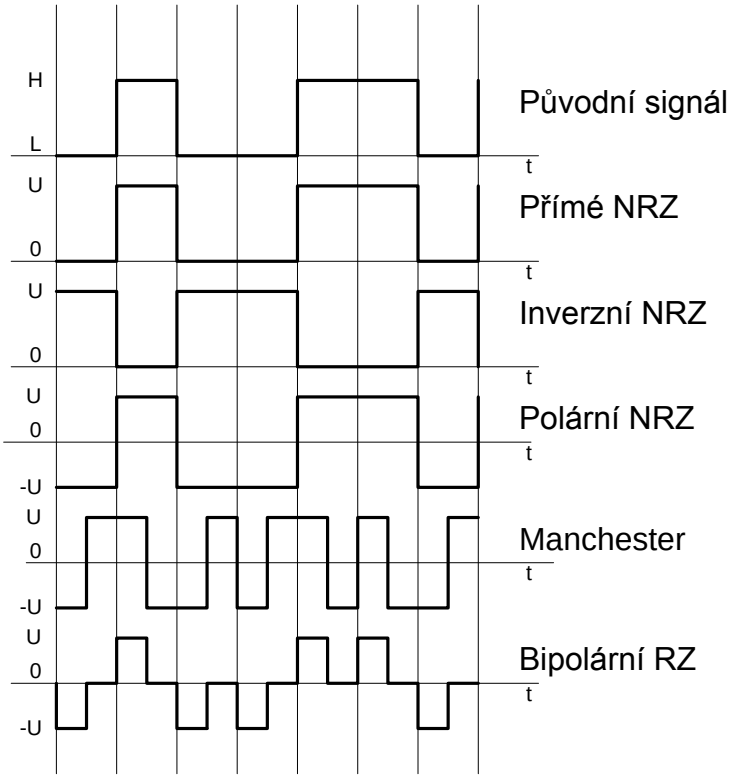
Při přenosu v základním pásmu je nutné, aby jednotlivé bity byly zakódovány do určitých úrovní fyzikálních veličin, zejména napětí nebo proudu [1, 8]. Existuje celá řada způsobů kódování, které se dají rozdělit do dvou základních skupin (obr. 3.4):

- NRZ (Non Return To Zero) - kódování, při kterém je po celý bitový interval konstantní úroveň signálu
  - Přímé kódování (např. 0V odpovídá log. 0 a 5V odpovídá log. 1)
  - Inverzní kódování (např. 5V odpovídá log. 0 a 0V odpovídá log. 1)
  - Polární kódování (např. -5V odpovídá log. 0 a 5V odpovídá log. 1)
- RZ (Return To Zero) - kódování, při kterém se signál v rámci bitového intervalu vrací do referenční úrovně. V podstatě to znamená, že datový signál je kombinovaný se synchronizačním signálem. U některých RZ kódování přechází signál v polovině bitového intervalu do referenční napěťové úrovně (pak log. 0 je hrana z vysoké do nízké úrovně signálu, log. 0 je hrana z nízké do vysoké). Takto funguje kódování Manchester. Další často používané kódování je označováno jako diferenciální Manchester, kde na začátku bitového intervalu dojde ke změně, pokud je log. 0, resp. nedojde ke změně, pokud je log. 1. Navíc uprostřed bitového intervalu se provádí ještě jedna změna pro zajištění synchronizace.

Kromě výše uvedených dvou základních kategorií se objevují různé modifikace:

- Kódování NRZI (Non Return To Zero Inversion) – změna polarity nastává jen na začátku bitového intervalu log. 0, pokud se přenáší log. 1 ke změně nedochází.
- AMI NRZ (Alternate Mark Inversion) –log. 0 a log. 1 střídavě mění polaritu.

- Kódování DUOBINARY – při úrovni log. 0 má signál nulovou úroveň, při log. 1 mění střídavě polaritu napětí.
- Aj.



Obr. 3.4 Příklady kódování.

3.4. Nejpoužívanější standardy pro fyzické vrstvy

RS232

Standard RS 232 je jedním z nejpoužívanějších sériových rozhraní. Od roku 1987 je používaný název EIA 232-D. Původně se tento standard používal pro připojení datového terminálu k modemu zajišťujícímu přístup na externí síť. Později se rozšířil jako jednoduchý komunikační kanál pro přenos dat mezi dvěma zařízeními. Známý je zejména z počítačové techniky, kde se dlouhou dobu používal jako základní sériové rozhraní pro připojení periferií (dnes se používá jen vyjímečně, je nahrazen rozhraním USB). V průmyslových aplikacích se stále poměrně často využívá. [1]

Základní parametry:

- Úrovně napětí jsou +3 až +15 V pro logickou 0 a –3 až –15 V pro logickou 1.
- Je použito inverzní kódování.
- Maximální přenosová rychlost se udává 19200 Bd/s při vzdálenosti 15m, 2400 Bd/s při 900m.
- Použitý konektor je Canon25, Canon9 nebo RJ45
- Základní typy zapojení jsou přímé propojení (komunikace DTE a DCE), nulový modem se vzájemným potvrzováním (7 vodičů), nulový modem bez potvrzování (3 vodiče)
- Výhody: jednoduchost, rozšířenost
- Nevýhody: komunikace pouze dvou zařízení, nízké přenosové rychlosti, malé vzdálenosti.

Zapojení konektoru pro Canon25:

Pin 1 – GND – ochranná zem, kostra.

Pin 2 – TD – vysílaná data, data vysílané z koncového zařízení (DTE) do modemu (DCE), pokud se žádná data nevysílají, udržuje se tento signál na log. 1.

Pin 3 – RD – přijímaná data, data přijímaná do koncového zařízení (DTE) z modemu (DCE), pokud se žádná data nevysílají, udržuje se tento signál na log. 1.

Pin 4 – RTS – žádost o vyslání dat – signál z DTE do DCE na uvolnění linky pro přenos.

Pin 5 – CTS – uvolnění vysílání – odezva z DCE do DTE jako indikace připravenosti linky po žádosti RTS.

Pin 6 – DSR – data připraveny. Indikace, že DCE je připraven přijímat data.

Pin 7 – SG – signálová zem, referenční úroveň 0V pro všechny signály.

Pin 8 – CD – detekce nosné.

Pin 20 –DTR – datový terminál přepraven. DTE připraven k činnosti.

Pin 22 – RI – indikace vyzvánění

RS422/RS423

Tyto standardy řeší některé nevýhody RS232, zejména malou délku přenosového média a nízkou přenosovou rychlost. [1]

RS 422 používá symetrické vysílače (symetrie impedance signálových výstupů vůči zemi), RS 423 nesymetrické. Základní parametry:

- Rozsahy signálů jsou 200mV až 6V a –200mV až –6V (log. 1/log. 0) u RS423 vzhledem k nulovému potenciálu vysílače, u RS422 mezi vodiči navzájem.
- Rozhraní RS422 dosahuje rychlost přenosu 100kbit/s na vzdálenost 1000m nebo až 10Mbit/s na vzdálenost 10m.
- Rozhraní RS423 dosahuje rychlost přenosu 3kbit/s na vzdálenost 1000m nebo až 300kbit/s na vzdálenost 10m.

Přes zlepšení přenosových parametrů, jsou i tyto standardy určeny pouze pro komunikaci dvou zařízení.

RS485

Tento komunikační standard již umožňuje realizaci vícebodového spojení, tzn. komunikaci mezi několika zařízeními. [1, 9]

Základní parametry:

- Přenosová rychlost 10MBd/s při vzdálenosti 15m, až 100 kBd/s při vzdálenosti 1200m.
- Pro přenos jsou nutné dva vodiče (často označované jako A, B), někdy, zejména u přenosů na delší vzdálenosti se vede rovněž signálová zem. V některých aplikacích se objevuje i plně duplexní varianta RS 485 se čtyřmi, resp pěti vodiči.
- Log. 1 je reprezentována rozdílovým napětím A - B < -300 mV, log. 0 rozdílovým napětím A - B > +300 mV.
- Na sběrnici může být až 32 zařízení (jednotkových zátěží), sběrnice musí být ukončena terminátory o hodnotě 100-120Ω.

Jedná se o velice často v současnosti používanou fyzickou vrstvu, zejména v průmyslových aplikacích. Je využívaná v celé řadě komunikačních systémů, jako například Profibus DP.

USB (Universal Serial Bus)

Nejpoužívanější sériové rozhraní u počítačů typu PC v současnosti. Používá se zejména pro připojení různých periferií k počítači.

Základní vlastnosti:

- Přenosová rychlost USB 1.1 – až 12 Mbit/s, USB 2.0 až 480 Mbit/s, USB 3.0 až 5 Gbit/s.
- Maximální délka kabelu je 5m.
- Kabel obsahuje 2 datové vodiče a 2 napájecí (5V a zem).
- Umožňuje používat rozbočovače (huby).

Fyzické vrstvy pro Ethernet

Ethernet využívá celou řadu fyzický vrstev, které nesou označení podle dosahované přenosové rychlosti a použitého typu přenosového média. Označení jsou např. tato 10Base-5, 10Base-T, 100Base-TX, 1000Base-SX apod. Další informace o těchto fyzických vrstvách jsou uvedeny v kapitole 9.

Shrnutí pojmů

V současné době se pro digitální přenos dat používá celá řada **přenosových médií**. Základní skupiny jsou:

- Metalická přenosová média.
- Optická přenosová média.
- Rádiofrekvenční bezdrátové spoje.
- Optické bezdrátové spoje (infračervené, laserové apod.).
- Ultrazvukové spoje.

Základní formy přenosů lze rozdělit na **sériové/paralelní**, **synchronní/asynchronní**, **přenos v základním/přeloženém pásmu**, **časový/frekvenční multiplex**.

Dále jemožné přenosy dělit na **simplexní přenos, poloviční duplex (half-duplex), plný duplex (full duplex).**

Při přenosu v základním pásmu je nutné, aby jednotlivé bity byly zakódovány do určitých úrovní fyzikálních veličin. Existuje celá řada způsobů kódování, které se dají rozdělit do dvou základních skupin – **NRZ** a **RZ**.

Mezi nejpoužívanější standardy pro fyzické vrstvy patří **RS232**, **RS422/423**, **RS485**, **USB** aj.

Otázky

1. Jaké jsou základní kvalitativní parametry přenosových médií?
2. Jaké typy přenosových médií se v současných komunikačních systémech používají?
3. Popište základní typy a vlastnosti metalických přenosových médií.
4. Popište základní typy a vlastnosti optických přenosových médií.
5. Jaké jsou způsoby přenosu dat ve fyzické lince?
6. Rozdělte přenosy podle možností šíření signálu.
7. Jaké jsou způsoby kódování bitů ve fyzické vrstvě?
8. Jaký je rozdíl mezi NRZ a RZ kódováním.
9. Jaké jsou základní standardy pro fyzické vrstvy.
10. Popište standard RS485.
11. Jaký jsou základní rozdíly mezi RS232 a RS485?

Další zdroje

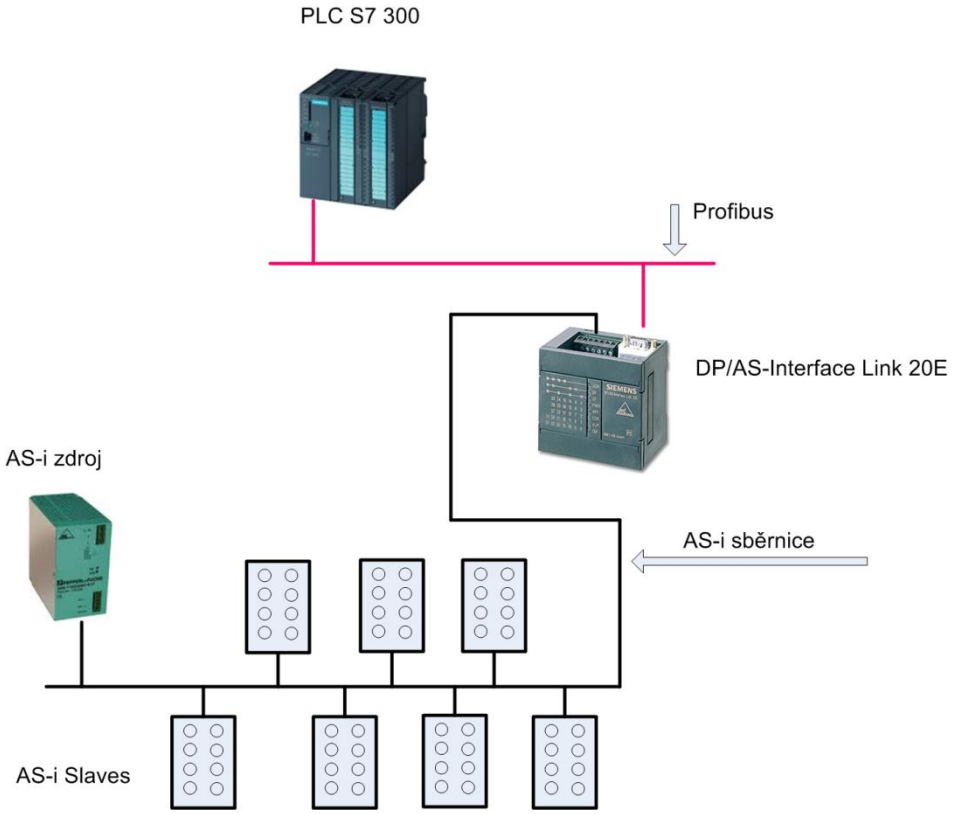
1. Kováč F. Distribuované riadiace systémy. Vydavatelstvo STU, Bratislava 1998. ISBN 80-227-1082-2.
2. Zezulka F.; Hynčica O. Průmyslový Ethernet II: Referenční model ISO/OSI. Automa 3/2007. ISSN 1210-9592.
3. Kroucená dvojlinka. Wikipedia. [online], [cit. 03-08-2010] http://cs.wikipedia.org/wiki/Kroucená_dvojlinka
4. Koaxiální kabel. [online], [cit. 03-08-2010] http://www.conrad.cz/koaxialni-kabel-aircom plus.k252930
5. Optický kabel. [online], [cit. 03-08-2010] http://www.world-trades.com
6. Báječný svět počítačových sítí, část VI. - Základy datových komunikací II. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/i_bajecnysvet.php3
7. Bezdrátové přenosové cesty. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a98/a842k180.php3
8. Základní formy přenosů. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a91/a140c110.php3
9. RS 485. Wikipedia. [online], [cit. 03-08-2010] http://cs.wikipedia.org/wiki/RS-485

Řešená úloha 3.1

Zadání: Seznamte se s charakteristikou DP/AS-i linku pro S7 300, který je určen pro komunikaci po sběrnici AS-i.

DP/AS-i link pro PLC S7 300/S7 400

DP/AS-i link je brána (rozhraní na všech vrstvách ISO-OSI modelu) mezi sběrnicemi AS-i a Profibus. Ukázka použití AS-i sběrnice v zapojení s DP/AS-i linkem, dvěma moduly AS-i slave, napájením sběrnice (AS-i power supply) je zobrazen na obr. 3.5.

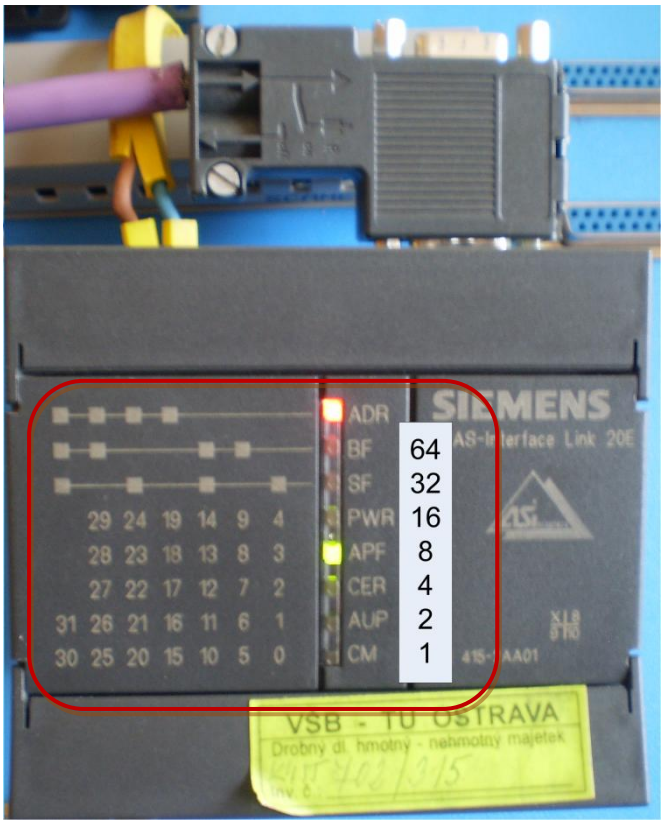


Obr. 3.5 Ukázka použití AS-i sběrnice v zapojení Profibus - AS-i

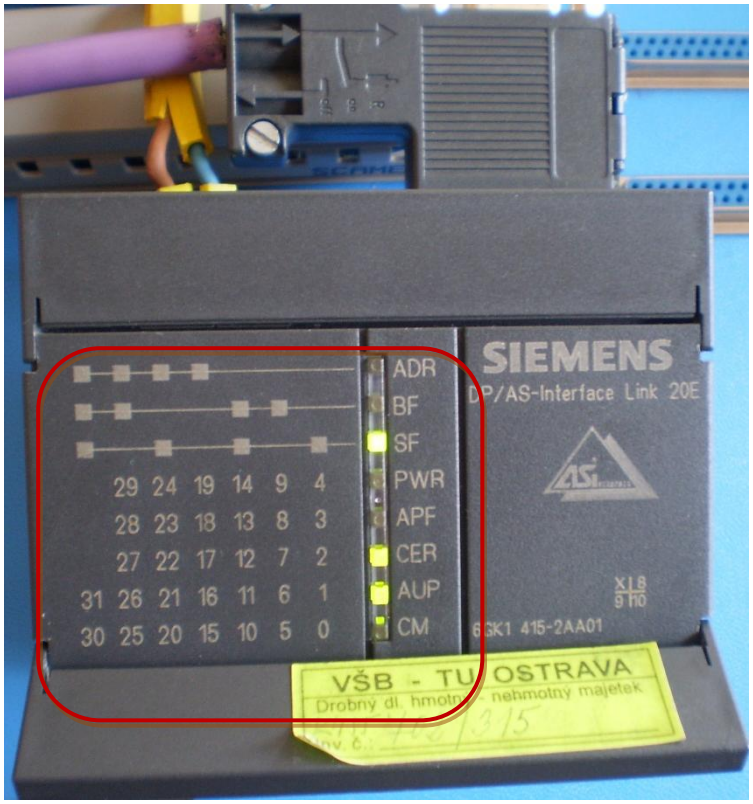
Na obr. 3.6 je zobrazen náhled na čelní panel DP/AS-i linku. Uprostřed čelního panelu lze vidět Status display s LED diodami signalizujícími stavy funkcí komunikačního procesoru.

Postupným klikáním na tlačítko „Display“ se zobrazují jednotlivé skupiny připojených slave modulů na sběrnici. Po poslední skupině je zobrazena profibus adresa DP/AS-i linku na sběrnici. (LED dioda ADR svítí červeně – obr. 3.7). Ukázka připojených slave modulů s adresami 1 a 2 na AS-i sběrnici je zobrazena na obr. 3.8.

Obr. 3.6 Náhled na čelní panel DP/AS-i linku.



Obr. 3.7 Zobrazení adresy DP/AS-i linku na sběrnici profibus – adresa zařízení je 8.



Obr. 3.8 Ukázka připojených slave modulů s adresami 1 a 2 na AS-i sběrnici.

Řešená úloha 3.2

Zadání: Vytvořte hardwarovou konfiguraci s PLC S7 300 (314-6CF02-0AB0) a DP/AS-i Linkem (6GK1 415-2AA01) pro připojení AS-i slave modulů k PLC S7 300. Nakonfigurujte sběrnici Profibus-DP a DP/AS-i link. DP/AS-i linku nastavte adresu 8 na sběrnici Profibus.

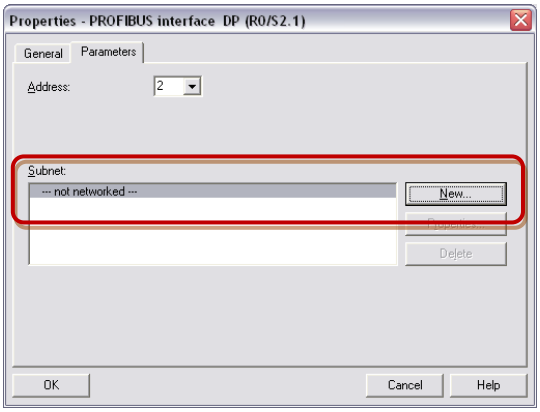
V laboratoři jsou k AS-i sběrnici připojeny čtyři AS-i slave moduly s adresami 1, 2, 7, 8 (pořadí slave modulů na stěně zleva: 2, 1, 8, 7).

Jsou-li AS-i slave moduly připojeny k DP/AS-i linku, který je na sběrnici profibus připojen k PLC S7 300/400, je nutno namapovat vstupy a výstupy slave AS-i modulů do paměti PLC. Toto namapování se provádí v hardwarové konfiguraci ve Step 7.

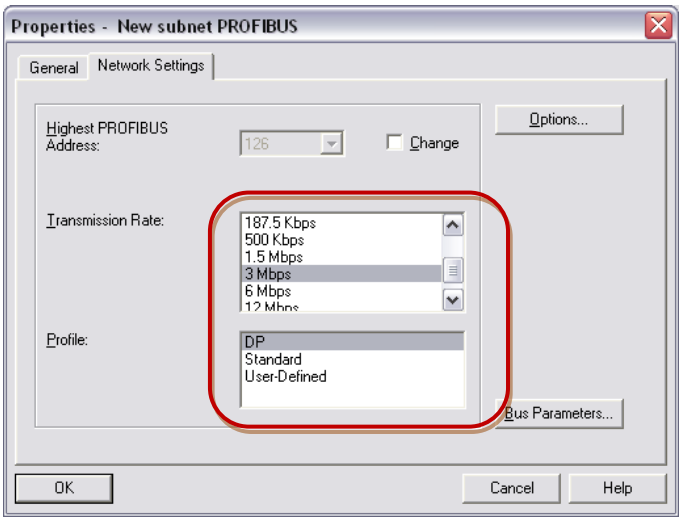
Hardwarová konfigurace bude obsahovat PLC S7-300, CPU 314C-2DP (6ES7 314-6CF02-0AB0) a periférii DP/AS-i link (6GK1 415-2AA01). CPU je umístěno ve složce CPU 300 a výběrem CPU 314C-2DP s objednacím číslem 6ES7 314-6CF02-0AB0 se vloží do slotu 2 připraveného racku.

Bezprostředně po vložení se zobrazí okno s konfigurací sběrnice Profibus-DP.

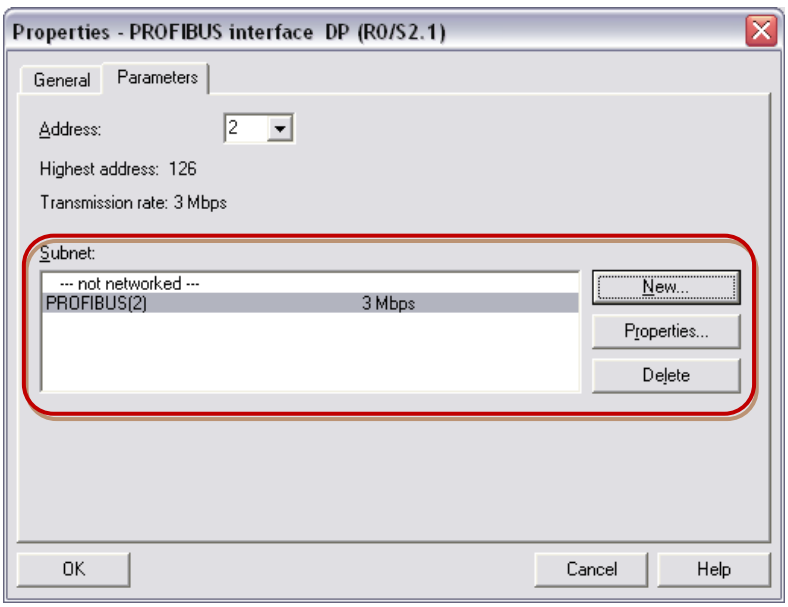
Adresa pro CPU je defaultně nastavena na 2. Kliknutím na tlačítko „New“ (obr. 3.9) se otevře okno s konfigurací sběrnice Profibus-DP. V okně „New subnet Profibus“ (obr. 3.10) v záložce „General“ lze zvolit přenosovou rychlost sběrnice (nastavíme 3Mbps) a profil (DP). Rychlost závisí na vzdálenosti periférií od CPU programovatelného automatu. Navíc pokud se v místě vedení trasy komunikační sběrnice vyskytuje rušení, měla by být rychlost pro větší spolehlivost přenosu snížena. Kliknutím na tlačítko OK se okno „New subnet Profibus“ zavře a následně se pomocí stisku na tlačítko OK zavře i okno „Profibus interface DP“ (obr. 3.11). Dokončená konfigurace sběrnice Profibus-DP je zobrazena na obr. 3.12.



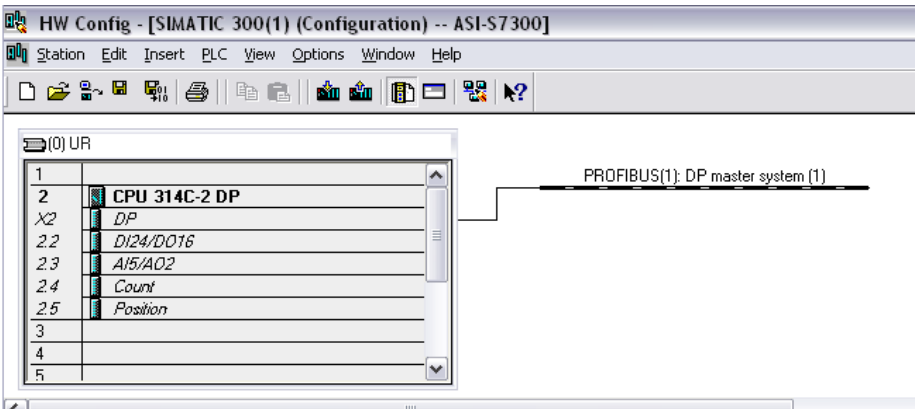
Obr. 3.9 Konfigurace Profibus-DP.



Obr. 3.10 Volba přenosové rychlosti a profilu sběrnice Profibus.

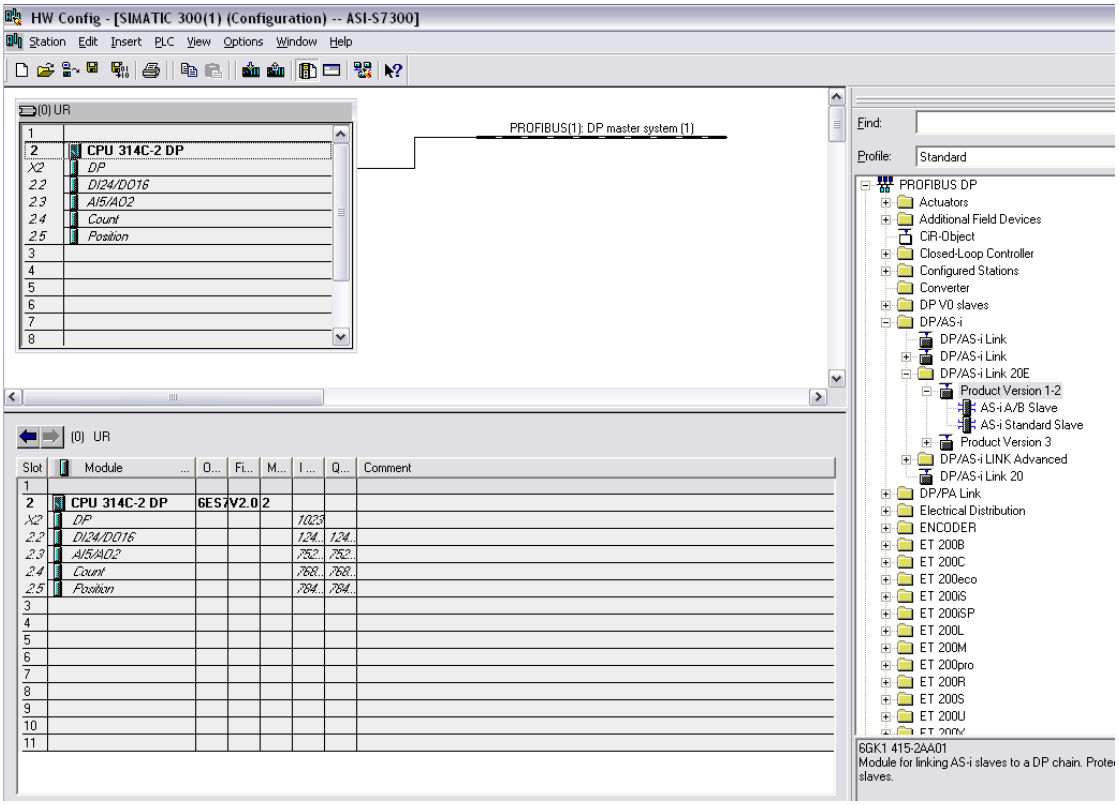


Obr. 3.11 Nastavení sběrnice Profibus-DP.

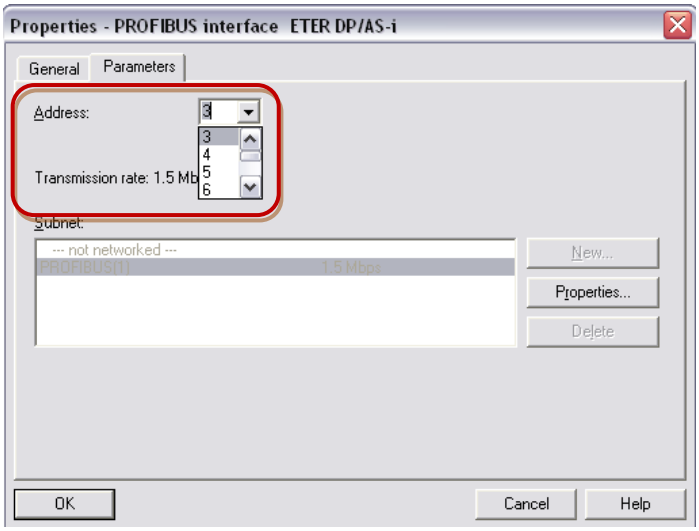


Obr. 3.12 Dokončená konfigurace sběrnice Profibus-DP.

DP/AS-i link je k dispozici ve sloce „Profibus-DP“ => DP/AS-i => DP/AS-i Link 20E (Product vision 1-2) (obr. 3.13). Kliknutím na ikonu DP/AS-i Link 20E (Product vision 1-2) a přetažením pomocí Drag&Drop se tento modul přemístí nad sběrnici a vloží. Po vložení se otevře okno se zadáním adresy DP/AS-i linku na Profibus-DP sběrnici. Adresu lze zjistit přímo na připojeném DP/AS-i linku pomocí tlačítka „Display“. V našem případě je adresa 8 (obr. 3.14).

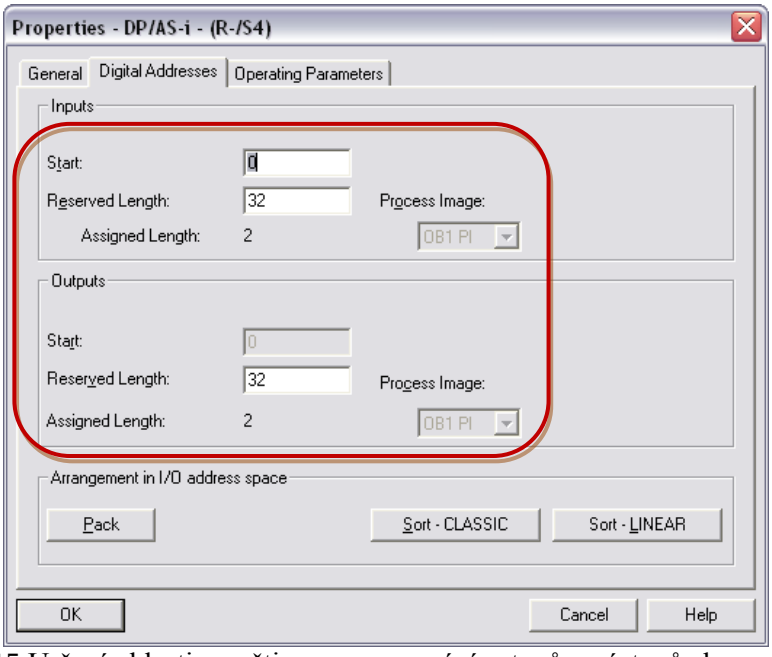


Obr 3.13 Umístění DP/AS-i linku v katalogu v hardwarové konfiguraci.



Obr 3.14 Pole pro zadání adresy DP/AS-i linku na sběrnici Profibus-DP.

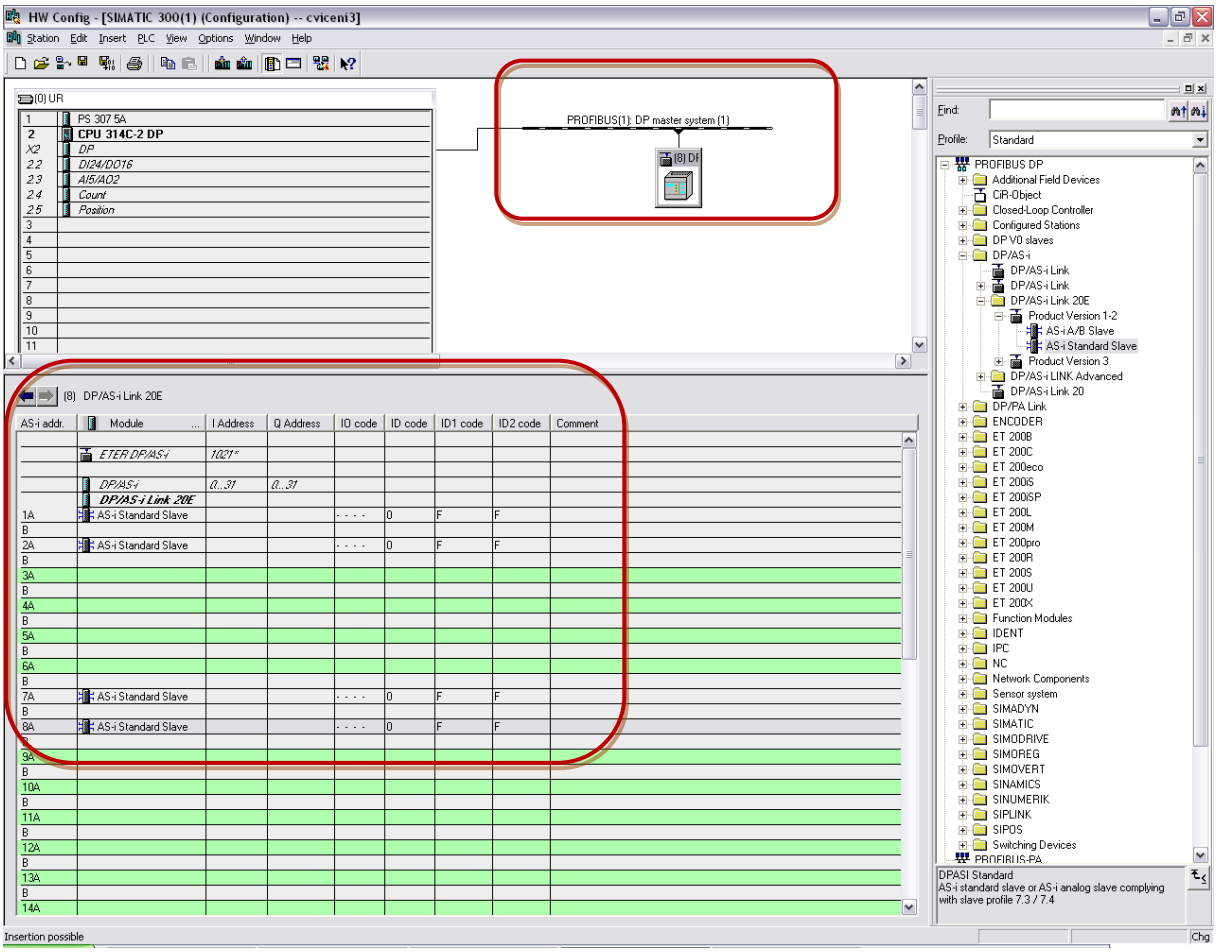
Kliknutím na vložený DP/AS-i link se dolní části otevřené hardwarové konfigurace objeví seznam adres pro slave moduly. Kliknutím na DP/AS-i se objeví okno, jehož náhled je na obr. 3.15. V záložce „Digital Addresses“ se definuje oblast paměti, kde se budou mapovat hodnoty vstupních a výstupních dat ze sběrnice AS-i. Pro vstupy a výstupy tedy definujeme počáteční adresu prvního vstupu. V našem případě ponecháme číslo nula.



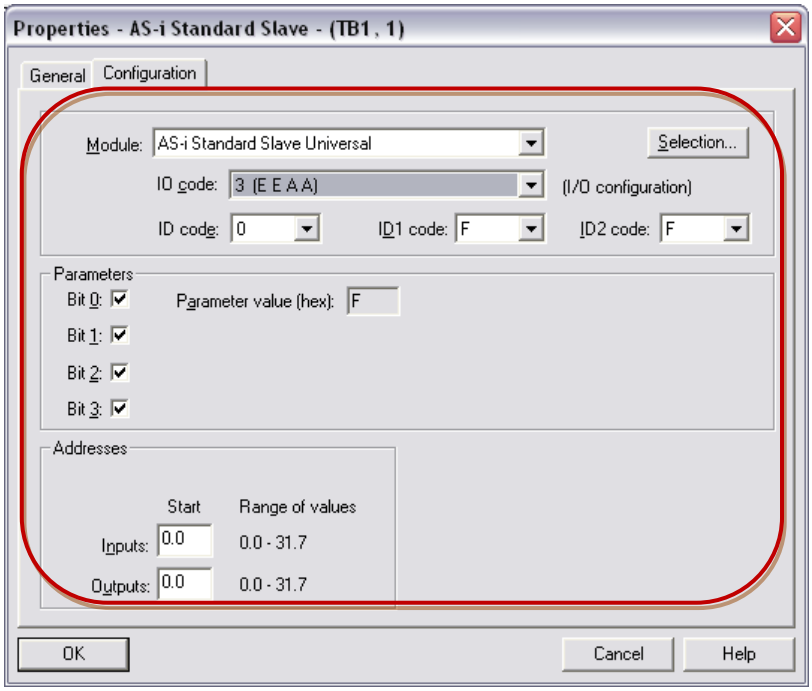
Obr 3.15 Určení oblasti paměti pro namapování vstupů a výstupů slave modulů.

V dalším kroku přistoupíme k vložení a nakonfigurování jednotlivých slave modulů DP/AS-i linku tak, aby konfigurace odpovídala reálného zapojení. Jednotlivé slave moduly (AS-i Standard Slave) jsou na adresách 1, 2, 7 a 8 (obr. 3.16) a do konfigurace jsou z katalogu pomocí Drag&Drop přeneseny stejně jako samotný DP/AS-i link. Každý slave modul je pak nutno nakonfigurovat podle toho, jaké typy slave modulů jsou fyzicky na AS-i sběrnici připojené. V našem případě jsou to moduly se dvěma vstupy a dvěma výstupy – nastavení je na kartě „Configuration“ po kliknutí na

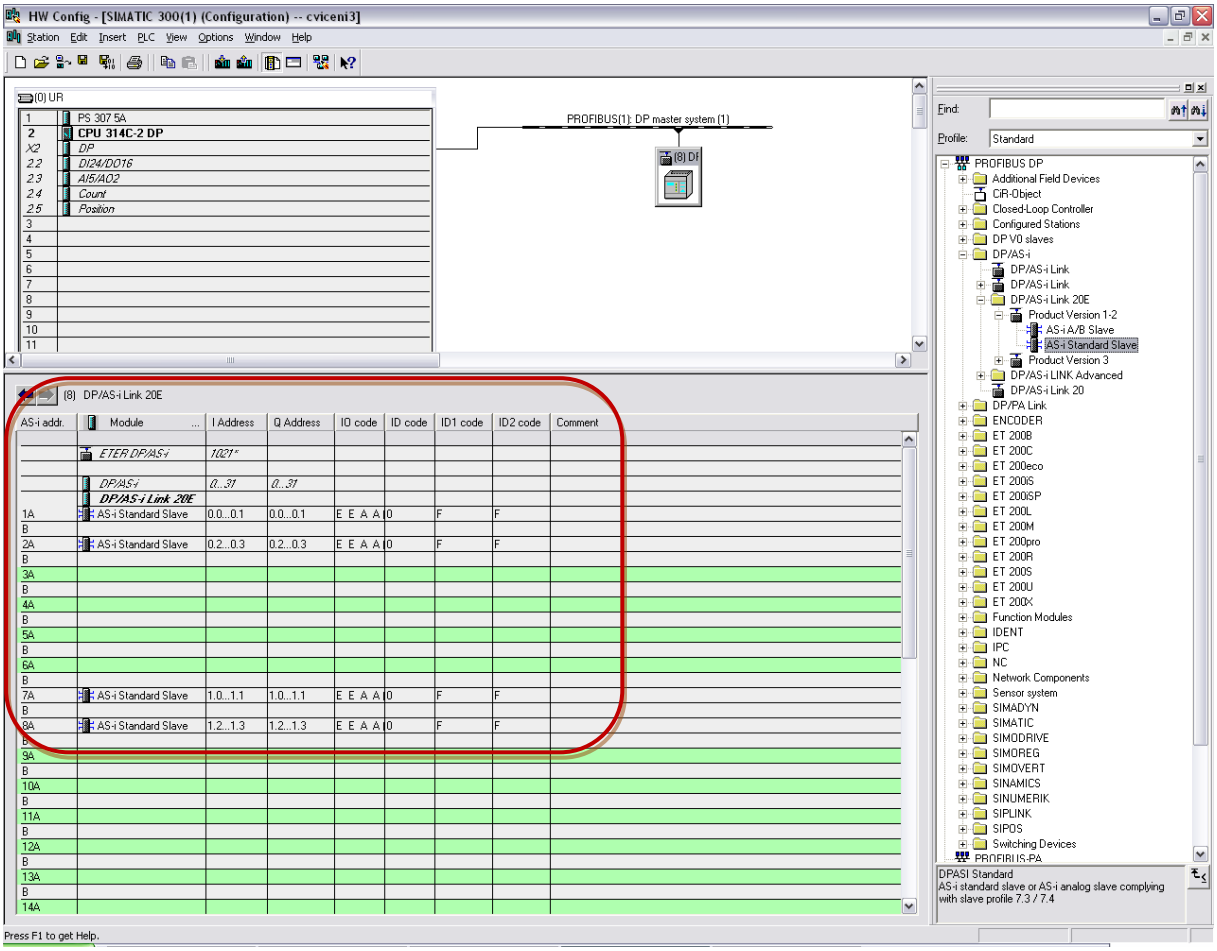
řádek s vloženým slave modulem. Parametry „ID code“, „ID1 code“ a „ID2 code“ je nutno určit z dostupných manuálů použitých AS-i slave mosulů. V našem případě platí nastavení shodné s obr. 3.17. Celkové konečné nastavení hardwarové konfigurace se zadaným CPU 314C-2DP a DP/AS-i linkem připojeným k CPU pomocí Profibus-DP, je zobrazeno na obr. 3.18. Z obr. 3.18 jsou pak i zřejmé adresy jednotlivých vstupů a výstupů, pomocí kterých budeme v programu přistupovat k daným vstupům a výstupům AS-i slave modulů.



Obr 3.16 Vložení jednotlivých slave modulů.



Obr 3.17 Konfigurace jednotlivých slave modulů.



Obr 3.18 Konečná konfigurace DP/AS-i linku – is adresami vstupů a výstupů.

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI3\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI3\

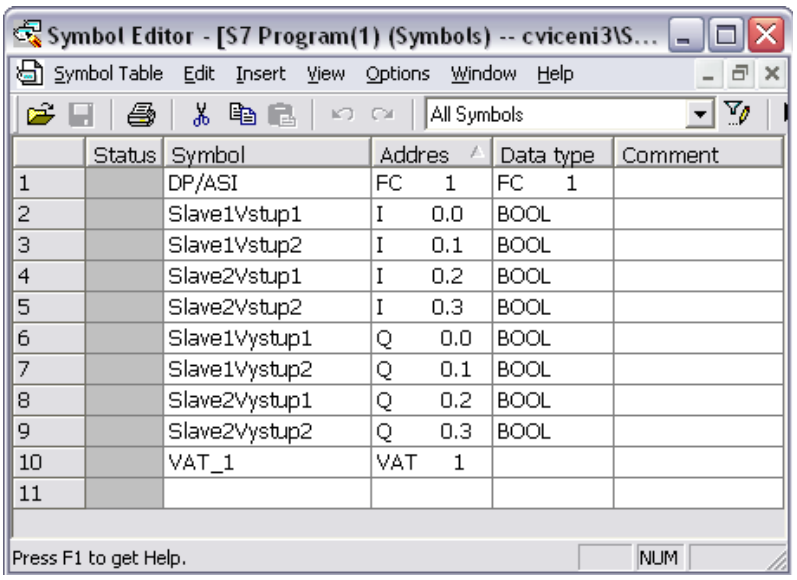
Řešená úloha 3.3

Zadání: Využijte vytvořené hardwarové konfigurace z řešené úlohy 3.2.

Na společný konektor AS-i slave modulů zapojených v jedné větvi v laboratoři připojte přípravek pro simulaci spínání vstupních signálů. Pro PLC S7 300 napište program tak, aby se po přivedení logického signálu na příslušný vstup na AS-i slave modulu tento signál zapsal na odpovídající digitální výstup na shodném AS-i slave modulu.

K řešení s výhodou využijeme vytvořené hardwarové konfigurace z řešené úlohy 3.2. V této úloze je vytvořena hardwarová konfigurace s PLC S7 300 (CPU 314-2DP) a s DP/AS-i Linkem připojeným k PLC přes sběrnici Profibus-DP. V hardwarové konfiguraci jsou namapovány vstupy a výstupy AS-i slave modulů do oblasti paměti PLC.

Tabulka symbolů pro vstupy a výstupy programu je zobrazena na obr. 3.19.

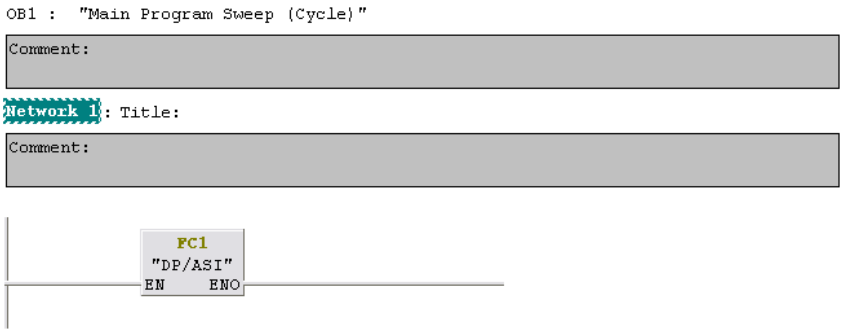


	Status	Symbol	Addres	Data type	Comment
1		DP/ASI	FC 1	FC 1	
2		Slave1Vstup1	I 0.0	BOOL	
3		Slave1Vstup2	I 0.1	BOOL	
4		Slave2Vstup1	I 0.2	BOOL	
5		Slave2Vstup2	I 0.3	BOOL	
6		Slave1Vystup1	Q 0.0	BOOL	
7		Slave1Vystup2	Q 0.1	BOOL	
8		Slave2Vystup1	Q 0.2	BOOL	
9		Slave2Vystup2	Q 0.3	BOOL	
10		VAT_1	VAT 1		
11					

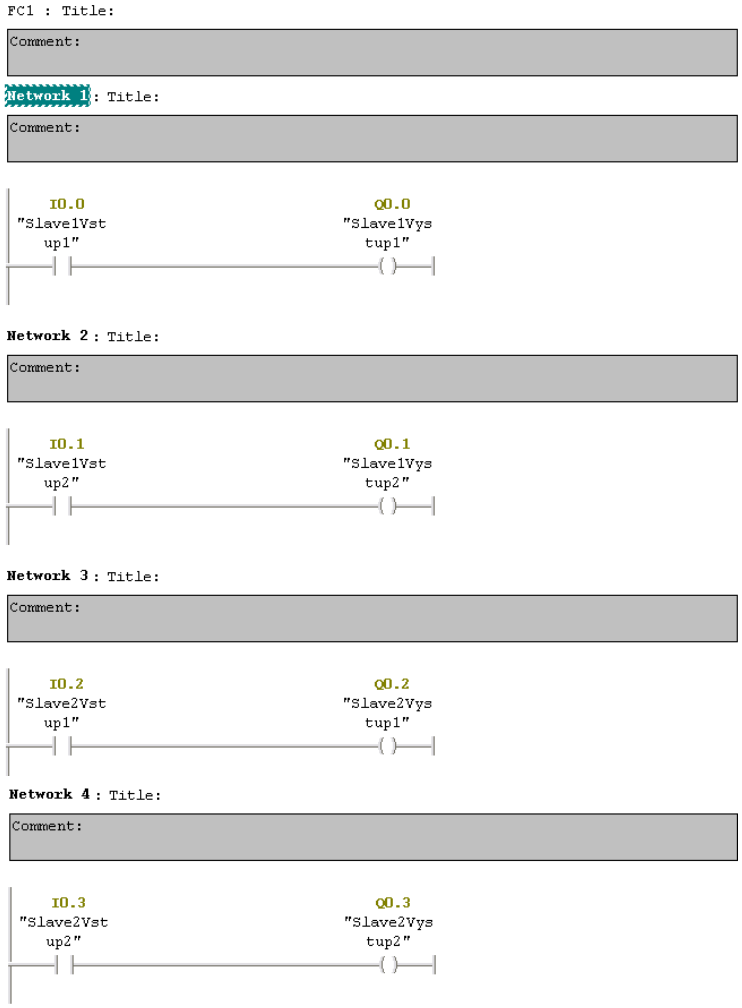
Obr. 3.19 Tabulka symbolů.

Program je tvořen organizačním blokem OB1, kterým je volána funkce FC1.

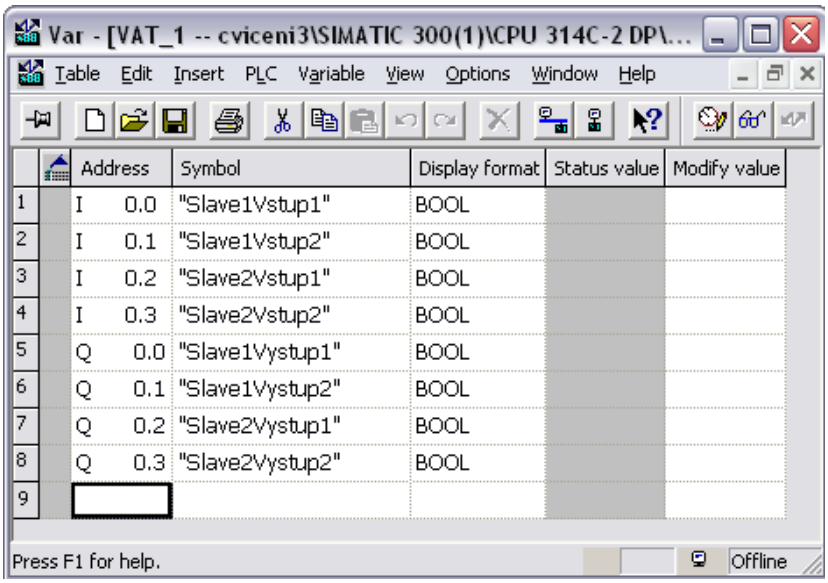
OB1:

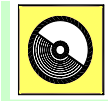


FC1:



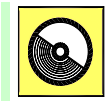
VAT tabulka:





DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI3\



DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI3\

4. LINKOVÁ VRSTVA ISO-OSI MODELU

Čas ke studiu: 3 hodiny

Cíl Po prostudování této kapitoly budete umět

- Popsat činnosti, které řeší linková vrstva ISO OSI modelu.
- Popsat způsoby řízení přenosu v linkové vrstvě.
- Popsat způsoby detekce a korekce v linkové vrstvě.
- Popsat způsoby potvrzování a řízení toku dat.
- Popsat způsoby přístupu ke komunikačnímu médiu.

Výklad

Linková vrstva je podobně jako fyzická vrstva velice důležitá a žádný komunikační systém se bez ní neobejde. Vyšší vrstvy naopak v řadě komunikačních systémů využity nejsou. U řady průmyslových komunikačních systémů se setkáváme s tím, že jsou definovány pouze na prvních dvou vrtsvách (např. Profibus DP, CAN apod.).

Linková vrstva zajišťuje následující funkce:

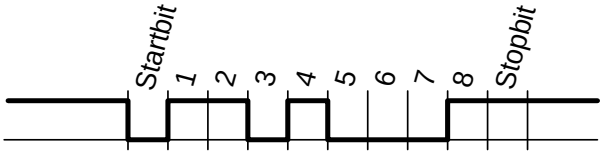
- Zajišťuje bezchybný přenos bloků dat mezi dvěma zařízeními.
- Rozpoznává začátek a konec rámce a jeho jednotlivé části – fyzická vrstva pouze přenáší jednotlivé bity, neinterpretuje jejich význam. To je úlohou linkové vrstvy, která musí rozpoznat řidicí informace v rámci a užitečná data.
- Zajišťuje přístup ke komunikačnímu médiu (Media Access Control)
- Řízení toku dat, synchronizaci na úrovni rámců.
- Detekci nebo korekci chyb.

4.1. Řízení přenosu v linkové vrstvě

Aby přijímač dokázal správně interpretovat přijímané data, musí jednotlivé bity detekovat ve správných okamžicích. Musí být tedy s vysílačem určitým způsobem synchronizován. Zcela nezbytné je to u synchronního přenosu, ale i asychnchronního přenosu jsou nutné určité synchronizační mechanizmy, které umožní správné rozpoznání přijímaných dat. [1, 2, 3]

Asynchronní sériový přenos

U tohoto typu přenosu jsou jednotlivé znaky přenášeny s libovolnými časovými odstupy. Je zde zaceden mechanizmu, který příjemci umožní správně rozpoznat začátek a konec znaku. Základem uvedeného mechanizmu je vložení příznaku na začátek a konec znaku. Tyto příznaky se označují STARTBIT a STOPBIT (viz. obr. 4.1). Mezi těmito příznaky se přenáší vlastní znak tvořený posloupností bitů. Startbit začíná hranou z klidového stavu sběrnice do opačného stavu a tím je rozpoznán začátek znaku. Od tohoto okamžiku je očekáván příjem jednotlivých bitů s předem stanovenou přenosovou rychlostí.



Obr. 4.1 Struktura znaku při asynchronním přenosu.

Pokud se pomocí asynchronního přenosu posílají bloky dat (rámce) tvořené posloupností znaků, je nutné dále správně rozpoznat začátek a konec bloků – zajistit synchronizaci na úrovni rámců. Zde mohou nastat dva základní případy:

- Přenášený blok dat obsahuje ASCII znaky – v tomto případě se začátek a konec bloku označuje speciálními řídicími znaky, které ASCII tabulka neobsahuje, tzn. se nemohou vyskytnout v přenášených datech – STX (Start of Text), ETX (End of Text) - viz. obr. 4.2.
- Přenášený blok dat obsahuje obecná binární data – tato data mohou obsahovat i znaky shodné s řídicími znaky. Pak je třeba zajistit transparentnost dat (zajištění toho, že jsou správně rozpoznány řídicí a datové znaky) pomocí vkládání znaků – DLE (Data Link Escape). Před každý řídicí znak se vkládá DLE, čímž se označí, že se jedná o řídicí znak. Pokud se DLE vyskytuje i mezi v přenášených datech, jeho výskyt se zdvojuje – tzn. pokud po DLE následuje STX nebo ETX, jedná se o řídicí znak, pokud znovu DLE, jedná se o data - viz. obr. 4.3.

Obr. 4.2 Struktura znaku při asynchronním přenosu.

Obr. 4.3 Struktura znaku při asynchronním přenosu.

Vkládáním startbitů, stopbitů a řídicích znaků se zvyšuje režie přenosu, jelikož je nutné přenést více dat, než obsahuje samotný rámec. Tím se snižuje reálná přenosová rychlost. Z pohledu režie přenosu je na tom lépe synchronní sériový přenos.

Synchronní sériový přenos

U synchronního přenosu se přenáší rámec bez vkládání startbitů a stopbitů. To, aby příjemce správně rozpoznal jednotlivé bity rámce, je zajištěno pomocí synchronizačních znaků SYN na začátku rámce. Tyto synchronizační znaky slouží k tomu, aby mohl přijímač správně určit délku bitového intervalu pro následující blok dat.

Synchronní sériové přenosy se dělí do následujících skupin:

- Znakově orientované přenosy - synchronizace na úrovni rámců se řeší pomocí vkládání řídicích znaků STX, ETX, DLE - viz. obr. 4.4.
- Blokově orientované přenosy – transparentnost přenosu se zabezpečí pomocí vložení informačního pole do rámce určující délku datového pole.
- Bitově orientované přenosy – rámec je uveden a zakončen skupinou bitů (nikoliv znaky). Tato skupina bitů se označuje jako FLAG a nesmí se vyskytovat v přenášených datech - viz.

obr. 4.5. U lokálních sítí se používá pro uvození rámce tzv. preambule (synchronizační pole), příznak začátku rámce, hlavička a délka přenášených dat - viz. obr. 4.6.

Obr. 4.4 Znakově orientovaný přenos.

Obr. 4.5 Bitově orientovaný přenos.

Obr. 4.6 Bitově orientovaný přenos.

4.2. Detekce a korekce chyb

Pro zajištění bezchybného přenosu dat mezi dvěma zařízeními musí mít linková vrstva implementovány algoritmy, které jsou schopny spolehlivě detekovat chybný přenos a případně chybu odstranit [1, 2, 3]. S tím souvisí pojmy detekce a korekce chyb:

- Detekce chyb (Error Detection) – k původní zprávě jsou přidané určité informace, na základě kterých přijímač zjistí, zda jsou přijatá data správná či nikoliv. To se používá tehdy, když je možné vysílači potvrdit správné/chybné přijetí zprávy a vyžádat nové vyslání dat. Tyto mechanizmy slouží k tomu, aby bylo možné říci, zda rámec byl přenesený dobře nebo špatně – nezjišťují počet a lokalizaci chyb.
- Korekce chyb (Error Correction) – k původní informaci se přidají informace, pomocí kterých je přijímač schopen poškozenou zprávu rekonstruovat. To se používá tehdy, když není možné vysílači potvrdit správné/chybné přijetí zprávy anebo by toto potvrzení bylo příliž časově náročné.

Metody detekce chyb

Používají se v případě, když je možné potvrzovat správné či chybné přijetí rámce. To je možné u poloduplexních a plně duplexních přenosů [1, 3, 4]. Základní metody detekce chyb jsou následující:

- Parita – jedná se o nejjednodušší mechanizmus, který však není příliž spolehlivý. Přenášený znak nebo blok dat se doplní o paritní bit, který se nastaví tak, aby celkový počet bitů ve znaku byl sudý (sudá parita, even parity) nebo lichý (lichá parita, odd parity). Pokud počet jedniček neodpovídá paritě, jedná se o chybu. Parita se používá u znaků nebo rámců (příčná parita) nebo u stejnolehlých bitů všech znaků rámce (podélná parita).
- Kontrolní součet – mechanizmus funguje tak, že vysílač provádí během vysílání součet všech vyslených znaků a výsledek vloží na konec přenášeného rámce. Přijímač pak také počítá součet z přijímaných znaků a výsledek porovná s přijatým kontrolním součtem. Pokud se hodnoty shodují, předpokládá se, zpráva byla přijata správně (přestože existuje určitá pravděpodobnost, že chybymají takový charakter, že se to na výsledku součtu neprojeví).

- CRC kódy (Cyclic Redundancy Code) – je v současné době nejpoužívanější a vyznačuje se velice dobrou účinností detekce chyby (99.99999998%). Principiálně funguje jako kontrolní součet, nicméně liší se v mechanizmu výpočtu přidané informace na konec rámce. Princip výpočtu kódu je popsán například zde [1, 4].
- Kromě těchto základních metod existují ještě doplňkové metody, jako například různé kontroly formátu zpráv apod.

Metody korekce chyb

Používají se v případě, když není možné vysílači potvrdit správné/chybné přijetí zprávy anebo by toto potvrzení bylo příliž časově náročné. To nastává zejména u simplexních přenosů nebo v případech, kdy doba přenosu signálu od vysílače k přijímači je dlouhá (například u satelitních přenosů). Korekce chyb funguje tak, že se s původními údaji přenáší i nadbytečná informace, která umožní rekonstruovat poškozenou zprávu. Potřebné redundantní údaje tvoří obyčejně 10-20% délky původního bloku. Tytomechanizmy se označují jako samoopravné kódy (nejčastěji jsou v této roli používány tzv. Hammingovy kódy).

4.3. Potvrzování, řízení toku dat

Potvrzování se používá u komunikačních systémů, kde se provádí detekce chyby. Jedná se o informování vysílače o tom, že přijímač přijal zprávu v pořádku nebo s chybou [1, 2, 3]. Způsoby potvrzování je možné rozdělit na dvě skupiny:

- Jednotlivé potvrzování – potvrzení se provádí po každém rámci, vysílač pokračuje ve vysílání až po potvrzení přijetí. Některé metody jsou založeny na potvrzování správně přijatého rámce (pozitivní potvrzování), některé na potvrzování chybně přijatého rámce (negativní potvrzování). Existují rovněž kombinace těchto dvou možností. Nevýhodou jednotlivého potvrzování je nutnost čekat na reakci protistrany.
- Průběžné potvrzování - používá se u delších dob přenosu. Vysílač vysílá nové rámce bez čekání na potvrzení. Potvrzení přichází opožděně a reaguje se na ně až v okamžiku, až když skutečně přijde.

Řízení toku dat je mechanizmus, který zajistí, aby přijímač nebyl zahlcen daty od vysílače. Linková vrstva zajišťuje, aby vysílač vysílal jen tehdy, kdy je přijímač schopen přijímat. Obvykle se pozastavuje vysílání nového rámce, pokud přijímač není připraven přijímat data. V případě jednotlivého potvrzování se čeká na potvrzení, že přijímač přijal poslední vyslaný rámec.

U kontinuálního potvrzování může vysílající vysílat dopředu bez potvrzení jen určitý maximální počet rámců.

4.4. Přístup ke komunikačnímu médiu

Pokud přistupuje k přenosovému kanálu více zařízení, je nutné zajistit, aby se jednotlivá zařízení při vysílání dat navzájem neovlivňovaly. Principiálně se řeší rozdělení přenosové kanálu pomocí časového a frekvenčního multiplexování, které byly popsány v kapitole 3. U průmyslových komunikačních sítí a lokálních sítí se používá prakticky výhradně časové multiplexování. Pak je přístupem ke komunikačnímu médiu myšlen mechanizmus, který určuje, které zařízení ve kterém okamžiku má k přenosovému kanálu přístup.

U komunikace dvou zařízení tento problém nenastává, jelikož obě zařízení mají pro vysílání svých dat samostatný vodič. U vícebodových spojů však je nutné zajistit, aby v jednom okamžiku vysílalo jen jedno zařízení. U vícebodových spojů jsou možné následující režimy:

- Jedno zařízení vysílá a jedno přijímá (unicast)

- Jedno zařízení vysílá a všechna ostatní přijímají (broadcast)
- Jedno zařízení vysílá a jen některá přijímají (multicast)

Metody přístupu na médium lze rozdělit na dvě základní skupiny:

- Deterministický přístup ke sdílenému médiu.
  - Centralizované řízení.
  - Distribuované řízení.
- Náhodný přístup ke sdílenému médiu.

Deterministický přístup ke sdílenému médiu

Jedná se způsob, kdy existuje jasný postup pro přidělování práva vysílat a lze jednoznačně určit, kdy bude mít kterékoliv zařízení možnost vyslat svá data [1, 3]. Mezi nejznámější patří tyto metody:

- Metoda centrálního arbitra – jedna stanice na síti je hlavní (arbitr), který přiděluje právo vysílat na základě požadavků ostatních stanic. Pro požadavky je třeba vyhradit určitý prostor, což snižuje přenosovou kapacitu pro vlastní přenos dat.
- Metoda výzvy – hlavní stanice sama cyklicky vyzývá ostatní stanice (poll), aby vyslaly svá data. Tento systém je použit u celé řady současných průmyslových sběrnic.

Hlavní stanice se u těchto systémů označuje jako centrální arbitr či master, ostatní stanice jako podřízené nebo slavy. Jakmile podřízená stanice dostane právo vysílat, může odeslat data masteru, jinému slavu nebo několika zařízením – to závisí na konkrétní implementaci v příslušném komunikačním systému. Značná nevýhoda těchto metod je v tom, že pokud přestane fungovat centrální arbitr, havaruje celá komunikace.

Existují však i jiné metody přístupu na komunikační médium, které nevyžadují existenci centrálního arbitra. Tyto metody obsahují mechanizmus, kdy žadatelé se mezi sebou dokážou dohodnout, kdo bude vysílat - decentralizovaný způsob řízení mnohobodového spojení. Může se jednat o metody s deterministickým nebo náhodným přístupem ke komunikačnímu médiu.

Příkladem deterministické metody přístupu ke komunikačnímu médiu s decentralizovaným způsobem řízení je metoda logického kruhu (Token Passing), která je využita například u lokálních sítí dle IEEE 802.4 nebo také jako jedna z metod u sběrnice Profibus DP. Jednotlivé stanice si předávají pověření vysílat a tvoří tak určitý „logický kruh“. Předpokladem je, že stanice sdílející přenosový kanál jsou označeny adresami a tyto adresy tvoří cyklickou posloupnost. Každá ze stanic zná svou vlastní adresu a adresu stanice, která smí vysílat po ní. Systém má rovněž mechanizmus pro start komunikace a pro případ výpadku některé ze stanic.

Náhodný přístup ke sdílenému médiu

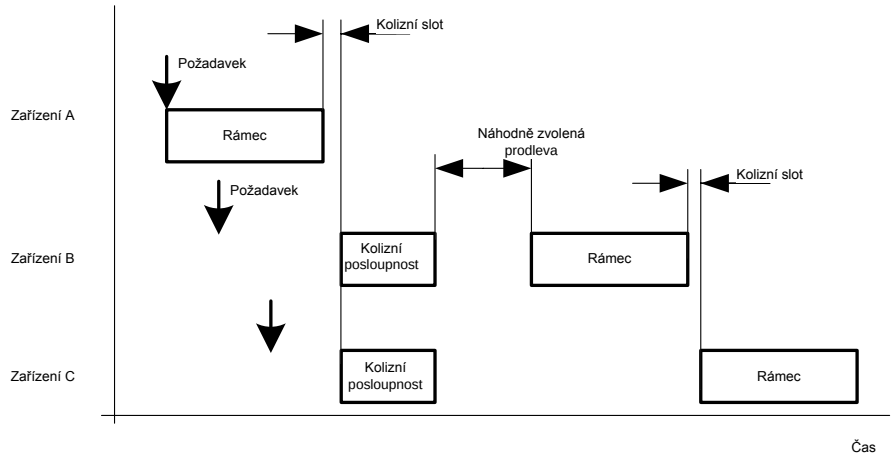
U těchto metod není dáno pořadí stanic, které budou vysílat. Všechny stanice jsou rovnocenné a mají právo zahájit vysílání dat prakticky kdykoliv. Tyto typy metod přístupu na komunikační médium jsou nejrozšířenější v dnešních lokálních sítích.

Prvními metodami založenými na tomto principu byly metody Aloha, které umožňovaly vyslat data jednotlivým stanicím kdykoliv. Velkou slabinou byl fakt, že stanice neodposlouchávaly provoz na síti a proto často docházelo ke kolizím (situacím, kdy dvě nebo více stanic vysílalo současně). Dnes se tyto metody již nepoužívají.

Mezi nejznámější metody náhodného přístupu ke komunikačnímu médiu patří v současné době skupina metod CSMA (Carrier Sense Multiple Access). Společným znakem těchto metod je fakt, že zařízení poslouchají provoz na síti předtím, než chtějí začít vysílat (Carrier Sense - naslouchání nosné). To brání tomu, aby zařízení začalo vysílat v okamžiku, kdy vysílá někdo jiný. Další

společnou vlastností je to, že se jedná o metodu určenou pro komunikaci více zařízení (Multiple Access - vícenásobný přístup). Mezi nejznámější verze tohoto systému patří [1, 5]:

- Čisté CSMA, naléhající CSMA, nenaléhající CSMA – u těchto variant se brání kolizím pouze tím, že zařízení odposlouchávají nosnou. Pokud dvě zařízení začnou vysílat v tomtéž čase, vzhledem ke konečné rychlosti šíření signálu médiem a času nutnému pro zpracování odposlouchávaných informací, dojde ke kolizi. Tu zařízení detekují pouze pomocí metod detekce chyb, jelikož kolize způsobí poškození vysílaných rámců. Zařízení pak opakují vysílání podle zvoleného mechanizmu (po náhodně zvolené době). Naléhající CSMA a nenaléhající CSMA se liší mechanizmem, kdy začínají vysílat svá data a v reakci po kolizi (naléhající CSMA začíná vysílat ihned po uvolnění kanálu, nenaléhající CSMA začíná vysílat po náhodně zvolené době od neúspěšného pokusu o zahájení vysílání apod.)
- CSMA/CD – jedná se patrně o nejznámější metodu, jelikož ji využívá například komunikační systém Ethernet. Od výše uvedených metod se liší zejména tím, že dokáže detekovat kolizi již v průběhu vysílání (Collision Detection) a dokáže vysílání přerušit. Pokud stanice vstoupila do kolize a tuto skutečnost rozpoznala, přeruší vysílání rámce. Před uvolněním média odešle kolizní posloupnost (jam). Tato posloupnost zajistí, že kolizi rozpoznají všechny kolidující stanice. O nové odeslání dat se stanice pokusí až náhodně zvolené době. Náhodná volba prodlevy brání periodickému opakování kolize. Volba prodlevy je důležitá, jelikož v určitých případech by mohla nastat situace periodického opakování kolizí a zablokování provozu na síti. Jelikož stanice sledují provoz na síti a nezahájí vysílání, pokud je síť obsazena, může dojít ke kolizi pouze v okamžiku, kdy zařízení začnou vysílat téměř současně, tzn. do doby, než signál od jednoho zařízení ještě neobsadil celé médium. Tato doba se označuje jako kolizní okénko. Jeho velikost je dána délkou média a zpožděními na aktivních prvcích sítě. Aby CSMA/CD mohlo fungovat, musí být kolizní okénko kratší, než je doba vysílání nejkratšího rámce (jinak by mohlo docházet k nezjištěným kolizím). Z toho vyplývá, že rámec nesmí být příliš krátký, maximální délka média a počet opakovačů jsou omezeny, zvýšení přenosové rychlosti vede ke zkrácení kolizního okénka a tedy zpravidla zkrácení maximální délky média.
- CSMA/CA – tato modifikace dokáže minimalizovat vznik kolizí (Collision Avoidance). Je založena na přímém CSMA. Obsahuje mechanizmus, který zabraňuje vysílání v okamžiku, kdy je největší pravděpodobnost kolize. Každé zařízení před začátkem vysílání určitý čas poslouchá, zda je přenosové médium volné. Pokud ano, zahájí vysílání. V opačném případě čeká na konec právě probíhajícího vysílání. CSMA/CA se využívá především v bezdrátových sítích, protože účastníci bezdrátového přenosu nejsou schopni zároveň vysílat a přijímat. Tato metoda navzdory svému označení nedokáže plně kolizím zabránit.
- CSMA/CD w/ AMP (with Arbitration on Message Priority). Jedná se o metodu náhodného přístupu ke komunikačnímu médiu, kde všechna zařízení mohou kdykoliv začít vysílat svá data, ale vzniku případných kolizí je zde zabráněno pomocí systému priorit zpráv. Metoda je použita u sběrnice CAN.
- Aj.



Obr. 4.7 Metoda CSMA/CD.

Shrnutí pojmů

Linková vrstva zajišťuje následující funkce:

- Zajišťuje bezchybný přenos bloků dat mezi dvěma zařízeními.
- Rozpoznává začátek a konec rámce a jeho jednotlivé části – fyzická vrstva pouze přenáší jednotlivé bity, neinterpretuje jejich význam. To je úlohou linkové vrstvy, která musí rozpoznat řidicí informace v rámci a užitečná data.
- Zajišťuje **přístup ke komunikačnímu médiu** (Media Access Control)
- **Řízení toku dat**, synchronizaci na úrovni rámců.
- **Detekci** nebo **korekci chyb.**

Metody přístupu na médium lze rozdělit na dvě základní skupiny:

- Deterministický přístup ke sdílenému médiu.
  - Centralizované řízení.
  - Distribuované řízení.
- Náhodný přístup ke sdílenému médiu.

Otázky

1. Popište funkce linkové vrstvy.
2. Popište asynchronní sériový přenos bloku dat.
3. Popište synchronní sériový přenos bloku dat.
4. Jaké jsou metody synchronního sériového přenosu bloku dat.
5. Popište metody detekce a korekce chyb.
6. Popište metody potvrzování.

7. Popište metody řízení toku dat.
8. Jaké existují metody přístupu na komunikační médium?
9. Popište deterministické metody přístupu ke sdílenému médiu.
10. Popište metody náhodného přístupu ke sdílenému médiu.
11. Popište metody CSMA.

Další zdroje

1. Kováč F. Distribuované riadiace systémy. Vydavatelstvo STU, Bratislava 1998. ISBN 80-227-1082-2.
2. Báječný svět počítačových sítí, část IX. - Zajištění spolehlivosti. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/b05/b1200001.php3
3. Linková vrstva - I. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a92/a218c110.php3
4. Zabezpečení dat při přenosech. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a91/a141c110.php3
5. Počítačové sítě. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/l218/index.php3

Řešená úloha 4.1

Zadání: Práce na projektu č.1.

Předmětem cvičení je práce na malém projektu č. 1. Zadání projektu se týká komunikace po sběrnici AS-i s PLC S7 200 nebo s PLC S7 300 podle vybraného zadání.

Projekty v předmětu Distribuované systémy řízení

V rámci předmětu studenti řeší tři úlohy:

Program č. 1 (10b.)

Program č. 2 (10b.)

Hlavní program (20b.)

Program č.1 a 2 mohou řešit ve dvojicích, hlavní program samostatně. Termín odevzdání programů bude stanoven na cvičeních. Ke každému programu bude vypracován protokol a program bude prakticky předveden. Pro realizaci programů budou studenti používat laboratorní modely. Jejich připojování k PLC se bude provádět výhradně pomocí instalovaných konektorů a prodlužovacích kabelů. Zapojení všech přípravků a modelů je k dispozici v laboratoři.

Protokol musí obsahovat tyto základní části – zadání, seznamy vstupů a výstupů, stručnou systémovou analýzu, schéma struktury řídicího systému, algoritmy řešení, komentovaný výpis programu.

Program č. 1 – AS Interface + S7 200 nebo S7 300

1. Řízení přechodu pro chodce.
2. Cyklické zapínání výstupních bitů AS-i slave.
3. Zobrazování hodnot 0-F na sedmi-segmentovém displeji.
4. Řízení přechodu pro chodce s využitím S7 300 a DP/AS-i Linku.
5. Cyklické zapínání výstupních bitů AS-i slave s využitím S7 300 a DP/AS-i Linku.

Program č. 2 – Profibus

1. Vytvoření hexa počítadla pomocí S7 314C-2 DP a ET200M.
2. Zápis hodnoty ze simulačních vstupů na displej S7 314C-2 DP a ET200M.
3. Řízení soustavy se žárovkou pomocí S7 315-2 DP a ET200M.
4. Řízení pohybu výtahu na dvě patra pomocí PLC Simatic S7 314C-2 DP a ET200M.
5. Řízení světelné křižovatky pomocí PLC Simatic S7 314C-2 DP a ET200M.

Hlavní programy

1. Řízení modelu křižovatky pomocí PLC B&R a průmyslové sítě Ethernet Powerlink.
2. Komunikace PLC S7 200 přes GSM modem (zasílání a příjem SMS zpráv) (2 lidi).
3. Komunikace PLC S7 300 přes GSM modem (zasílání a příjem SMS zpráv) (2 lidi).
4. Distribuovaná řídicí aplikace s PLC S7 300, distribuovanou periferií ET 200M a frekvenčním měničem Micromaster.
5. Distribuovaná řídicí aplikace pro model výtahu s PLC S7 200 a AS-i.
6. Vytvoření internetového vizualizačního a informačního rozhraní pro S7 200 pomocí CP 243-1 IT pro laboratorní model přechodu pro chodce.
7. Vytvoření internetového vizualizačního a informačního rozhraní pro S7 300 pomocí CP 343-1 IT pro laboratorní model regulační soustavy.
8. Vytvoření internetového vizualizačního a informačního rozhraní pro B&R pro laboratorní model regulační soustavy se žárovkou s využitím VNC serveru.
9. Komunikace mezi třemi PLC Simatic S7 300 přes síť Industrial Ethernet.
10. Vytvoření demonstrační řídicí aplikace využívající sběrnici AS-i s DP/AS-i Linkem a s připojeným systémem LOGO!.
11. Vytvoření distribuované aplikace se dvěma PLC B&R System 2003 a Powerpanelem PP120.
12. Vytvoření distribuované řídicí aplikace, kde bude propojen systém LOGO, sada vypínačů, světlo propojeno pomocí sběrnice EIB/KNX a DP/EIB Linku k S7 300.
13. Komunikace PLC S7 200 a S7 300 přes Ethernet.
14. Vytvoření distribuované řídicí aplikace využívající síť MPI, kde budou dva programovatelné automaty S7 300 a operátorský panel TP177A. K jednomu automatu bude navíc připojena periferie ET 200M pomocí sítě Profibus DP. Na periferii bude připojen model křižovatky, na obou automatech budou simulační I/O, které budou ovlivňovat průběh řízení křižovatky. Na TP bude vizualizace procesu.
15. Vytvořte řídicí aplikaci s programovatelným automatem S7 300, který bude řídit zvolený laboratorní model. Automat bude vysílat e-maily dvěma operátorům, které budou obsahovat informace o řízení a stavech procesu.
16. Vytvořte řídicí aplikaci s programovatelným automatem S7 300, který bude řídit zvolený laboratorní model. Automat bude ukládat na FTP server umístěném na počítači typu PC datové soubory, které budou obsahovat informace o řízení a stavech procesu.
17. Vytvoření distribuované řídicí aplikace s PLC Rockwell Automation CompactLogix, vzdálenou periferií a frekvenčním měničem vzájemně propojených sítí Ethernet (2 studenti).
18. Vytvoření větve sběrnice AS-i s využitím AS-isafe.
19. Inovace dvou větví AS Interface v učebně a vytvoření demonstračních úloh.

5. VRSTVY 3-7 ISO-OSI MODELU, SÍŤOVÝ MODEL TCP/IP

Čas ke studiu: 3 hodiny

Cíl Po prostudování této kapitoly budete umět

- Popsat vlastnosti vrstev 3-7 ISO OSI modelu.
- Popsat síťový model TCP/IP.
- Popsat topologie komunikačních sítí.
- V praktické části se naučíte vytvořit jednoduchou řídicí aplikaci pro programovatelný automat Simatic S7 300 s využitím komunikační sběrnice Profibus DP.

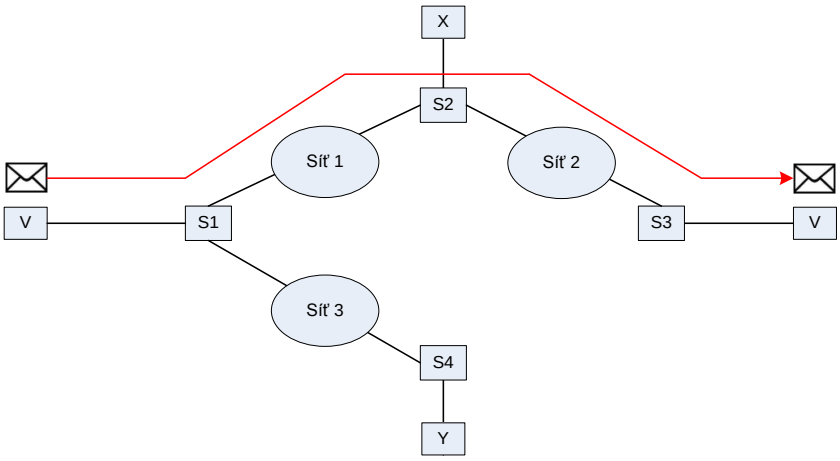
Výklad

Fyzická a linková vrstva mají zásadní význam u všech komunikačních systémů. U řady z nich jsou jedinými vrstvami, které jsou využity. Týká se to systémů, kde existuje přímé spojení mezi jednotlivými účastníky přenosu a kde se přenášejí data s jednoduchou strukturou. Těmito vlastnostmi se obvykle vyznačují průmyslové komunikační systému používané na nejnižších úrovních pro řízení v reálném čase (Actuator Sensor Level a Field Level).

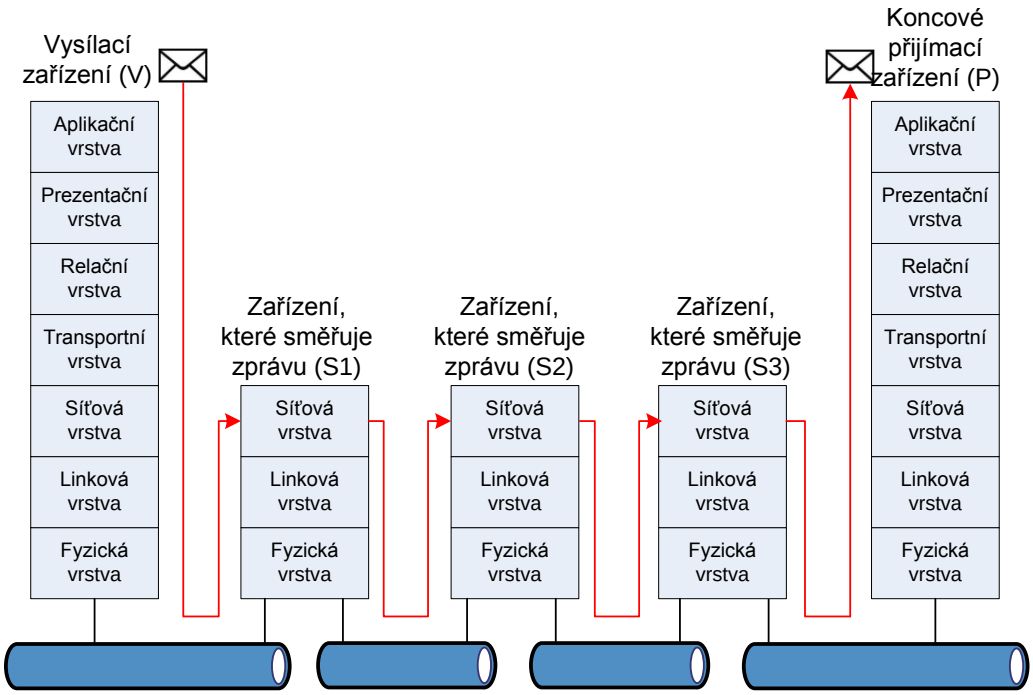
U systémů, které mají složitější topologii sítě a mezi účastníky neexistuje přímé spojení, je nezbytné využití i síťové vrstvy. Ta zná topologii sítě a dokáže dopravit zprávu k cíli. Transportní vrstva se pak zabývá pouze tím, že odesílá zprávu od vysílače ke koncovému příjemci, aniž by řešila, jakou cestou zpráva půjde. V těchto případech linková vrstva nemá představu, kdo je koncovým příjemce zprávy, stará se pouze o přenos zprávy do jiného uzlu sítě, se kterým má bezprostřední spojení [1, 2].

5.1. Síťová vrstva

Komunikační systémy, u kterých je použitá složitější topologie, kdy neexistuje přímé spojení mezi jednotlivými účastníky přenosu, přenos probíhá přes zařízení, které leží „na cestě“ mezi vysílacím zařízením a koncovým příjemcem datm. Může existovat několik cest, jak přenést zprávu. A právě o zajištění tohoto přenosu a výběr vhodné cesty se stará síťová vrstva.
Zařízení, které se nachází na cestě mezi vysílačem a koncovým nemusí být nutně plnohodnotným uzlem sítě, může to být zařízení, jehož účelem je propojování sítí a předávání zpráv mezi jednotlivými částmi sítě. Princip průchodu zprávy komunikační sítí s komplexní topologií je znázorněn na obrázcích 5.1 a 5.2.



Obr. 5.1 Průchod zprávy sítí.



Obr. 5.2 Průchod zprávy sítí.

Základním úkolem síťové vrstvy je tedy směřování (volba cesty) bloku dat (packetu) vysla-ného odesílatele topologií sítě ke koncovému příjemci. Směřování se označuje anglickým slovem routing a od toho je odvozeno označení zařízení, které se ke směřování používá, což je router.

Pokud se nachází odesílatel i příjemce v jedné síti (tzn. mají vzájemné přímé spojení), jedná se o přímý přenost packetu. To, co se označuje pojmem směřování (routing), je nepřímý přenos packetu, který nastává v případě, že nejsou odesílatel i příjemce v jedné síti.

Směřování se účastní směřovače a koncová zařízení (odesílající zařízení). Odesílající zařízení musí rozhodnout, zda je koncový příjemce packetu v dané síti, nebo zda zprávu odešle přes vhodný směřovač. Aby toto mohlo fungovat, mělo by každé koncové zařízení znát adresu výchozího směřovače (výchozí brány), kterou použije, pokud se příjemce nachází v jiné síti.

Směřovače uchovávají informace potřebné ke směřování v tzv. směřovacích tabulkách. Tabulky obsahují informace o tom, jak je cílová síť daleko a kudy je třeba paket předat, aby se dostal blíže k cílové síti.

Tabulky pro směřovače se sestavují dvěma základními způsoby [1, 2]:

- Pomocí neadaptivních algoritmů – obsah tabulky je pevně dán a nepřizpůsobuje se provozu sítě (například při přidání nového zařízení do sítě se tabulka automaticky neaktulizuje). Obsah tabulky může měnit například správce sítě. Tento způsob je odolný proti ovlivňování zvenčí a nemá režii nutnou pro aktualizaci tabulky.
- Pomocí adaptivních algoritmů – obsah tabulky se za provozu průběžně aktualizuje a odráží tak aktuální topologii sítí a reaguje na její změny. Aktualizace tabulky znamená určitou časovou zátěž (režii).

Směřování se dá dále rozdělit na následující typy [1, 2]:

- Centralizované směřování – rozhodování o volbě nejvhodnější cesty provádí centrální prvek (route server).
- Izolované směřování – jednotlivé směřovače samy rozhodují o volbě cesty.
- Distribuované směřování – kombinace předchozích. Rozhodování je rozděleno (distribuováno) mezi jednotlivé uzly, které na něm spolupracují.

5.2. Transportní vrstva

Transportní vrstva řeší koncové řízení komunikace (tj. mezi původním odesílatelem a konečným příjemcem). Je rozhraním mezi aplikačním softwarem a externí sítí. Poskytuje transparentní, spolehlivý přenos dat s požadovanou kvalitou. Tento přenos dat může mít charakter spojované nebo nespojované služby.

Vrstvy 1-3 jsou „hardwarově orientované“, kdy se starají o vlastní přenos dat – jsou poskytovateli přenosových služeb. Vrstvy 5-7 jsou spíše „softwarově nebo aplikačně orientované“, kde zajišťují práci s přenášenými daty a jsou uživateli přenosových služeb.

Transportní vrstva je tedy rozhraním mezi těmito skupinami vrstev.

Transportní vrstva, jak je patrné z obrázku 5.2 je přítomná jen v koncových uzlech, nikoliv však v zařízeních, která směřují packety na komunikační cestě. Transportní spojení je pak komunikační spojení dvou koncových zařízení, které je realizováno pomocí jednoho nebo více síťových spojení (v rámci jednoho transportního spojení mohou packety procházet ke koncovému zařízení různými cestami, tzn. různými síťovými spojeními).

Transportní vrstva při odesílání dat vytváří jednotlivé pakety, do kterých rozděluje přenášené údaje a při přijímání je zase skládá do původního tvaru. Tyto packety mohou být přenášeny pomocí různých síťových spojení. Dokáže zajistit přenos libovolně velkých zpráv, i když jednotlivé pakety mají jen omezenou velikost. [1, 3]

5.3. Relační vrstva

ISO OSI model definuje nad transportní vrstvou další tři vrstvy – relační, prezentační a aplikační. Model TCP/IP však má nad transportní vrstvou přímo aplikační vrstvu, relační a prezentační vynechává. Jedním z důvodů může být i to, že v celé řadě aplikací služby těchto vrstev nejsou využívány a proto není nutné je vždy implementovat.

Základním úkolem relační vrstvy dle ISO OSI modelu je usnadnění a podpora vzájemné interakce (relace) mezi komunikujícími stranami. Dále se vrstva zabývá zajištěním bezpečnosti takovéto relace, synchronizací komunikujících stran (ve smyslu obnovy spojení po výpadku, zahájení přenosu od bodu před výpadkem apod.).

Samostatná relační vrstva, jak již bylo naznačeno výše, se u současných komunikačních systémů objevuje jen velmi zřídka. [1, 4]

5.4. Prezentační vrstva

Úlohou prezentační vrstvy je konverze dat takovým způsobem, aby data měla stejný význam pro obě komunikující strany. Formát dat se v komunikujících systémech může lišit a také je někdy nutné upravit formát dat pro účely přenosu. Příkladem činností prezentační vrstvy jsou převody kódů (ASCII, EBCDIC, Unicode apod.) a znakových sad, modifikace grafického uspořádání, přizpůsobení pořadí bajtů, formátu čísel, komprese dat, šifrování apod. Vrstva se zabývá jen strukturou dat, ale ne jejich významem, který je znám jen vrstvě aplikační.

Prezentační vrstva stejně jako relační nefiguruje jako samostatná vrstva v modelu TCP/IP. Zde se předpokládá, že pokud aplikace potřebují funkčnost původně poskytovanou těmito vrstvami, zajistí si ji samy případně případně s využitím „pseudovrstev“. [1, 4]

5.5. Aplikační vrstva

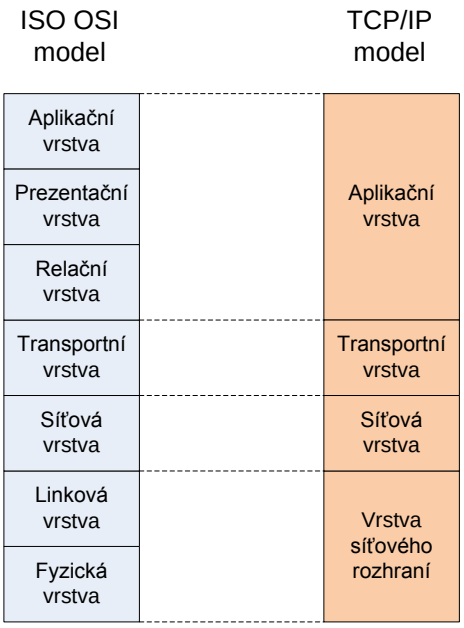
Aplikační vrstva představuje rozhraní mezi komunikačním kanálem a koncovou aplikací, která vyžaduje komunikaci. Tzn., že aplikační vrstva neobsahuje vlastní aplikace, ale pouze části aplikací, které řeší všeobecně použitelné mechanizmy.

Pokud hovoříme o aplikaci pro elektronickou poštu, obsahuje aplikační vrstva část, které zajišťuje předávání zpráv, formátování zpráv, jednotný styl adres apod. Uživatelské rozhraní pro práci s elektronickou poštou je pak součástí konkrétní aplikace. [1, 4]

5.6. Síťový model TCP/IP

Pod pojmem TCP/IP se obvykle chápe soustava protokolů pro komunikaci v počítačových sítích (nikoliv pouze protokoly TCP a IP). Dá se říci, že se jedná o síťový model srovnatelný s ISO OSI modelem [1, 5]. Základními rozdíly mezi oběma modely jsou:

- Síťový model TCP/IP definuje jen 4 vrstvy (viz. obr. 5.3).
- Síťový model TCP/IP je založen spíše na nespojovaných službách, zatímco ISO OSI model spíše na spojovaných a spolehlivých službách.



Obr. 5.3 ISO OSI x TCP/IP model.

Vrstva síťového rozhraní (Network Interface Layer, Link Layer)

Má na starosti vlastní přenos dat komunikačním médiem, vysílání, příjem packetů. Dle typu komunikačního systému se může jednat o jednoduché rozhraní, ale také složitý subsystém s vlastním linkovým přenosovým protokolem. Při srovnání ISO OSI a TCP/IP model se obvykle uvádí, že vrstva síťového rozhraní pokrývá linkovou a fyzickou vrstvu ISO OSI. Někdy se také uvádí hardwarová úroveň až pod vrstvou síťového rozhraní. [1, 5]

V současné době jsou nečasteji používanými systémy pro vrstvu síťového rozhraní Ethernet, Token Ring, FDDI, apod.

Síťová vrstva (Internet Layer, IP Layer)

Tato vrstva se označuje jako Internet Layer a základním protokolem, který se zde používá je IP (Internet Protocol). Základním úkolem této vrstvy je směřování packetu od vysílače ke koncovému příjemci dat, tzn. stejný význam, jaké má síťová vrstva u ISO OSI modelu. Vzhledem k nespojovanému charakteru přenosů v TCP/IP je na úrovni této vrstvy zajišťována jednoduchá (tj. nespolehlivá) datagramová služba. [1, 5]

Dalšími protokoly, které se v současné době nečasteji používají v síťové vrstvě jsou ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) aj.

Transportní vrstva (Transport Layer)

Jejím úkolem je zajistik komunikaci mezi dvěma koncovými zařízeními. Může ovlivňovat tok dat oběma směry, zajišťovat spolehlivost přenosu a také měnit nespojovaný charakter přenosu (v síťové vrstvě) na spojovaný. Odpovídá svým účelem transportní vrstvě v ISO OSI modelu. [1, 5]

Dominantními protokoly na této vrstvě jsou:

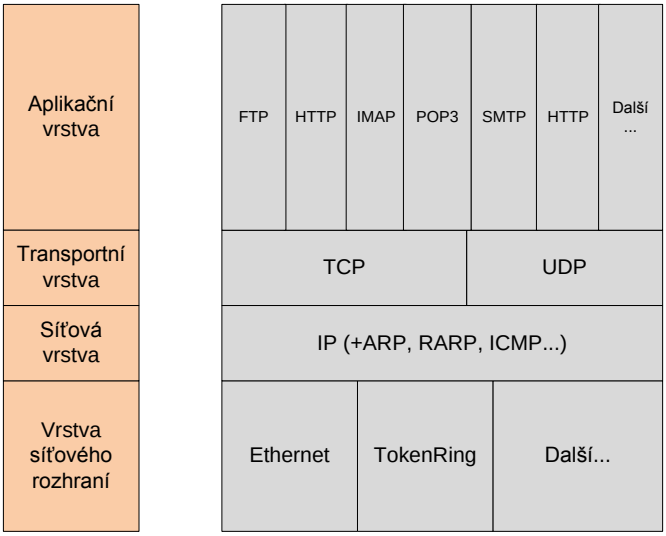
- TCP (Transmission Control Protocol) - spojově orientovaný protokol pro přenos toku bajtů na transportní vrstvě se spolehlivým doručováním.
- UDP (User Datagram Protocol) - protokol založený na odesílání nezávislých zpráv. Nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů nebo zda se některý datagram nedoručí vícekrát.

Dalšími protokoly jsou DCCP (Datagram Congestion Control Protocol), SCTP (Stream Control Transmission Protocol), aj.

Aplikační vrstva

Je nejvyšší vrstvou TCP/IP modelu. Poskytuje aplikačním programům přístup ke komunikačnímu systému. [1, 5] Používá se zde celá řada protokolů, jako např:

- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- POP3 (Post Office Protocol, version3)
- SMTP (Simple Mail Transfer Protocol)

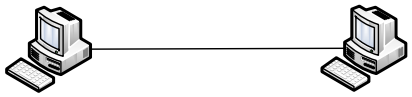


Obr. 5.4 Struktura TCP/IP modelu.

5.7. Topologie sítí

Dvoubodový spoj

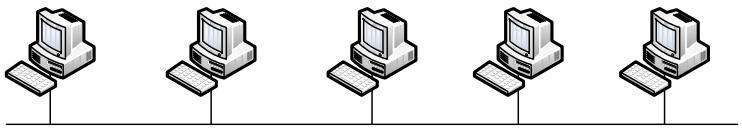
Je základní topolodií, jedná se o přímé spojení mezi mezi dvěma koncovými zařízeními.



Obr. 5.5 Dvoubodový spoj.

Sběrnicová topologie

Toplogie, kdy komunikační médium propojuje všechny uzly sítě. Má liniovou strukturu. Má nízké pořizovací náklady a je jednoduchá. Nedělí síť na kolizní domény, takže v ní může docházet ke kolizím. Ve většině aplikací vyžaduje méně kabeláže, než ostatní topologie. Snadno se rozšiřuje. Je vhodná spíše pro menší sítě s omezeným počtem zařízení. Je často používaná v průmyslových aplikacích.

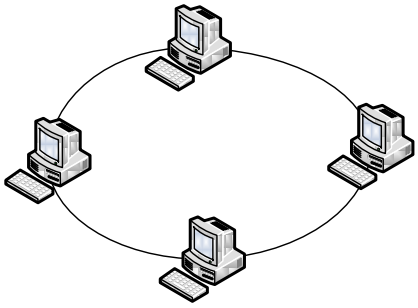


Obr. 5.6 Sběrnicová topologie.

Kruhová topologie

Topologie kdy je každé zařízení spojeno se dvěma dalšími tak, aby společně vytvořily kruh. Přenos dat je relativně jednoduchý, nevznikají kolize. Určitou nevýhodou je to, že data musí projít přes mnoho uzlů než se dostanou ke svému cíli. Přenos dat probíhá jedním směrem. Výpadek jednoho uzlu ochromí celou síť. Při výpadku jednoho uzlu je v některých případech možné využít cestu

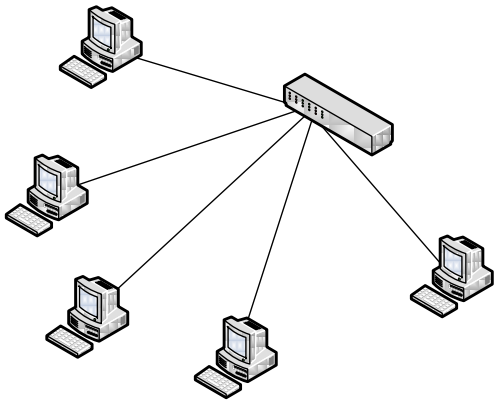
druhým směrem (redundantní cesta), zařízení však musí tuto možnost podporovat (obvykle probíhá přenos jedním směrem).



Obr. 5.7 Kruhová topologie.

Hvězdicová topologie

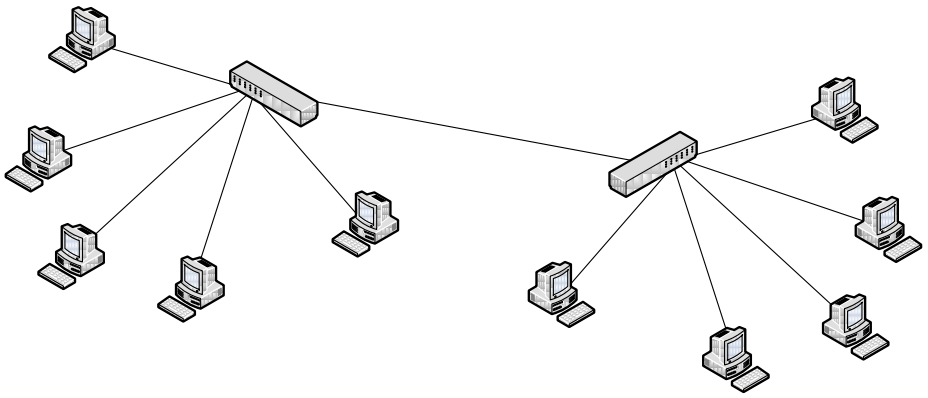
V současnosti často používaná topologie u počítačových sítí. Každý počítač je připojený pomocí kabelu k centrálnímu prvku - hubu nebo switchi. Mezi každými dvěma stanicemi existuje vždy jen jedna cesta. Selhání jedné stanice neomezí provoz sítě. Porucha centrálního uzlu způsobí výpadek celé sítě. Pokud je centrální zařízení switch, nedochází ke kolizím. Snadno se rozšiřuje. Nevýhodou je, že vyžaduje rozsáhlejší kabeláž, nutnost použití centrálních prvků (huby, switche).



Obr. 5.8 Hvězdicová topologie.

Stromová topologie

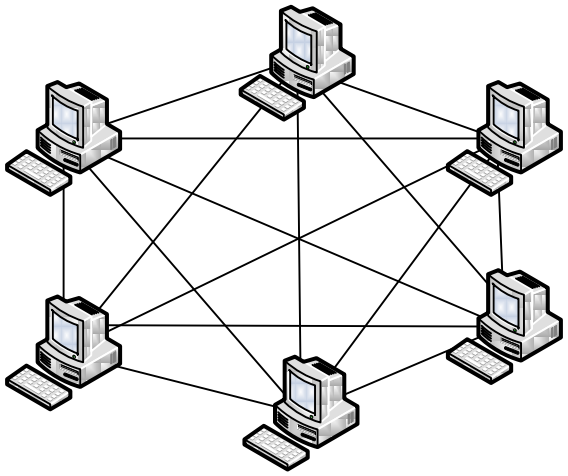
Používá se u rozsáhlejších počítačových sítí. Jedná se prakticky o propojení několika sítí s hvězdicovou topologií. Výhody a nevýhody jsou obdobné, jako u hvězdicové topologie.



Obr. 5.9 Stromová topologie.

Mesh topologie

Toplogie, kde každé zařízení je propojeno s každým. Může být plně nebo částečně propojená. Umožňuje rekonfigurovatelnost při výpadcích. Obvykle se používá u bezdrátových komunikačních systémů.



Obr. 5.10 Mesh topologie.

Shrnutí pojmů

Základním úkolem **síťové vrstvy** je tedy směřování (volba cesty) bloku dat (packetu) vyslaného odesílatele topologií sítě ke koncovému příjemci. Směřování se označuje anglickým slovem routing a od toho je odvozeno označení zařízení, které se ke směřování používá, což je **router.**

Transportní vrstva řeší koncové řízení komunikace (tj. mezi původním odesílatelem a konečným příjemcem). Je rozhraním mezi aplikačním softwarem a externí sítí. Poskytuje transparentní, spolehlivý přenos dat s požadovanou kvalitou.

Síťový model TCP/IP definuje následující vrstvy:

- Vrstva síťového rozhraní (Network Interface Layer, Link Layer)

- Síťová vrstva (Internet Layer, IP Layer)
- Transportní vrstva (Transport Layer)
- Aplikační vrstva

V distribuovaných systémech se používají zejména následující **topologie sítí**:

- Dvoubodový spoj
- Sběrnicová topologie
- Kruhová topologie
- Hvězdicová topologie
- Stromová topologie
- Mesh topologie

Otázky

1. Popište význam a funkce síťové vrstvy?
2. Popište význam a funkce transportní vrstvy?
3. Popište význam a funkce relační vrstvy?
4. Popište význam a funkce prezentační vrstvy?
5. Popište význam a funkce aplikační vrstvy?
6. Co je to model TCP/IP?
7. Popište vrstvu síťového rozhraní modelu TCP/IP.
8. Popište síťovou vrstvu modelu TCP/IP.
9. Popište transportní vrstvu modelu TCP/IP.
10. Popište aplikační vrstvu modelu TCP/IP.
11. Jaké topologie se používají v distribuovaných systémech?

Použitá literatura a další zdroje

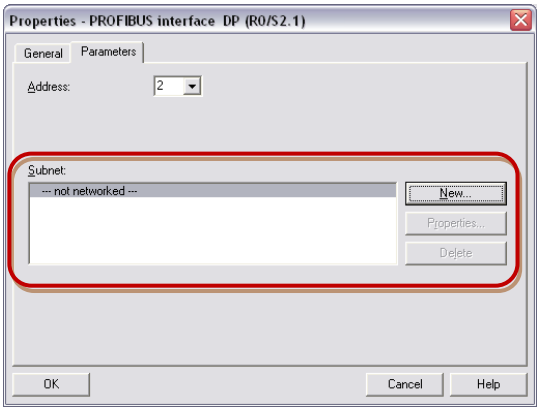
1. Kováč F. Distribuované riadiace systémy. Vydavatelstvo STU, Bratislava 1998. ISBN 80-227-1082-2.
2. Báječný svět počítačových sítí, část XI: Síťová vrstva a směrování. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/b06/b0200001.php3
3. Báječný svět počítačových sítí, část XII: Transportní vrstva. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/b06/b0300001.php3
4. Báječný svět počítačových sítí, část XIII: Aplikačně orientované vrstvy. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/b06/b0400101.php3
5. Síťový model TCP/IP. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a92/a231c110.php3

Řešená úloha 5.1

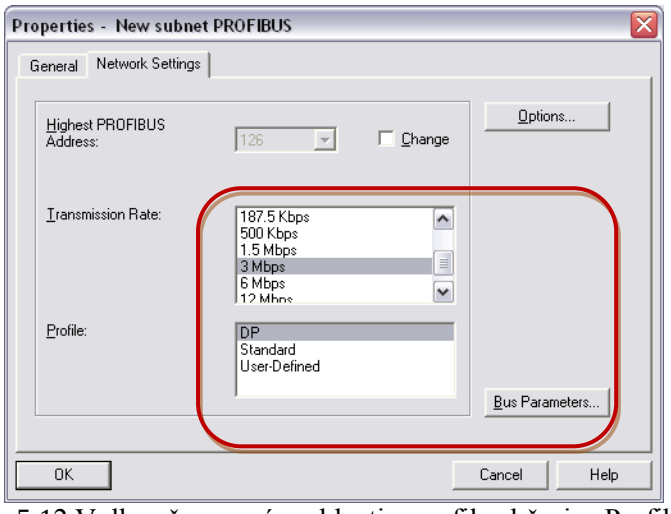
Zadání: Vytvořte hardwarovou konfiguraci PLC s CPU 314-2DP komunikující se vzdálenou periférií ET 200M (IM153-1) po sběrnici Profibus-DP. Adresa vzdálené periférie je 9 a obsahuje tyto rozšiřující karty: AI4/AO2 (6ES7 334-OKE0-0AB0), DI16 (6ES7 321-1BH01-0AA0), DO16 (6ES7 322-1BH01-0AA0).

Hardwarová konfigurace bude obsahovat PLC S7-300, CPU 314C-2DP (6ES7 314-6CF02-0AB0) a periférii ET 200M (IM153-1: 6ES7 153-1AA02-0XB0). CPU je umístěno ve složce CPU 300 a výběrem CPU 314C-2DP s objednacím číslem 6ES7 314-6CF02-0AB0 se vloží do slotu 2 připraveného racku. Bezprostředně po vložení se zobrazí okno s konfigurací sběrnice Profibus-DP.

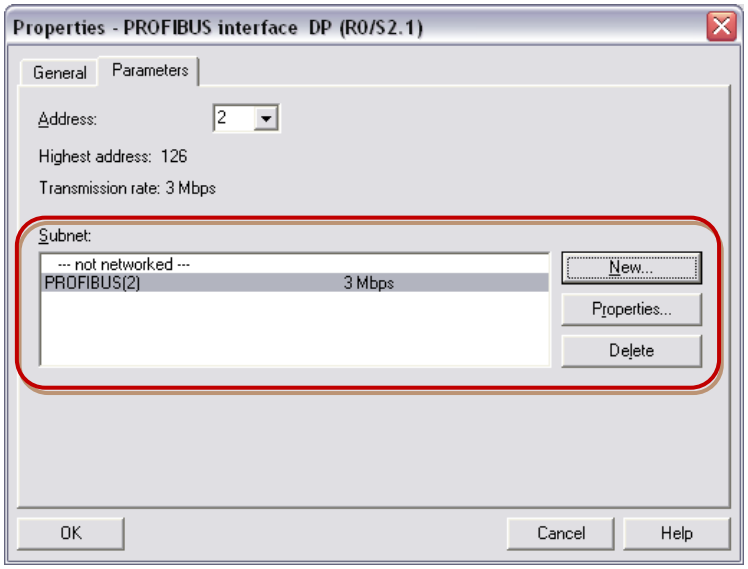
Adresa pro CPU je defaultně nastavena na 2. Kliknutím na tlačítko „New“ (obr. 5.11) se otevře okno s konfigurací sběrnice Profibus-DP. V okně „New subnet Profibus“ (obr. 5.12) v záložce „General“ lze zvolit přenosovou rychlost sběrnice (nastavíme 3Mbps) a profil (DP). Rychlost závisí na vzdálenosti periférii od CPU programovatelného automatu. Navíc pokud se v místě vedení trasy komunikační sběrnice vyskytuje rušení, měla by být rychlost pro větší přesnost přenosu snížena. Kliknutím na tlačítko OK se okno „New subnet Profibus“ zavře a následně se pomocí stisku na tlačítko OK zavře i okno „Profibus interface DP“ (obr. 5.13). Dokončená konfigurace sběrnice Profibus-DP je zobrazena na obr. 5.14.



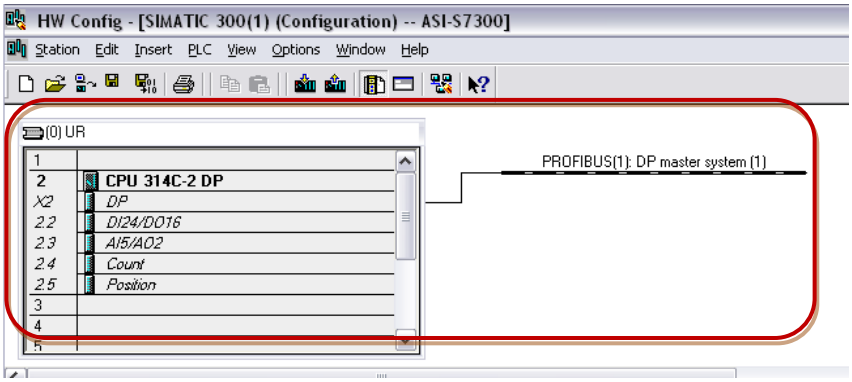
Obr. 5.11 Konfigurace Profibus-DP.



Obr. 5.12 Volba přenosové rychlosti a profilu sběrnice Profibus.



Obr. 5.13 Nastavení sběrnice Profibus-DP.



Obr. 5.14 Dokončená konfigurace sběrnice Profibus-DP.

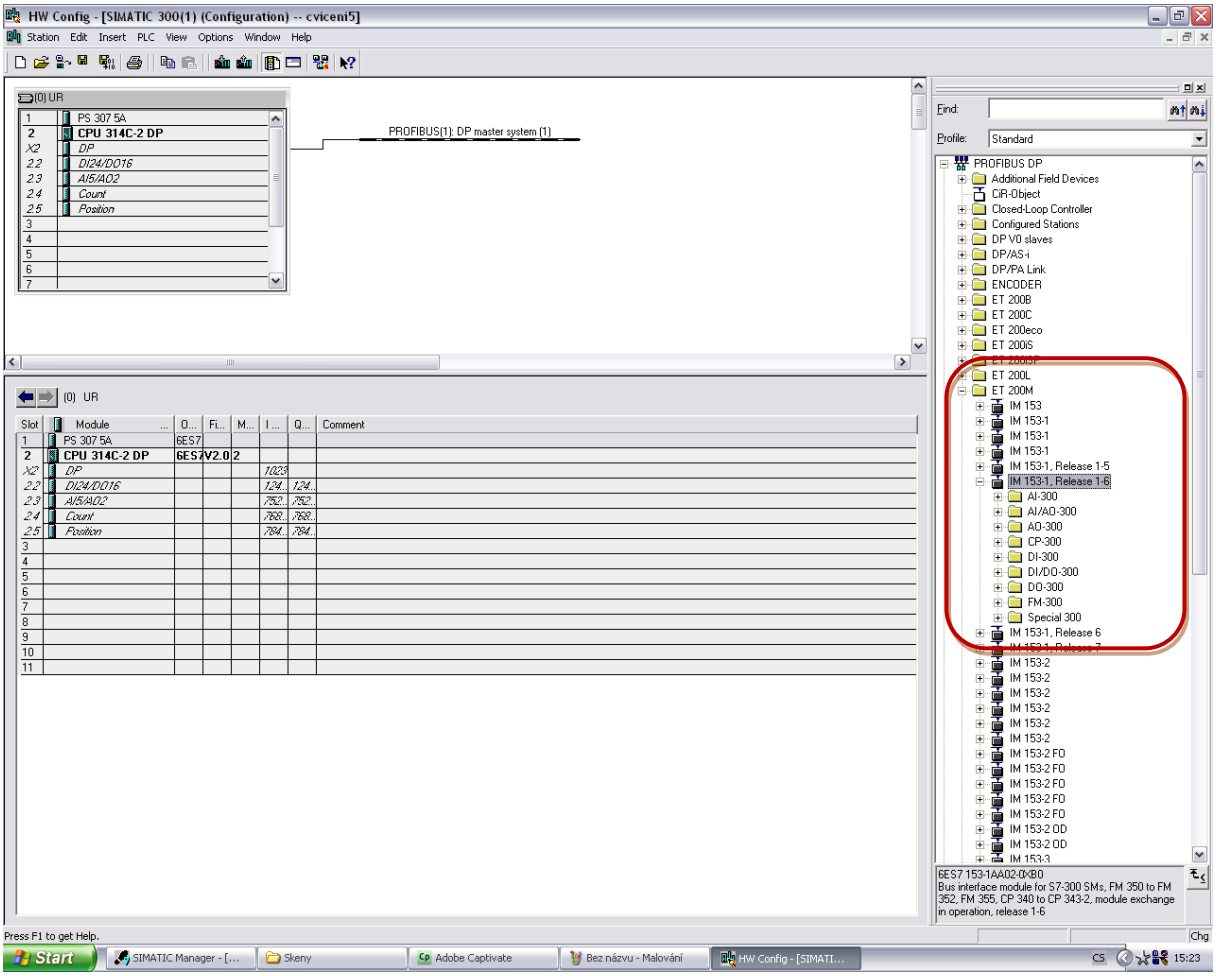
Periférie ET 200M je k dispozici ve složce „Profibus-DP“ => ET 200M => IM 153-1 (6ES7 153-1AA02-0XB0) (obr. 5.15). Kliknutím na ikonu IM 153-1 a přetažením pomocí Drag&Drop se tento modul přemístí nad sběrnici a vloží. Po vložení se otevře okno se zadáním adresy periférie na Profibus-DP sběrnici (obr. 5.16). V našem případě je adresa 9. Adresa lze zjistit nebo ji lze nastavit pomocí přepínačů DIP přímo na připojené periférii (obr. 5.17).

Za modul ET 200M jsou dále řazeny jednotlivé karty vstupů, výstupů (analogové, digitální) či karty speciálních funkcí (čítačové, řídicí karty s regulátory, moduly pro krokové motory, moduly pro vážení a další…) podle nabídky po rozkliknutí konkrétního modulu. Pro každou kartu je nutné nakonfigurovat adresy vstupů a výstupů a další parametry v závislosti na použité kartě (např. u karty analogových vstupů typ měření a rozsahy měření).

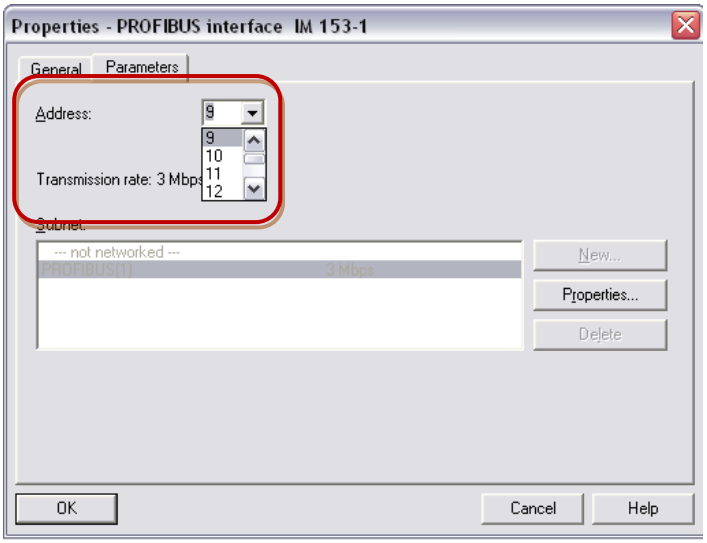
V našem konkrétním příkladě se vloží podle zadání tři rozšiřující karty:

- Karta analogových vstupů a výstupů AI4/AO2 (6ES7 334-OKE0-0AB0).
- Karta digitálních vstupů DI16 (6ES7 321-1BH01-0AA0).
- Karta digitálních výstupů DO16 (6ES7 322-1BH01-0AA0).

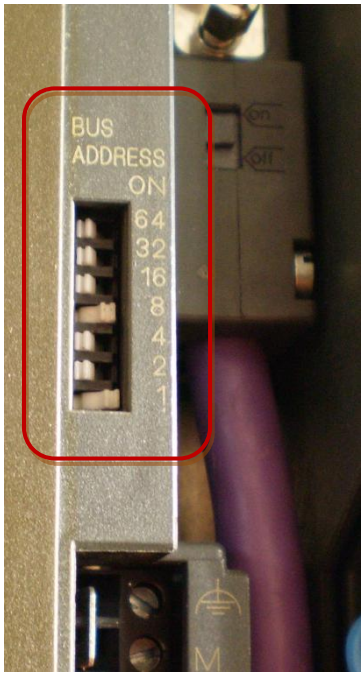
Konečná hardwarová konfigurace řešeného příkladu je zobrazena na obr. 5.18 a obr. 5.19.



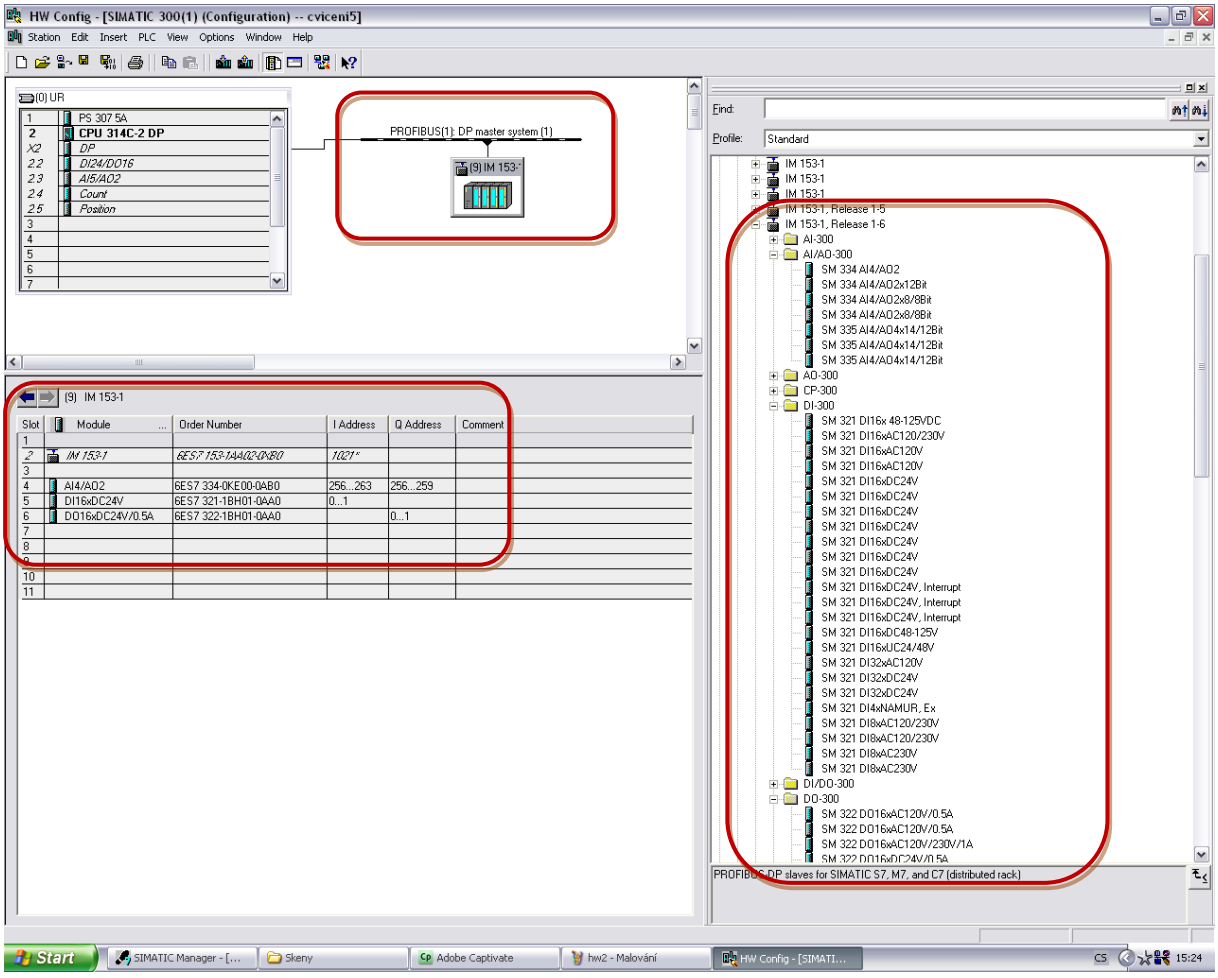
Obr 5.15 Umístění ET 200M v katalogu v hardwarové konfiguraci.



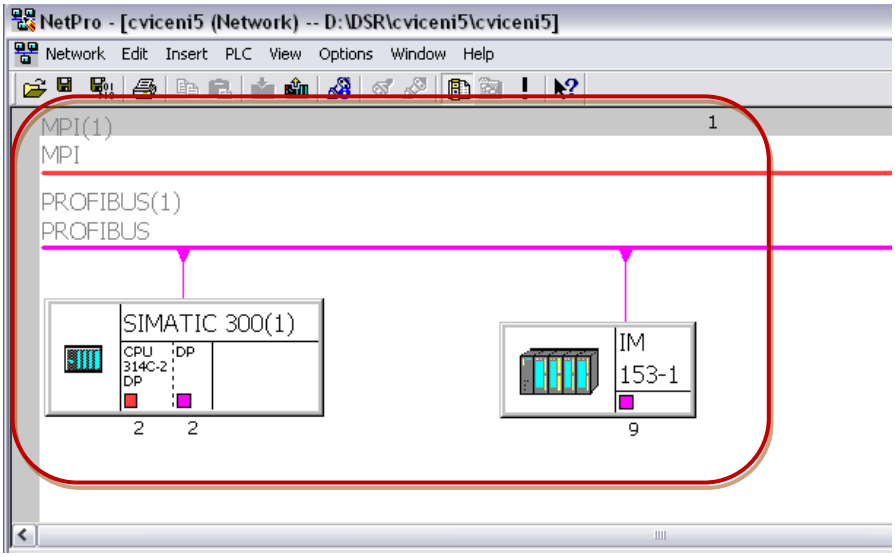
Obr 5.16 Adresa periférie ET 200M na sběrnici Profibus-DP.



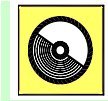
Obr 5.17 Určení adresy periférie připojené přes Profibus-DP.



Obr 5.18 Periférie ET 200M s vloženými kartami vstupů a výstupů.

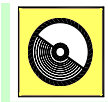


Obr 5.19 NetPro.



DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI5\



DVD-ROM

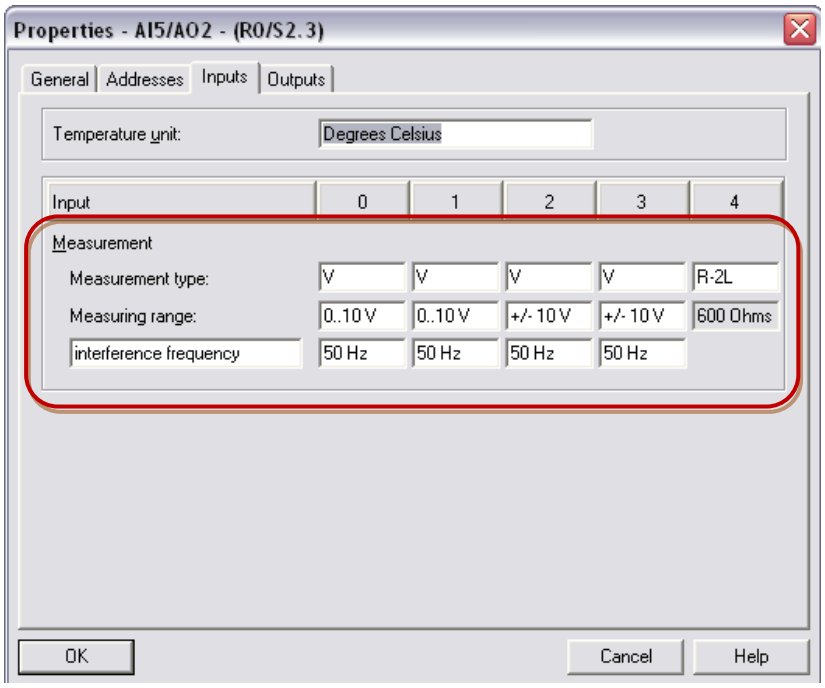
K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI5\

Řešená úloha 5.2

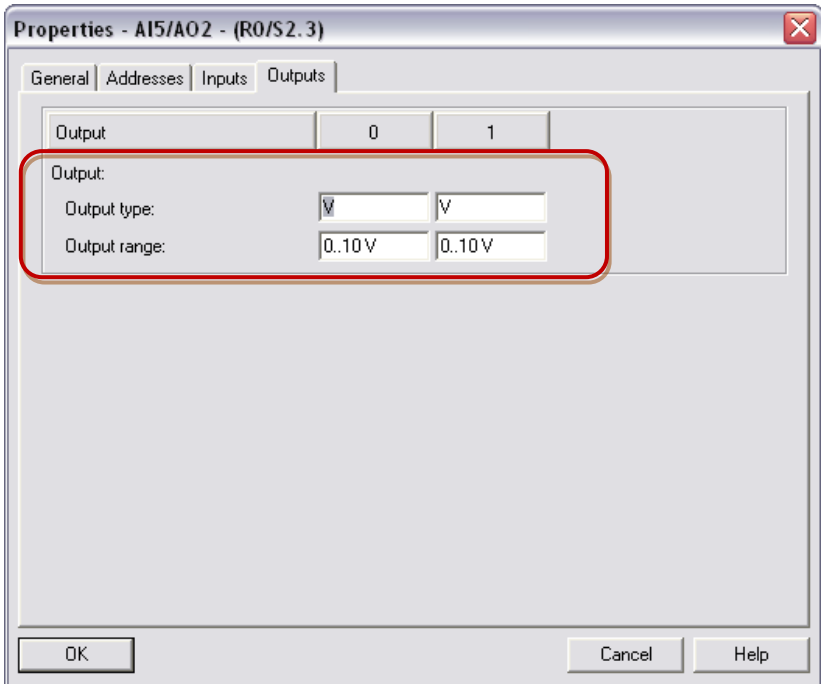
Zadání: Použijte hardwarovou konfiguraci vytvořenou z řešené úlohy 5.1. Na kartu digitálních vstupů na vzdálené periférii připojte přípravek pro simulaci spínání vstupních signálů. K vstupům a výstupům PLC připojte simulátor regulovaných soustav (RC člen).

Pro PLC vytvořte program s PID regulátorem FB41 „CONT_C“, který bude řídit napětí na výstupu RC členu (bude načítat data z prvního analogového vstupu PLC a bude zapisovat analogovou hodnotu na první analogový výstup PLC). Zajistěte periodické volání (100ms) tohoto PID regulátoru. Konstanty PID regulátoru nastavte experimentálně. Režim regulátoru (automatický/manuální), volbu P, I a D složky regulátoru a restart regulátoru nastavujte pomocí přípravku pro simulaci spínání vstupních signálů, který připojte na digitální vstupy vzdálené periférie.

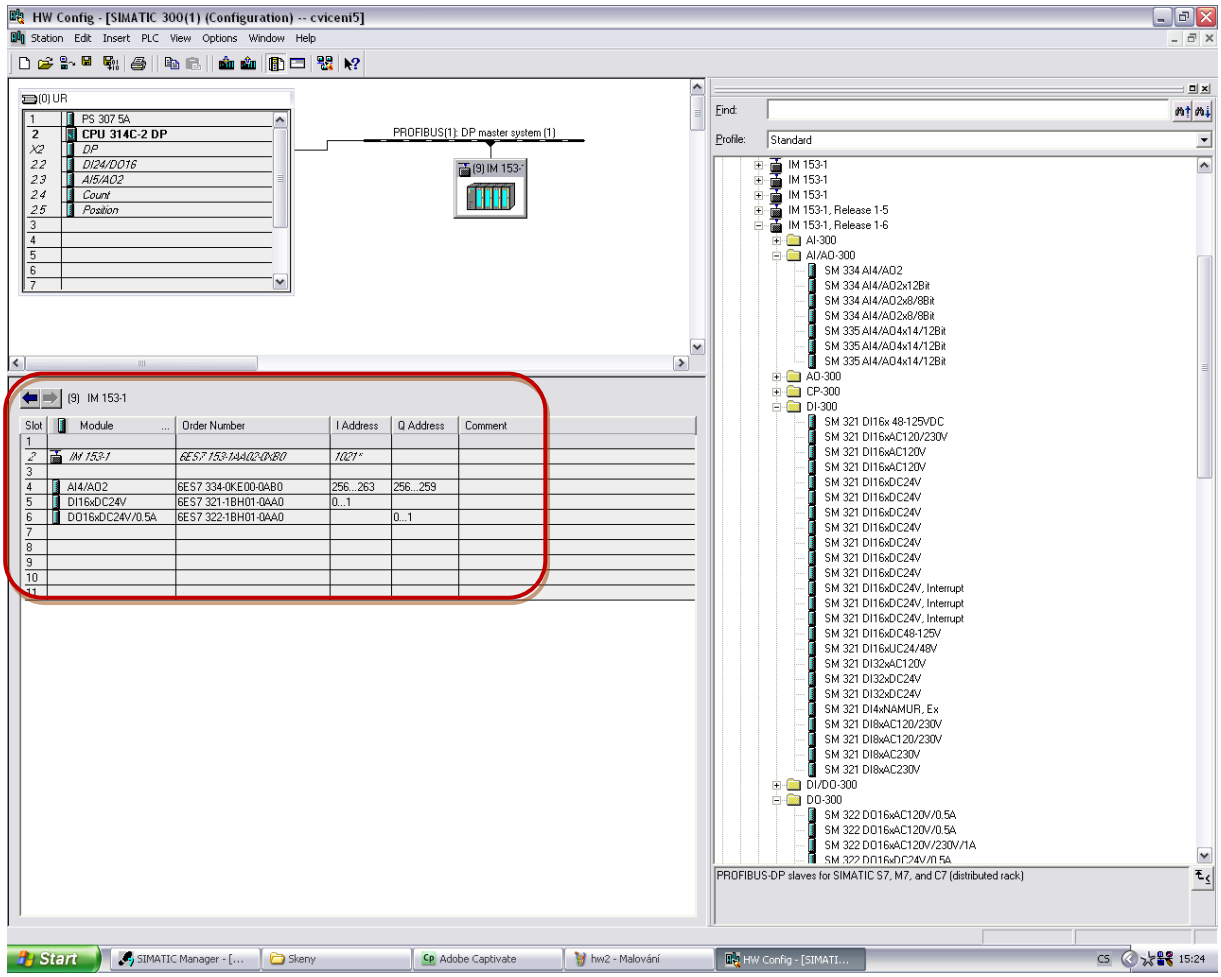
Hardwarová konfigurace bude obsahovat PLC S7-300, CPU 314C-2DP (6ES7 314-6CF02-0AB0) a periférii ET 200M (6ES7 153-1AA02-0XB0) s přídavnými kartami podle zvolené periferie z přední stěny v laboratoři. Hardwarovou konfiguraci vytvořte podle návodu v řešené úloze 5.1. Nastavení analogových vstupů a analogových výstupů je zobrazeno na obr. 5.20 a obr. 5.21. Vytvořená hardwarová konfigurace podle zadání je na obr. 5.22. Nastavení vzorkovací periody pro OB35 v hardwarové konfiguraci je znázorněno na obr. 5.23.



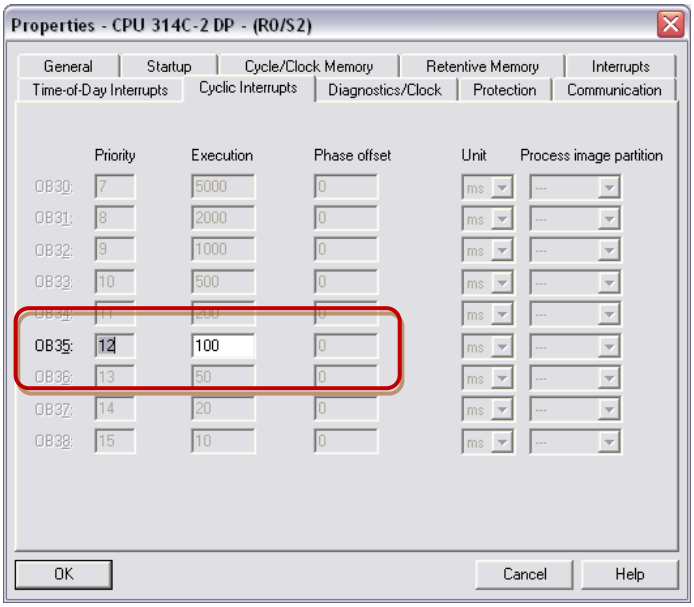
Obr. 5.20 Nastavení analogových vstupů.



Obr. 5.21 Nastavení analogových výstupů.



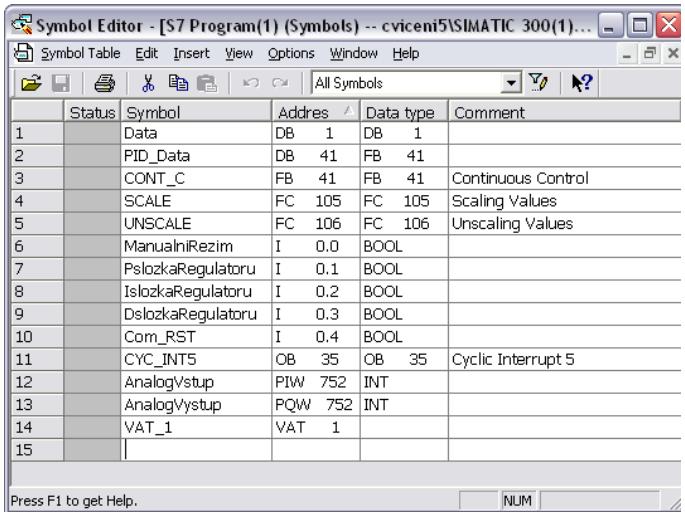
Obr. 5.22 Vytvořená hardwarová konfigurace.



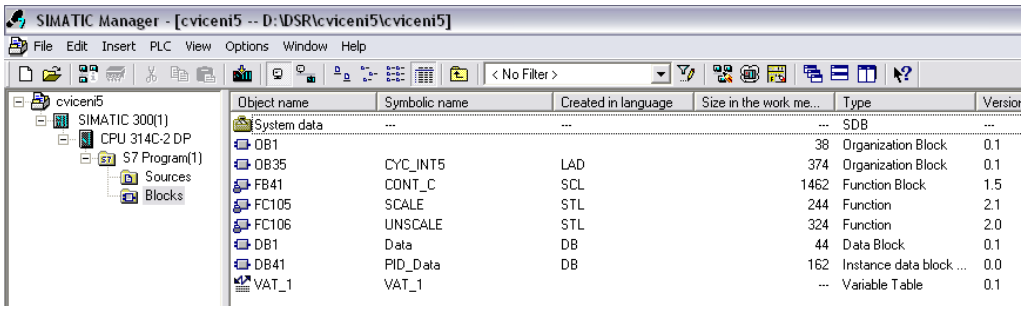
Obr. 5.23 Nastavení vzorkovací periody pro organizační blok OB35.

Řešení programu v LAD:

Program je řešen v cyklicky volaném organizačním bloku OB35. V prvním networku je funkce SCALE, která přepočítává vstupní hodnotu z převodníku vstupní analogové karty periférie na reálnou hodnotu s plovoucí desetinnou čárkou. Ve druhém networku je umístěn PID regulátor. Ve třetím networku je pak umístěna funkce UNSCALE, která přepočítává akční veličinu vypočtenou PID regulátorem na hodnotu typu INTEGER pro převodník výstupní analogové karty periférie.

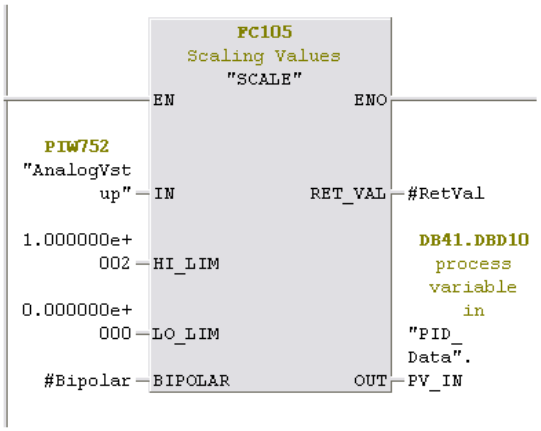


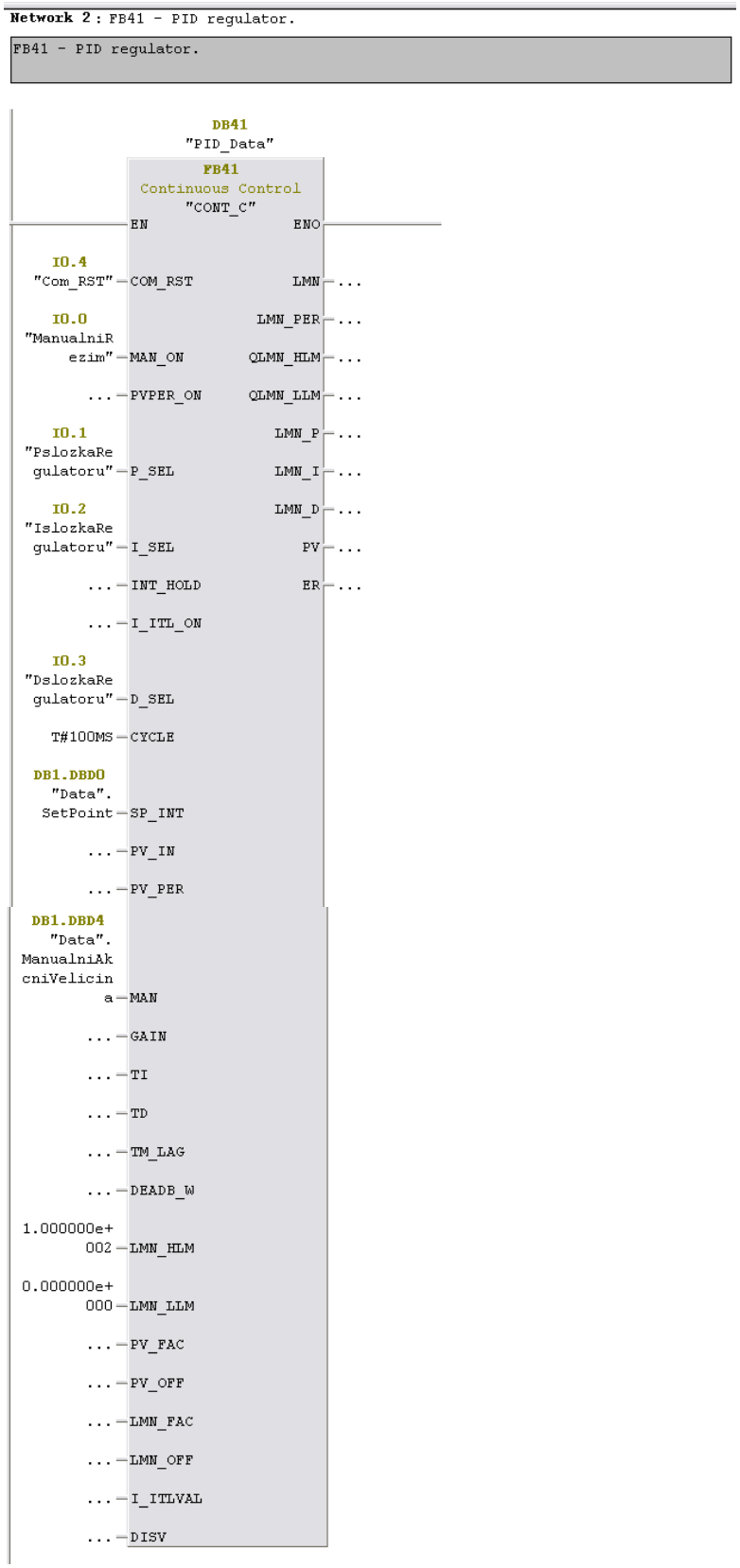
Obr. 5.24 Tabulka symbolů.



OB35:

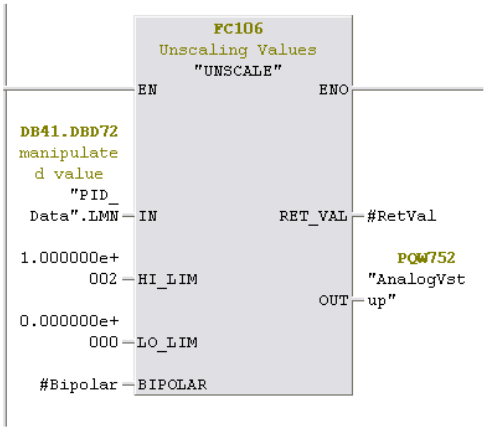
```
OB35 :  "Cyclic Interrupt"
Comment:

Network 1: Title:
Comment:
```

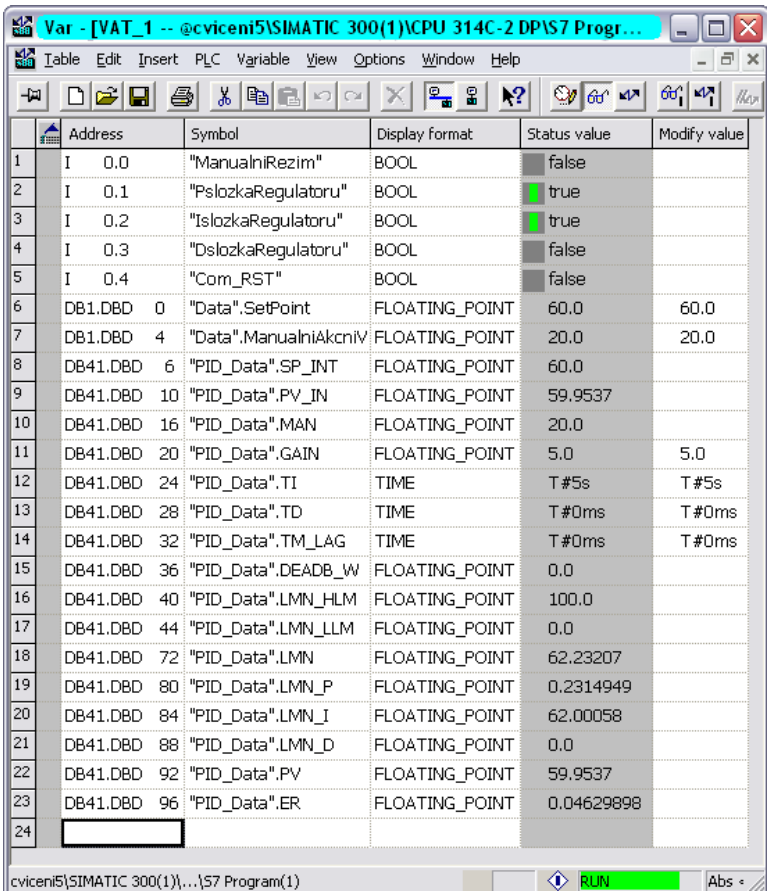



Network 2 : FB41 - PID regulator.
FB41 - PID regulator.
DB41
"PID_Data"
FB41
Continuous Control
"CONT_C"
EN
ENO
I0.4
"Com_RST"
COM_RST
LMN
...
I0.0
"ManualniRezim"
MAN_ON
LMN_PER
QLMN_HLM
...
PVPER_ON
QLMN_LLM
I0.1
"PslozkaRegulatoru"
P_SEL
LMN_P
LMN_I
I0.2
"IslozkaRegulatoru"
I_SEL
LMN_D
PV
ER
INT_HOLD
I_ITL_ON
I0.3
"DslozkaRegulatoru"
D_SEL
T#100MS
CYCLE
DB1.DBD0
"Data".SetPoint
SP_INT
PV_IN
PV_PER
DB1.DBD4
"Data".ManualniAkcniVelicina
MAN
GAIN
TI
TD
TM_LAG
DEADB_W
1.000000e+002
LMN_HLM
0.000000e+000
LMN_LLM
PV_FAC
PV_OFF
LMN_FAC
LMN_OFF
I_ITLVAL
DISV

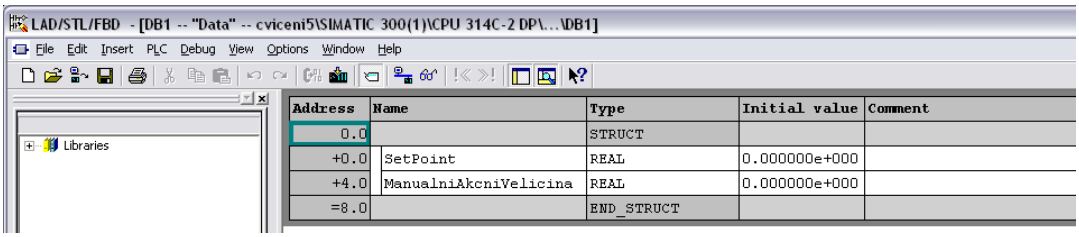
Network 3 : FC 106 - Unscale funkce.

```
Funkce Unscale prepocitava realnou vstupni hodnotu typu FLOATING POINT (omezena
hornim HI_LIM a dolnim LO_LIM limitem) na hodnotu typu INT (OUT).
OUT = [ ((IN-LO_LIM)/(HI_LIM-LO_LIM)) * (K2-K1) ] + K1
BIPOLAR: vystup je mezi -27648 az 27648, pak K1=-27648.0 a K2=+27648.0
UNIPOLAR: vystup je mezi 0 a 27648, pak K1 = 0.0 a K2 = +27648.0
```





DB1:



DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI5\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI5\

6. LOKÁLNÍ SÍTĚ, STANDARD IEEE 802

Čas ke studiu: 2 hodiny

Cíl Po prostudování této kapitoly budete umět

- Definovat pojem lokální sítě.
- Popsat standard IEEE 802.
- Popsat zařízení pro propojování sítí a jejich vlastnosti.
- Praktická výuka bude v tomto týdnu věnována práci na projektu č. 2.

Výklad

6.1. Lokální sítě

Pojmem Local Area Network (LAN, lokální síť, místní síť) se označuje síť, která umožňuje komunikaci mezi propojenými zařízeními. Lokální sítě jsou charakteristické vysokými přenosovými rychlostmi a malým dosahem. Lokální sítě pracují obvykle v režimu bez spojení (komunikující zařízení nenavazují spojení). [1, 2]

Naproti tomu se lze setkat se zkratkou WAN (Wide Area Network), která označuje rozsáhlou síť. WAN síť, která pokrývá rozsáhlou plochu (která např. překračuje hranice města, regionu nebo státu). Nejznámějším příkladem sítě WAN je Internet.
Další obdobné zkratky jsou:

- DAN (Departmental Area Network) – síť sdílená jedním oddělením
- FAN (Facility Area Network) – síť sdílená jedním pracovištěm
- MAN (Metropolitan Area Network) – metropolitní sítě – propojení lokálních sítí v rámci městské zástavby.
- PAN (Personal Area Network) - jedná se o velice malou počítačovou síť, kterou člověk používá pro propojení osobních elektronických zařízení (např. Bluetooth, IrDA).

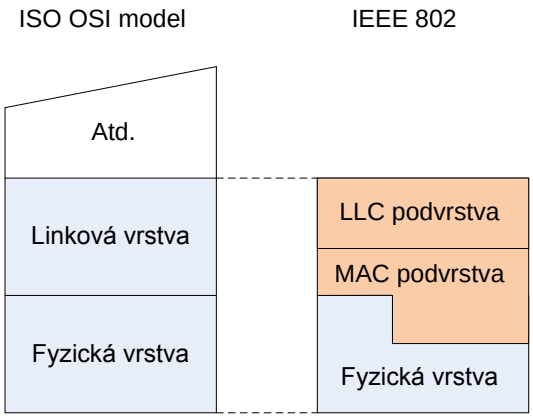
Rozlehlost sítě lze hodnotit parametrem a, který udává poměr mezi zpožděním signálu τ a střední dobou potřebnou pro vyslání jednoho paketu t_0 při dané přenosové rychlosti: $a = \tau / t_0$. Sítě, kde $a > 1$ se označují jako rozlehlé. Lokální sítě mají $a < 1$. [1, 2]

6.2. Standard IEEE802

Standard IEEE 802 je souhrnou specifikaci lokálních a metropolitních sítí. Vznikl v roce 1980 a stále se rozvíjí. Popisuje služby a protokoly, které odpovídají dvěma nejnižším úrovním ISO OSI modelu. [1, 2, 7] Tento standard však dělí a označuje tyto vrstvy poněkud jiným způsobem – linkovou vrstvu ISO OSI modelu dělí na dvě podvrstvy:

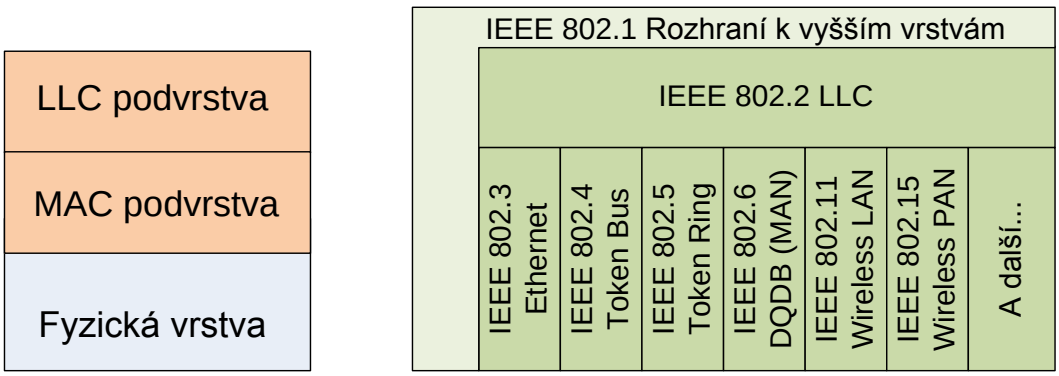
- MAC (Medium Access Control) – nižší podvrstva, je v ní implementovaná příslušná metoda přístupu ke komunikačnímu médiu. Funkcionalita MAC vrstvy bývá vestavěna přímo v hardware síťového rozhraní. Nejběžnější metody popsané v uvedeném standardu jsou založeny na CSMA a nebo předávání pověření.

– LLC (Logical Link Control) – vyšší podvrstva, zajišťuje řízení logického spojení, tzn. ostatní úkoly linkové vrstvy (kontrola chyb, adresování, řízení toku dat apod.)



Obr. 6.1 Srovnání ISO OSI modelu a IEEE 802.

IEEE 802 obsahuje řadu částí a každá z nich je zaměřena na konkrétní funkce a služby používané v LAN a MAN sítích. Zjednosušená struktura standardu a jeho základní části jsou uvedeny na obrázku 6.2.



Obr. 6.2 Struktura standardu IEEE 802 a jeho základní části.

Základní části IEEE (celkem obsahuje desítky částí a dílčích částí) [1, 2, 7]:

– IEEE 802.1 (Bridging and Network Management) – zastřešuje ostatní doporučení řady, definuje jejich strukturu a vzájemnou vazbu. Popisuje také propojení lokálních sítí opřené o MAC adresaci – mosty (bridges).

– IEEE 802.2 (Logical link control) - definuje funkce a služby linkové vrstvy. Jde o dva základní druhy služeb - nepotvrzovanou datagramovou službu (Connectionless Service), potvrzovanou datagramovou službu a virtuální spojení (Connection-oriented Service). Nepotvrzovaná datagramová služba využívá vysoké kvality přenosových kanálů lokálních sítí a nezajišťuje potvrzovací mechanismus, ten nechává na vyšších vrstvách a aplikačních programech. Potvrzovaná datagramová služba a virtuální spojení naproti tomu potvrzování zajišťují.

– IEEE 802.3 (Ethernet) - viz. kapitola 9.

– IEEE 802.11 a/b/g/n (Wireless LAN (WLAN) & Mesh) – standard pro bezdrátové lokální sítě WLAN. Zahrnuje šest druhů modulací pro posílání radiového signálu, přičemž všechny

používají stejný protokol. Modulace jsou popsány v dodatcích ke standardu, označených a, b, g, n, y.

- IEEE 802.15 (Wireless PAN) - standard se zabývá bezdrátovými osobními sítěmi. Jsou v něm popsány sítě jako Bluetooth (802.15.1), ZigBee (IEEE 802.15.4) aj.
- A další…

Některé v minulosti velice známé části IEEE 802, resp. pracovní skupiny, zabývající se známými standardy, jsou dnes neaktivní nebo rozpuštěny a nepokračují ve vývoji těchto standardů (IEEE 802.4 Token bus, IEEE 802.5 (Token Ring), IEEE 802.6 (DQDB-MAN), IEEE 802.7 (Broadband LAN using Coaxial Cable) a další. Je to dáno tím, že uvedené standardy byly v průběhu let překonány jinými technologiemi.

6.3. Zařízení pro propojování sítí

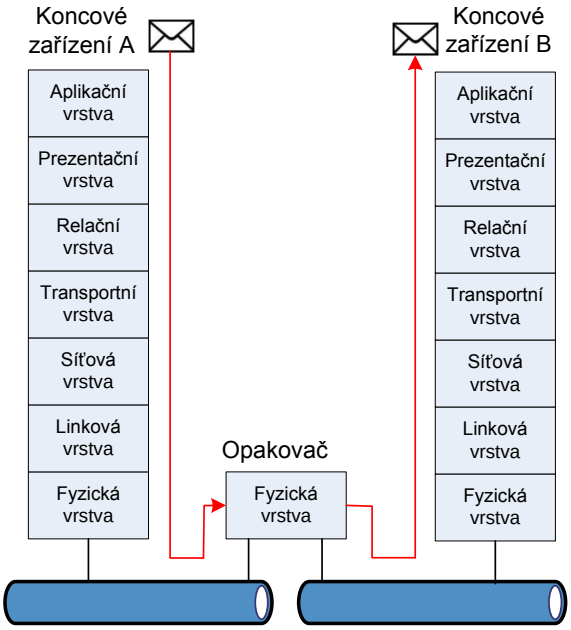
Opakovač (Repeater)

Opakovač je zařízení, které pracuje pouze na úrovni fyzické vrstvy a funguje jako zesilovač elektrického signálu. Všechny přenosové kanály mají určitou maximální delku média, která je dána zejména útlumem signálu při přechodu tímto médiem. Hlavním úkolem opakovačů je tedy zesílení signálu a jeho „očištění“ signálu, jelikož průchodem médiem dochází také k různým zkreslením a deformacím. Opakovače vnímají pouze přenášení bity, to co přijmou na jedné straně, na druhé odešlou. Je tedy pro signál plně průchozí.

Hlavním důvodem použití je to, že zvyšují délku segmentu. Nevýhodou je to, že propouštějí celý provoz z jednoho segmentu do druhého, i když to není nutné (když obě koncová zařízení jsou na jedné straně od opakovače).

Obdobné zařízení je rozbočovač (hub) – multiportový opakovač. Zatímco běžný opakovač propojuje jen dva segmenty, hub umožňuje propojit více segmentů. Je jedním ze základních zařízení používaných pro hvězdicovou topologii. Základní vlastností je to, že hub přeposílá data z jednoho segmentu do všech ostatních, tzn. všechny segmenty tvoří jedno sdílené médium.

U počítačových sítí se od využívání hubů upouští, nahradily je tzv. switch (viz. mosty), nicméně u některých průmyslových sběrnic se nadále používají (Ethernet Powerlink). [1, 3]

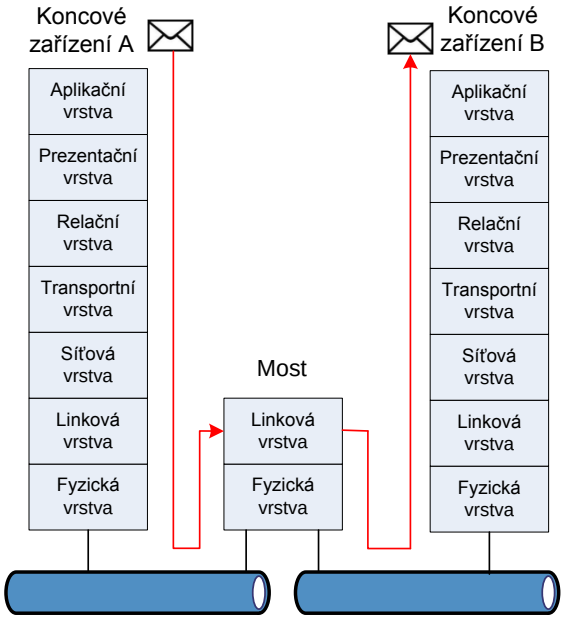


Obr. 6.3 Princip fungování opakovače.

Most (Bridge)

Most je podobné zařízení jako opakovače, pracuje však nejen na fyzické vrstvě, ale i na linkové. Dokáže však rozpoznat, zda data mohou zůstat v daném segmentu nebo zda mají být přepuštěny do dalšího segmentu sítě. Jeho výhodou je to, že nezatěžuje zbytečně provoz v ostatních segmentech. Tím, že pracuje na úrovni linkové vrstvy, rozpoznává fyzické adresy vysílače a příjemce.

Most vzájemně propojuje dva segmenty sítě, ale i zde, podobně jako u opakovačů, existují zařízení, které propojují několik segmentů. Těmto zařízením se říká víceportový most (switch). Switche se staly v současnosti jedním ze základních stavebních prvků přepínaného Ethernetu, jelikož dokáží rozdělit síť na jednotlivé kolizní domény (na rozdíl od hubů). [1, 4]



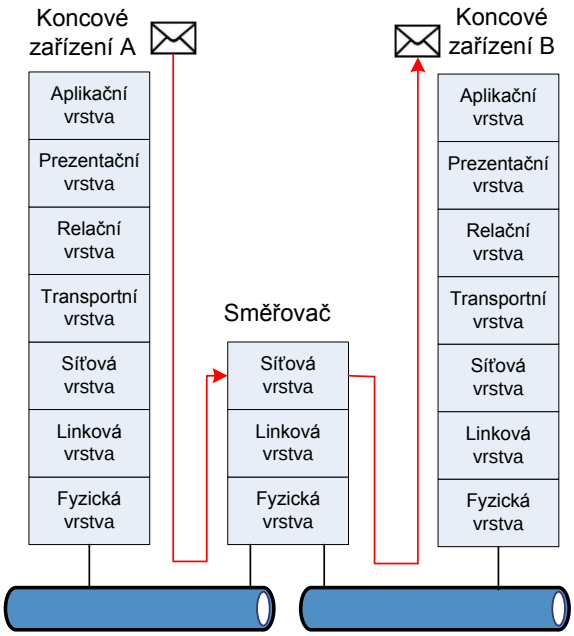
Obr. 6.4 Princip fungování mostu.

Směrovač (Router)

Směřovač je zařízení pro propojování na úrovni síťové vrstvy. Uvědomuje si topologii sítě, vnímá vlastní obsah rámců, dokáže správně rozpoznat formát jednotlivých paketů, které jsou v rámcích přenášené a využít informace v nich obsažené. Hlavní úlohou směrovače je doručit pakety od odesílatele k příjemci (tedy stejná, jako úloha síťové vrstvy). Směrovače rozhodují, kudy poslat jednotlivé pakety. Způsoby směřování byly popsány v kapitole 5.1.

Směrovače jsou na rozdíl od mostů na úrovni síťové vrstvy pro ostatní entity viditelné a mají své síťové adresy. Aby mohlo směřování správně fungovat, musí všechny propojované sítě používat stejný protokol na úrovni síťové vrstvy.

Toto omezení (nutnost stejného protokolu u propojovaných sítí) řeší multiprotokolové směrovače. Jsou schopné současně komunikovat více protokoly. Takový směřovač musí být schopen rozpoznat typ paketu přicházejícího z linkové vrstvy a podle toho potom aplikovat ten směrovací algoritmus, které k danému síťovému protokolu přísluší. [1, 5]



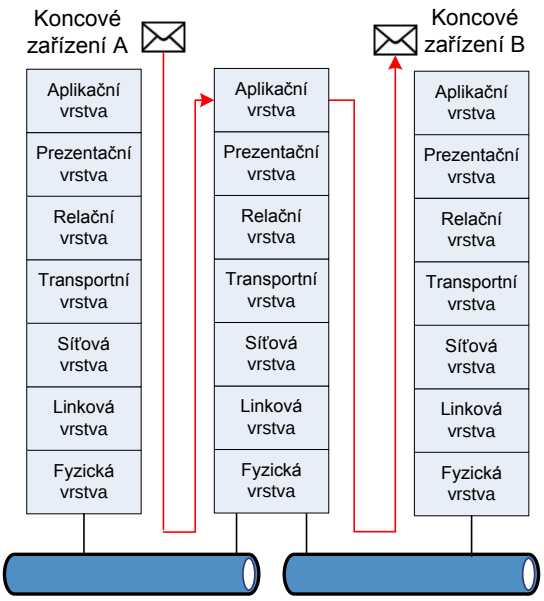
Obr. 6.5 Princip fungování směřovače.

Brouter (Bridge/Router)

Jedná se o zařízení, které kombinuje funkci mostu a směřovače. Funguje jako směrovač až do okamžiku, kdy pro nějaký paket nedokáže aplikovat směrovací algoritmus. Pak jej propustí dále podobně jako most. Použití nachází u komunikačních systémů, kde fungují i protokoly nevyužívající síťovou vrstvu. [1, 6]

Brána (Gateway)

Jedná se o zařízení, které propojuje dva zcela odlišné komunikační systémy, tzn. sítě úplně odlišných koncepcí. Provádí konverzi komunikačních protokolů. Pracuje na všech úrovních, na které je nutné tuto konverzi provést - tedy v některých případech i na aplikační vrstvě. [1, 6]



Obr. 6.6 Princip fungování brány.

Shrnutí pojmů

Pojmem Local Area Network (LAN, lokální síť, místní síť) se označuje síť, která umožňuje komunikaci mezi propojenými zařízeními. Lokální sítě jsou charakteristické vysokými přenosovými rychlostmi a malým dosahem. Lokální sítě pracují obvykle v režimu bez spojení (komunikující zařízení nenavazují spojení).

Standard IEEE 802 je souhrnou specifikaci lokálních a metropolitních sítí. IEEE 802 obsahuje řadu částí a každá z nich je zaměřena na konkrétní funkce a služby používané v LAN a MAN sítích.

Pro propojování sítí se používají následující zařízení:

- Opakovač (Repeater).
- Most (Bridge).
- Směrovač (Router).
- Brouter (Bridge/Router).
- Brána (Gateway)

Otázky

1. Co je to Local Area Network?
2. Co je to Wide Area Network?
3. Jakým parametrem lze definovat rozlehlost sítě?
4. Co definuje standard IEEE 802?
5. Na jaké podvyrstvy dělí standard IEEE 802 linkovou vrstvu ISO OSI modelu?

6. Srovnejte strukturu ISO OSI modelu a IEEE 802?
7. Vyjmenujte a popište základní části standardu IEEE 802.
8. Popište vlastnosti a funkce opakovače?
9. Popište vlastnosti a funkce mostu?
10. Popište vlastnosti a funkce směřovače?
11. Popište vlastnosti a funkce Brouteru?
12. Popište vlastnosti a funkce brány?
13. Jaké zařízení se označují hub a switch?

Použitá literatura a další zdroje

1. Kováč F. Distribuované riadiace systémy. Vydavatelstvo STU, Bratislava 1998. ISBN 80-227-1082-2.
2. Janeček J., Bílý M.: Lokální sítě. Vydavatelství ČVUT, Praha 1998.
3. Repeater. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a93/a340c120.php3
4. Bridge. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a93/a341c120.php3
5. Router. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a93/a342c120.php3
6. Brouter, gateway. Archív článků a přednášek Jiřího Peterky. [online], [cit. 03-08-2010] http://www.earchiv.cz/a93/a343c120.php3
7. IEEE 802. [online], [cit. 03-08-2010] http://standards.ieee.org/about/get/

Řešená úloha 6.1

Zadání: **Práce na projektu č.2**.

Předmětem cvičení je práce na projektu č. 2. Zadání projektu se týká komunikace po sběrnici Profibus-DP s PLC S7 300 podle vybraného zadání.

7. AS-INTERFACE

Čas ke studiu: 2 hodiny

Cíl Po prostudování této kapitoly budete umět

- Popsat základní vlastnosti sběrnice AS Interface.
- Popsat vlastnosti fyzické vrstvy AS Interface.
- Popsat vlastnosti linkové vrstvy AS Interface.
- Praktická výuka je zaměřena na komunikaci po MPI u programovatelného automatu Simatic S7 300, komunikace pomocí global data.

Výklad

7.1. AS-i (Actuator Senzor Interface)

Standard AS-i (Actuator Sensor Interface) [1] vznikl počátkem devadesátých let. V současnosti standard udržován konsorciem výrobců, je však přihlášen ke standardizaci organizací IEC. Paralelně existuje (od roku 1991) i organizace uživatelů.

Pro další rozvoj standardu je důležitá jeho podpora firmou Siemens, která má také nejširší nabídku produktů s tímto rozhraním.

Charakteristické rysy lze shrnout do několika následujících bodů:

- Nestíněná dvoudrátová sběrnice s libovolnou topologií.
- Přenos dat a napájení po jediném vedení.
- Délku vedení maximálně 100 m při proudu 2A, při použití opakovačů 300 m.
- Maximálně 31 účastnických stanic.
- Maximálně 124 senzorů a 124 akčních členů.
- Řízení komunikace na principu Master – Slave.
- Kódování dat kódem Manchester.
- Zabezpečení telegramu paritou.
- Vysoká rychlost komunikace (cyklus sběrnice kratší než 5 ms).
- Velmi jednoduchá instalace.

Cílem standardu je podpora binárních akčních členů a senzorů na nejnižších úrovních procesní automatizace. Jde o sběrnici s Master-Slave řízením, současně lze připojit až 31 účastnických jednotek. Důležitým rysem standardu je možnost jejich napájení po sběrnici, která tak slouží pro napájení i pro přenos dat.

Velkou výhodou je také neexistence terminátorů na koncích vedení a prakticky libovolná topologie. Nejčastěji se však používá sběrnicová topologie. S ohledem na praktické použití lze použít další

topologie (strom, hvězda, kruh s pasivním připojením) a jejich kombinace. Délka vedení je do 100m včetně odboček ke stanicím. Lze použít nanejvýše dva opakovače k rozšíření délky vedení maximálně do 300m včetně odboček ke stanicím.

Pro realizaci Slave zařízení připojených k rozhraní AS-i se nejčastěji používají obvody ASIC (Application-Specific Integrated Circuit).

7.2. Verze specifikace AS-i

Verze 2.0 - původní specifikace (1994)

Je možnost připojení maximálně 31 zařízení. Každé zařízení má maximálně 4 digitální vstupy a 4 digitální výstupy.

Verze 2.1 - rozšíření specifikace (1998)

V nové specifikaci rozhraní je navíc definován rozšířený adresovací mód. Pokud všechna připojená zařízení podporují tento mód, je možné připojení až 62 zařízení. Adresový prostor je rozdělen na Slave zařízení A (1A až 31A) a Slave zařízení B (1B až 31B).

Verze 3.0 - další rozšíření specifikace (2005/2007)

V důsledku dalších požadavků uživatelů na možnosti komunikace přes AS-i komunikační rozhraní, vedly tyto požadavky k rozšíření specifikace umožňující přenos analogových hodnot. Také byly novou specifikací rozšířeny možnosti diagnostiky funkčnosti vytvořením speciálních diagnostických funkcí. V zájmu zachování plné zpětné kompatibility se velikost přesnášených telegramů nezvyšuje.

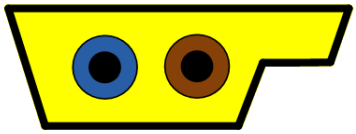
Současné PLC běžně pracují s analogovými vstupy a výstupy. Pro AS-i byl proto definován profil přesně specifikující postup přenosu digitalizovaných analogových hodnot. Ze čtyř datových bitů je jeden využit jako řídicí a analogová data jsou proto rozdělena do tříbitových postupně přenášených skupin, kterých je maximálně šest. Celkem tak lze přenést až 18-ti bitové slovo. [1]

7.3. Fyzická vrstva sběrnice

Vzhledem k využití jediného vedení pro přenos napájení i datových signálů je definice fyzické vrstvy zcela specifická. Nominální hodnota napájecího napětí je 24 V. Součástí napájecího zdroje je i standardem definovaná indukčnost, která se podílí na přenosu dat. Při vysílání mění jednotlivé stanice odběr proudu, což vyvolá vznik napěťových impulsů (kladných a záporných) na vedení. Tyto napěťové impulsy jsou superponovány na napájecím napětí, jejich výskyt a polarita jsou sledovány a vyhodnocovány [1].

AS-i kabel

Standard AS-i používá vlastní kabel. Jde o plochý kabel se dvěma vodiči dle obr. 7.1. Hnědý vodič má kladnou polaritu, modrý vodič má zápornou polaritu.

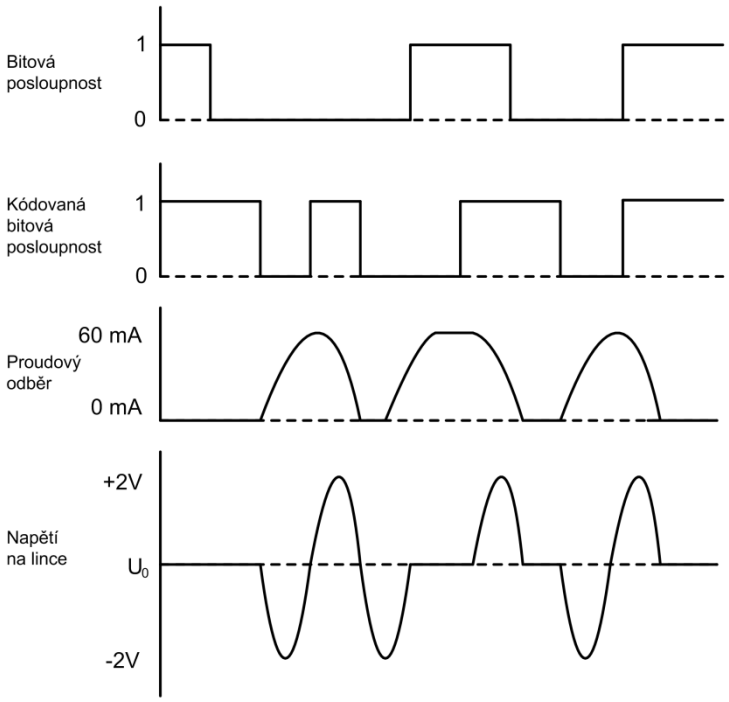


Obr. 7.1 Profil kabelu pro AS-i [1].

Připojení modulů k tomuto kabelu je realizováno krempováním, tzn. nejsou třeba žádné konektory ani odizolování spojů. Tato metoda současně zrychluje a zjednodušuje instalaci, neboť tvar kabelu brání připojení s opačnou polaritou.

Kódování dat

Kódování dat [1] definované standardem je zřejmé z následujícího obrázku.



Obr. 7.2 Kódování dat u AS-i [1].

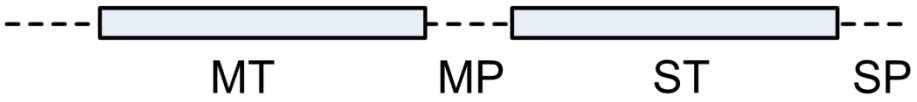
Binární posloupnost je nejprve zakódována kódem Manchester (ve středu bitového intervalu bitu s úrovní log. 0 je v zakódovaném signálu přechod log. 1 -> log. 0, ve středu bitového intervalu bitu s úrovní log. 1 je v zakódovaném signálu přechod log. 0 -> log. 1). Kódovaná bitová posloupnost je vysílačem převedena na změny odběru proudu, které se pak na lince projeví výše zobrazenými napěťovými impulsy.

Délka bitového intervalu je cca 6 ms, což odpovídá přenosové rychlosti 166 Kb/s. Skutečný přenosový výkon je vzhledem k prodlevám v komunikaci poněkud nižší.

7.4. Linková vrstva standardu

Linková vrstva standardu

Linková vrstva používá řízení přístupu Master-Slave a specifický formát telegramů. Jednotlivé účastnické stanice jsou cyklicky oslovovány stanicí řídicí, celý cyklus trvá podle počtu účastnických stanic maximálně 5 ms pro 31 účastnických stanic. Při menším počtu dotazovaných účastnických stanic se doba trvání cyklu úměrně zkracuje [1].

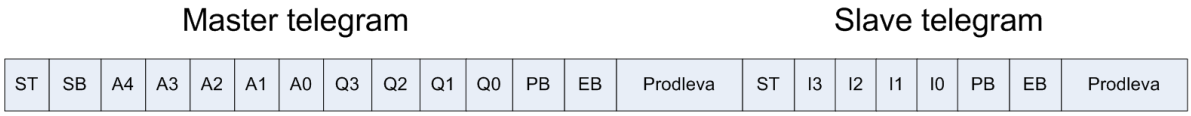


Obr. 7.3 Struktura telegramu AS-i.

Komunikace mezi řídicí a jednou účastnickou stanicí je zřejmá z obr. 7.3. Tato posloupnost se cyklicky opakuje pro všechny účastnické stanice v síti. Význam jednotlivých symbolů je následující:

- MT - telegram řídicí stanice (Master telegram).
- MP - prodleva po telegramu řídicí stanice (Master prodleva).
- ST - telegram účastnické stanice (Slave telegram).
- SP - prodleva po telegramu účastnické stanice (Slave prodleva).

Telegram řídicí stanice představuje výzvu pro účastnickou stanici, telegram účastnické stanice je pak reakcí na tuto výzvu. Obě časové prodlevy pak pomáhají synchronizaci komunikace. Komunikaci zahajuje Master vysláním Master telegramu a vyžaduje, aby Slave modul odpověděl v definované časové lhůtě. Master telegram se skládá z 5-bitové adresy Slave zařízení a 4-bitového datového paketu (např. hodnoty digitálních výstupů). Odpověď Slave zařízení je 7 bitů dlouhá obsahující 4 bity informací (např. hodnoty digitálních vstupů). Podrobný obsah Master a Slave telegramu je uveden na obr. 7.4.



Obr. 7.4 Podrobný obsah Master a Slave telegramu.

Master telegram začíná start bitem (ST) s hodnotou log. 0. Následuje řídicí bit (SB), který rozlišuje, zda je obsahem telegramu povel (SB = log. 1) nebo výměna dat popř. nastavování parametrizačních výstupů či adresy Slave zařízení (SB = log. 0). Za řídicím bitem je adresa Slave zařízení (bity A0 až A4, maximálně 31 adres). Bity Q0 až Q3 nesou předávanou informaci (data, povel apod.). Bit PB je sudá parita vysílaných dat. Bit EB je zakončovací stop bit, který má vždy hodnotu log. 1. Prodleva mezi telegramy trvá obvykle 3 až 5 a maximálně 10 bitových časových jednotek.

Slave telegram obsahuje čtyři informační bity (I0 až I3), adresátem je implicitně Master stanice. Informační bity jsou uvozeny stejně jako Master telegram start bitem (ST) s hodnotou log. 0, dále sudým paritním bitem PB a zakončovacím stop bitem EB, který má vždy hodnotu log. 1.

V rozšířené specifikace rozhraní (v2.11) je navíc definován rozšířený adresovací mód. V rozšířeném adresovacím módu je bit Q3 Master telegramu využit jako šestý bit adresy. Pokud všechna připojená zařízení podporují tento mód, je možné připojení až 62 zařízení. Adresový prostor je rozdělen na Slave zařízení A (1A až 31A) a Slave zařízení B (1B až 31B).

7.5. Zabezpečení přenosu

Zabezečení přenosu využívá toho, že struktura vysílaných telegramů obsahuje řadu pevně stanovených či pravidelně se opakujících prvků [1].

Datové přenosy jsou zabezpečeny následujícími prvky:

- Start bit - prvním impulsem, který se vyskytne na sběrnici při přenosu telegramu, musí být negativní impuls.
- Alternace impulsů - vzhledem ke zvolenému typu modulace musí mít dva následující impulsy opačnou polaritu.
- Mezera mezi impulsy - mezi dvěma impulsy uvnitř telegramu smí být mezera o délce maximálně délky jednoho impulsu.
- Informační obsah - ve druhé polovině bitového intervalu musí být vždy impuls.
- Kontrola parity - v kódovém slově telegramu musí být sudý počet bitů hodnoty log. 1.
- Stop bit - Posledním impulsem, kterým končí přenos telegramu po sběrnici, musí být kladný impuls.
- Délka telegramu - po ukončení telegramu stop bitem již na sběrnici nesmí následovat žádné další impulsy.

Sledováním těchto a dalších pravidelností a kontrolou parity lze dosáhnout zbytkové chybovosti, která je při ojedinělých a nezávislých chybách v řádu 10^{-12}.

Shrnutí pojmů

AS Interface je průmyslová komunikační sběrnice, která je určena pro přenos dat mezi řídicím systémech, senzory a akčními členy na nejnižší úrovni v distribuovaných řídicích systémech.

Standard AS-i používá vlastní kabel. Jde o profilovaný plochý kabel se dvěma vodiči.

Linková vrstva používá řízení přístupu Master-Slave a specifický formát telegramů.

Otázky

1. Popište základní vlastnosti AS Interface?
2. Popište fyzickou vrstvu u AS Interface?
3. Popište použité přenosové médium a způsob připojování zařízení.
4. Jaké způsob kódování dat je použitý u AS Interface?
5. Popište linkovou vrstvu u AS Interface?

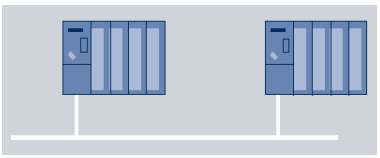
6. Jaká metoda přístupu ke komunikačnímu médiu je použita u AS Interface?
7. Popište způsoby zabezpečení přenosu u AS Interface?

Použitá literatura a další zdroje

1. Becker R. : AS-Interface, The Automation Solution. AS-International Association, 2002.

Řešená úloha 7.1

Zadání: Seznamte se s možnostmi komunikace po MPI u PLC S7 300/400.



Parametry a vlastnosti MPI komunikace:

- Fyzická vrstva: RS485.
- Topologie – linie.
- Maximální vzdálenost na segment: 50m.
- Maximální vzdálenost (metalické vedení): 100m (1x repeater).
- Přenosová rychlost: 187,5 kbps.
- Maximální počet stanic: 62 stanic.

Tab. 7.1 Možnosti komunikace pomocí MPI mezi jednotlivými CPU.

Služba	**Maximálně dat obecně**	**Bloky**
Global Data	22 B (S7-300) 54 B (S7-400)	- -/GDSEND, GDRCV
S7 basic komunikace	76 B 84 B	XSEND, XRCV XPUT, XGET
S7 komunikace (s7-400)	64 kB (S7-400) 440 B (S7-400)	BSEND, BRCV USEND, URCV, PUT GET

Konkrétní hodnoty maximální velikosti přenášených dat se různí podle použitého CPU.

MPI komunikace je dostupná nejen pro CPU S7 300, S7 400, ale i pro různé typy operátorských panelů.

Výhody MPI:

- MPI mají všechna CPU S7 300 a S7 400.
- Jednoduchost.

Nevýhody:

- Omezené množství přenášených dat.
- Delší doba odezvy v porovnání s dalšími typy komunikace.
- Malý dosah sítě.
- PLC jiných výrobců většinou nemají MPI rozhraní.

Řešená úloha 7.2

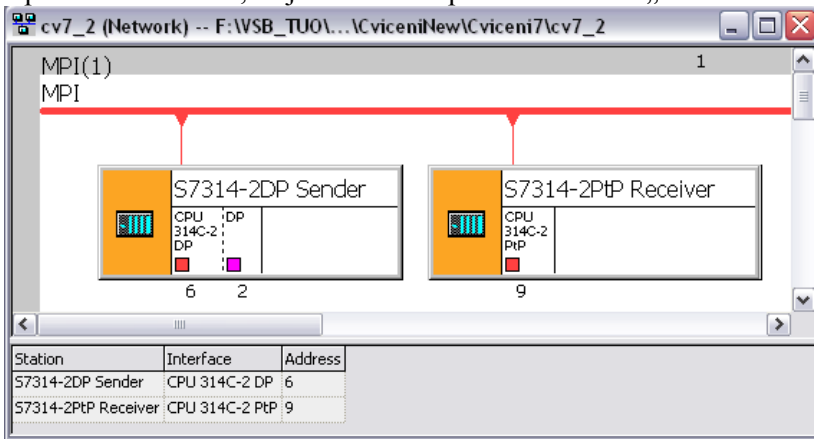
Zadání: Nastavte komunikaci mezi dvěma PLC (CPU 314C-2DP a CPU 314C-2PtP) po MPI. Pro komunikaci použijte globální data. Adresa PLC CPU 314C-2DP na sběrnici je 6, adresa PLC CPU 314C-2PtP je 9.

Z jednoho PLC posílejte hodnotu typu WORD a pět hodnot typu INTEGER. Zpět do prvního PLC posílejte reálné číslo. Oblasti paměti pro posílání zvolte podle svého uvážení.

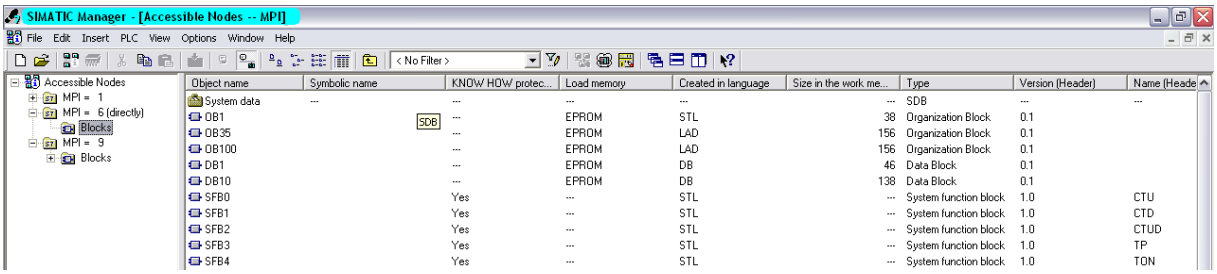
Prvním krokem řešení úlohy je hardwarová konfigurace dvou PLC.

Pro komunikaci je potřeba nastavit každému prvku na sběrnici jinou adresu. Defaultně je nastavena adresa MPI na všech automatech v laboratoři na 2 a adresy operátorských panelů na 1. Proto musíme adresu obou automatů podle zadání změnit. MPI adresy se nastavují v hardwarové konfiguraci automatu a to otevřením záložky CPU automatu. Nahrání nové konfigurace se však provádí nahráním na starou adresu automatu, proto je nutné, aby byl připojen na sběrnici pouze ten automat, na kterém chceme změnu provést. V hardwarové konfiguraci tedy nastavíme odlišné adresy na sběrnici MPI. CPU 314C-2DP na sběrnici je 6, adresa PLC CPU 314C-2PtP je 9.

Celkovou konfiguraci sítě si můžeme prohlédnout v nástroji NetPro (obr. 7.5). Po nahrání hardwarových konfigurací obě PLC spojíme sériovým komunikačním kabelem. Pro shlédnutí zařízení na sběrnici použijeme tlačítko „Accessible Nodes“ v hlavním okně Simatic Manageru (obr. 7.6). Pro připomenutí uveďme, že je nutno mít správně nastaven „PG/PC interface“.



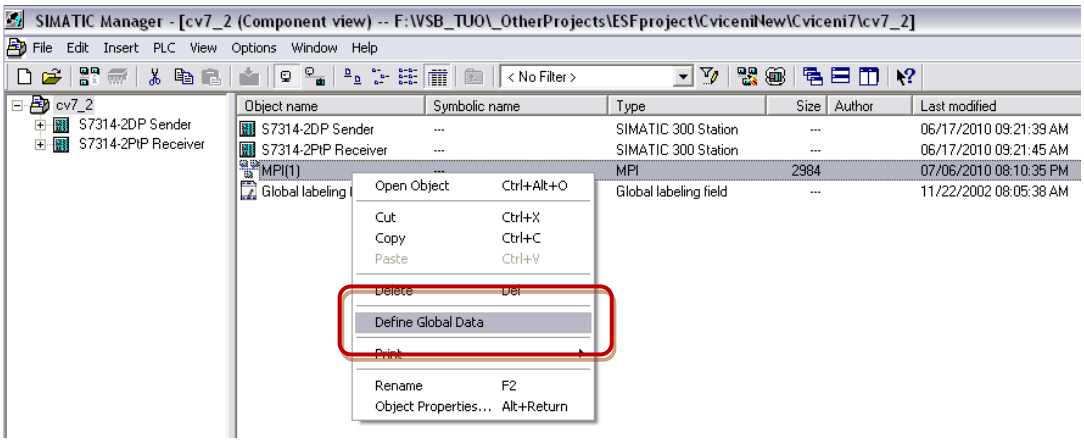
Obr. 7.5 NetPro.



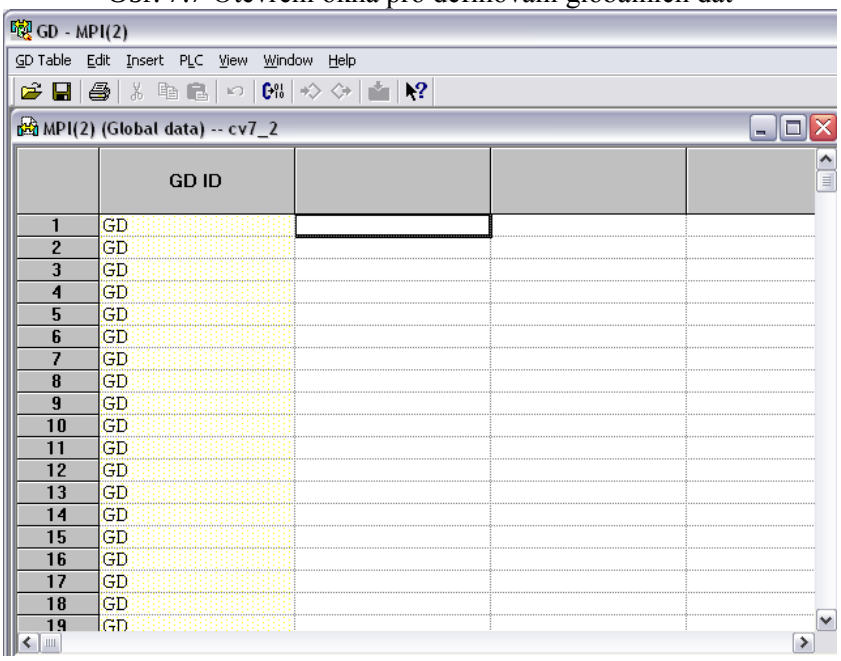
Obr. 7.6 Accessible Nodes.

Pokud máme obě PLC nakonfigurována, nadefinujeme globální data podle zadání. V hlavním okně Simatic Manageru pravým klikem na síť MPI spustíme pod položkou „Define Global Data“ (obr. 7.7) okno pro definování globálních dat (obr. 7.8). V prvním sloupci tabulky je tzv. GD ID (global data identifikátor). Dvojklikem na druhý sloupec se otevře nabídka (obr. 7.9) se stromem projektu. Vybereme první CPU a stiskneme OK. Tím jsme druhému sloupci tabulky přiřadili první

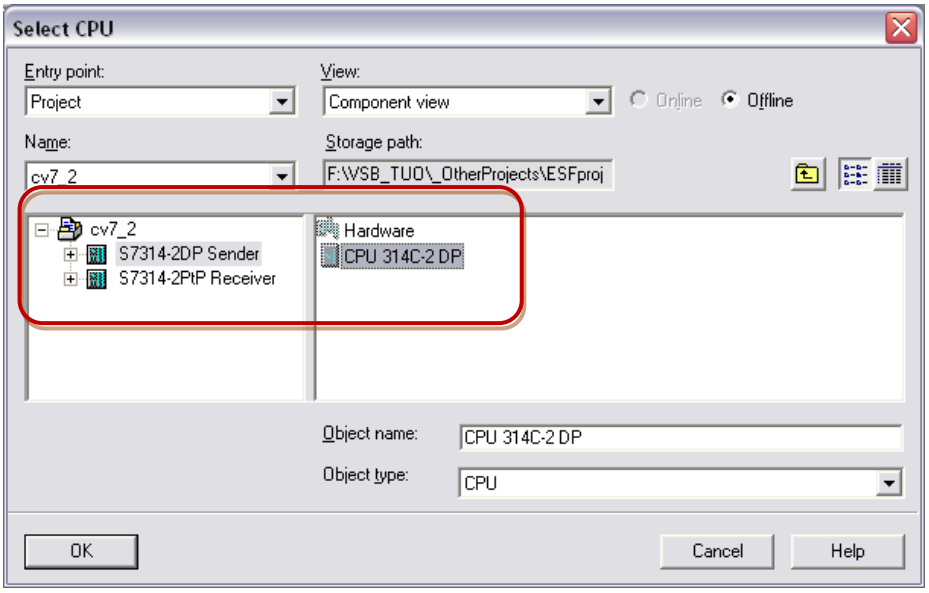
CPU. Dále dvojklikem na třetí sloupec vybereme druhé CPU a přiřadíme tím třetímu sloupci druhé CPU projektu. Konečný stav vybraných CPU je zobrazen na obr. 7.10.



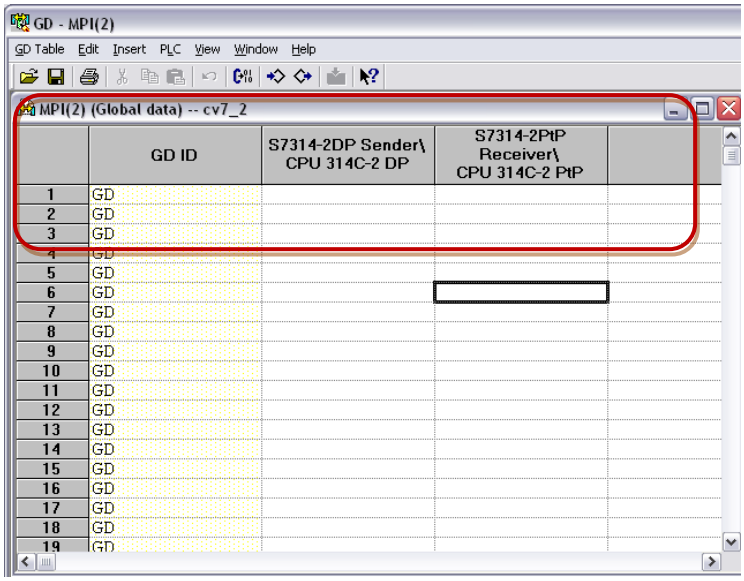
Obr. 7.7 Otevření okna pro definování globálních dat



Obr. 7.8 Okno pro definování globálních dat



Obr. 7.9 Výběr CPU projektu

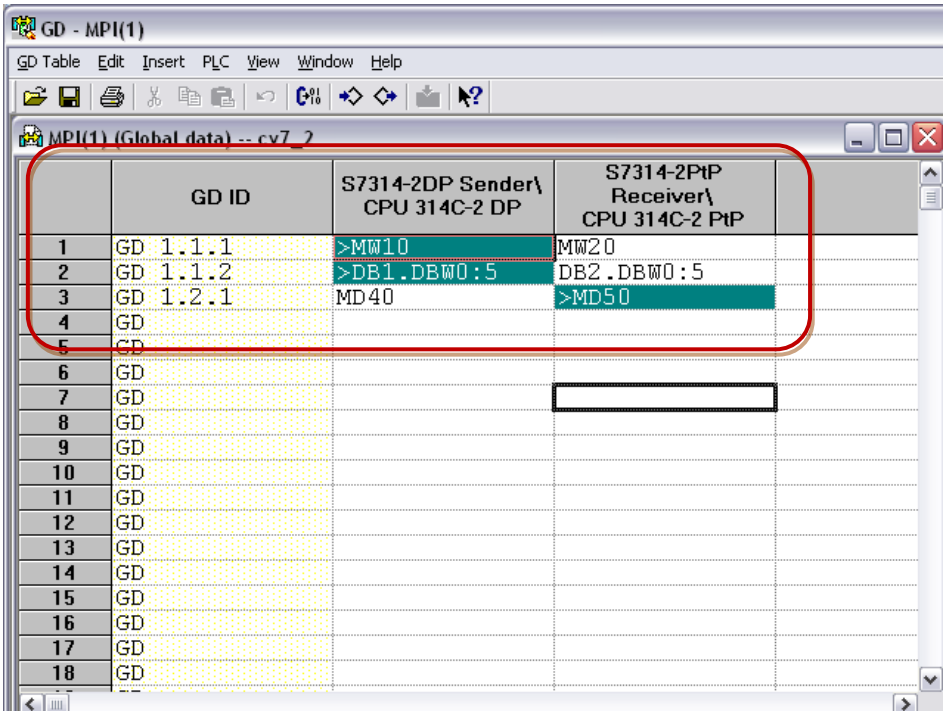


Obr. 7.10 Konečný výběr CPU projektu

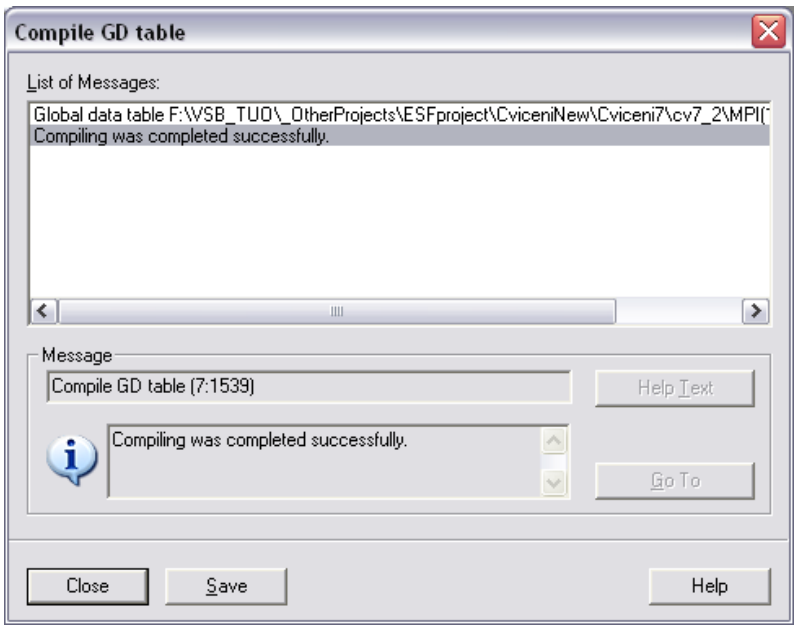
Dále přistoupíme k definování globálních dat. Pro určení globálních dat se nepoužívají symboly, ale pouze fyzické adresy.

V prvním řádku sloupce prvního CPU a druhého CPU definujeme oblast paměti globálních dat (obr. 7.11). V tomto případě MW10 u prvního CPU a MW20 u druhého CPU. Dále je nutno upozornit na tři tlačítka v nabídce pod menu: „Compile“, „Select as receiver“, „Select as sender“. Standardně jsou ihned po zapsání oblasti dat všechny datové buňky označeny jako „Select as receiver“. Proto datovou buňku prvního CPU označíme jako „Select as sender“, to znamená, že MW10 z prvního CPU se bude přenášet na cyklicky na MW20 druhého CPU. Stejný postup pak provedeme pro MD40 prvního CPU a MD50 druhého CPU s tím rozdílem, že jako vysílač slouží nyní druhé CPU. Poslední oblastí globálních dat je prvních deset paměťových buněk typu WORD datového bloku DB1 u prvního CPU a prvních deset paměťových buněk typu WORD datovém bloku DB2 druhého CPU, kde první CPU je vysílač. Povšimněte si automaticky generovaného GD ID v každém sloupci nakonfigurovaných globálních dat. Po konečné konfiguraci globálních dat se musí nastavení zkompilovat pomocí tlačítka „Compile“. Příklad výsledku kompilace je uveden na obr. 7.12.

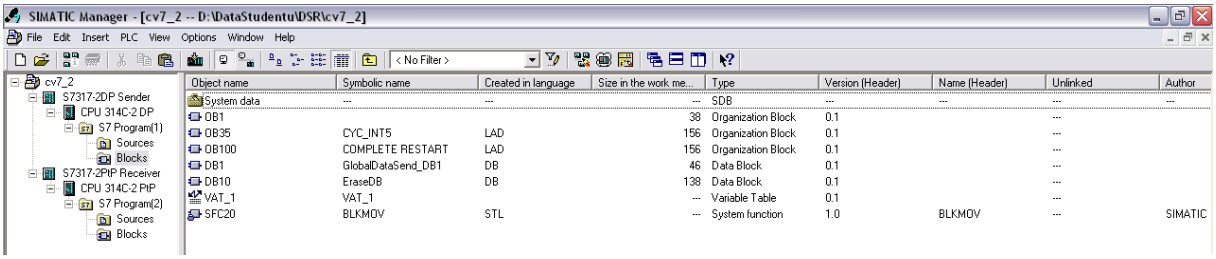
Každý sloupec tabulky je tedy přiřazen jednomu CPU projektu. Maximálně lze použít až 15 CPU projektu. Vždy musí být právě jedna buňka v řádku konfigurována jako „Sender“, ostatní vyplněné jsou pak automaticky jako „Receiver“. Vložení větší oblasti dat (více dat stejného datového typu), lze stejně jako je ukázáno u použitého datového bloku přes dvojtečku – například IW4:3 znamená: 3 wordy od adresy IW4. Pokud chceme adresy v řádcích později editovat, stiskneme F2 tlačítko a editace je umožněna.



Obr. 7.11 Vložení globálních dat

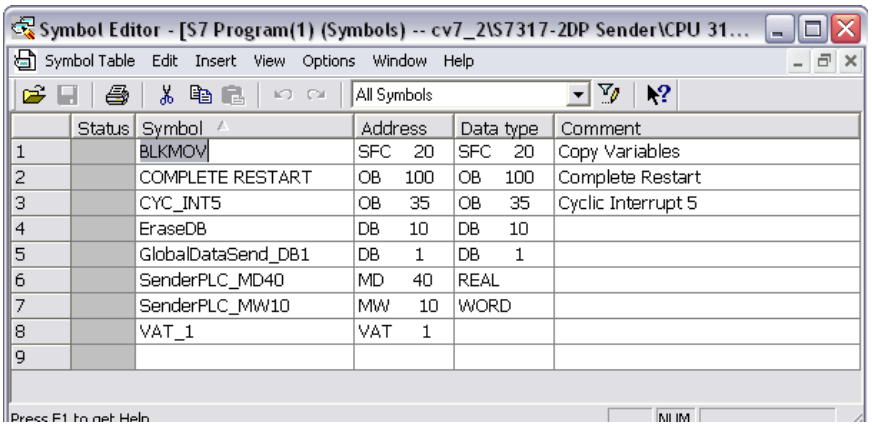


Obr. 7.12 Výsledek kompilace tabulky globálních dat

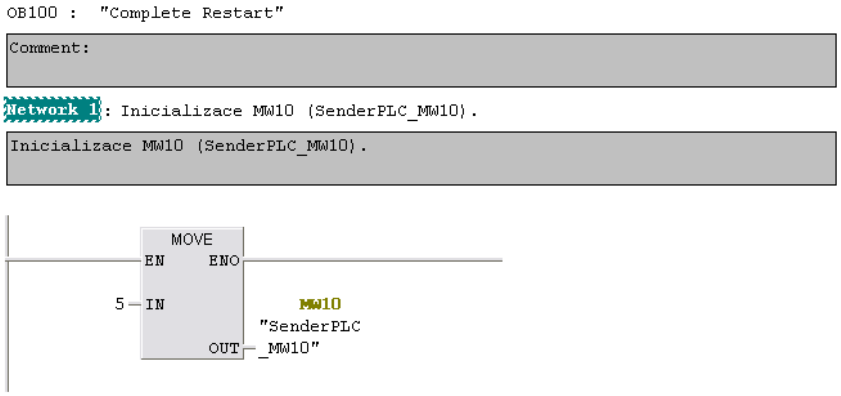


Program v LAD

PLC1:

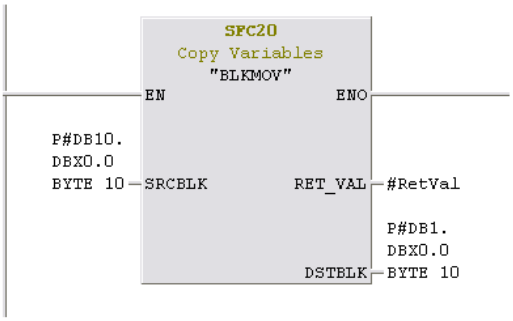


OB100:



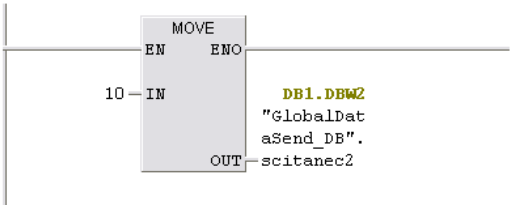
Network 2 : Pomoci DB10 vymaz vsechny hodnoty vsech promennych v DB1.

Pomoci DB10 vymaz vsechny hodnoty vsech promennych v DB1.



Network 3 : Inicializuj scitanec2.

Inicializuj scitanec2.



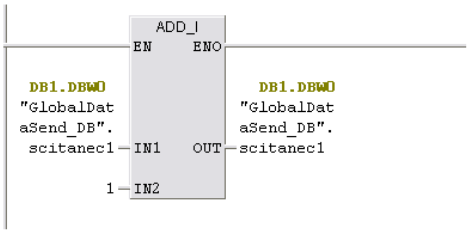
OB35:

OB35 : Block Call Timer-Controlled Every 100 ms

OB35 je volán každých 100ms.

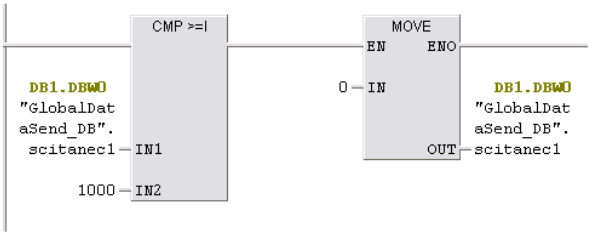
Network 1: Použití komunikace po MPI: Global data.

DB1.DBW0 je globální komunikační proměnná. DB1.DBW0 (SenderPLC_MW10) je co 100ms inkrementován o hodnotu jedna.



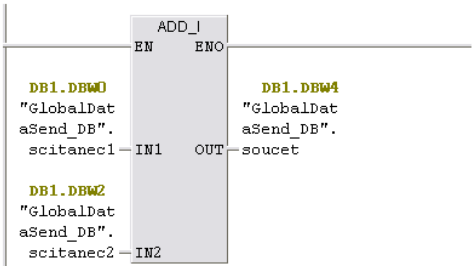
Network 2: Použití komunikace po MPI: Global data.

Když je hodnota DB1.DBW0 větší nebo rovna 1000, tak se vynuluje.



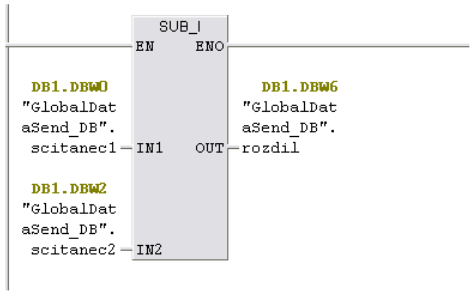
Network 3: DB1.DBW4 je globalni komunikacni promenna.

DB1.DBW4 je globalni komunikacni promenna - soucet db1.dbw0 a db1.dbw2.



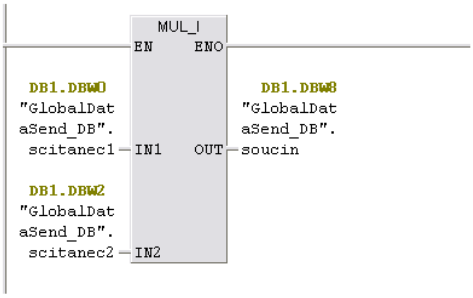
Network 4: DB1.DBW6 je globalni komunikacni promenna.

DB1.DBW6 je globalni komunikacni promenna - rozdil db1.dbw0 a db1.dbw2.

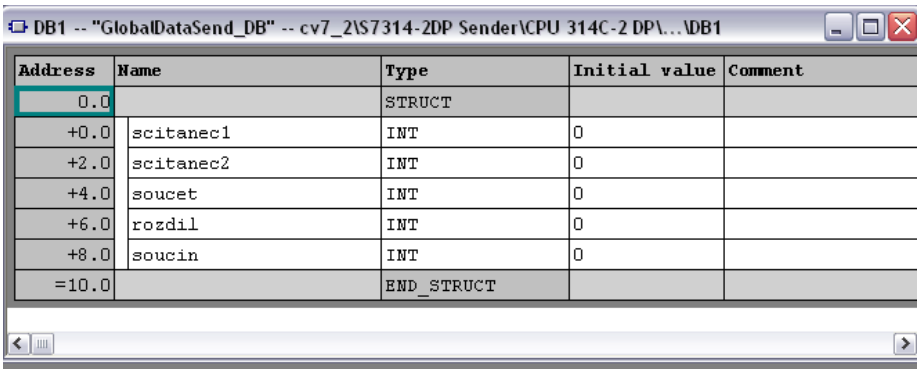


Network 5 : DB1.DBW8 je globalni komunikacni promenna.

```
DB1.DBW8 je globalni komunikacni promenna - soucin db1.dbw0 a db1.dbw2.
```



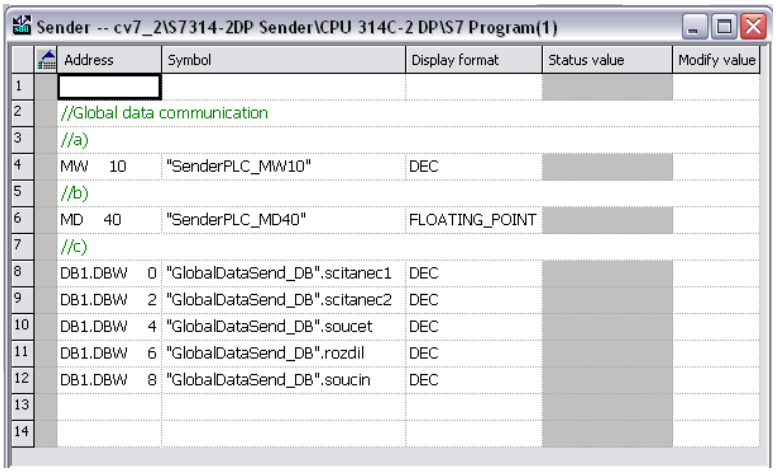
DB1:



DB1 -- "GlobalDataSend_DB" -- cv7_2\S7314-2DP Sender\CPU 314C-2 DP\...\DB1

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	scitanec1	INT	0	
+2.0	scitanec2	INT	0	
+4.0	soucet	INT	0	
+6.0	rozdil	INT	0	
+8.0	soucin	INT	0	
=10.0		END_STRUCT		

VAT tabulka:



Sender -- cv7_2\S7314-2DP Sender\CPU 314C-2 DP\S7 Program(1)

	Address	Symbol	Display format	Status value	Modify value
1					
2	//Global data communication				
3	//a)				
4	MW 10	"SenderPLC_MW10"	DEC		
5	//b)				
6	MD 40	"SenderPLC_MD40"	FLOATING_POINT		
7	//c)				
8	DB1.DBW 0	"GlobalDataSend_DB".scitanec1	DEC		
9	DB1.DBW 2	"GlobalDataSend_DB".scitanec2	DEC		
10	DB1.DBW 4	"GlobalDataSend_DB".soucet	DEC		
11	DB1.DBW 6	"GlobalDataSend_DB".rozdil	DEC		
12	DB1.DBW 8	"GlobalDataSend_DB".soucin	DEC		
13					
14					

PLC2:

S7 Program(2) (Symbols) -- cv7_2\S7314-2PtP Receiver\CPU 314C-2 ...

	Status	Symbol	Addres	Data type	Comment
1		GlobalDataReceiv...	DB 2	DB 2	
2		EraseDB	DB 10	DB 10	
3		ReceiverPLC_MD50	MD 50	REAL	
4		ReceiverPLC_MW20	MW 20	WORD	
5		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
6		COMPLETE REST...	OB 100	OB 100	Complete Restart
7		BLKMOV	SFC 20	SFC 20	Copy Variables
8		Receiver	VAT 1		
9					

OB100:

```
OB100 :  "Complete Restart"
Comment:

Network 1: Inicializace MD50.
Inicializace MD50.

                MOVE
               EN  ENO
5.000000e+
      002 -IN
                   OUT-MD50
                       "ReceiverP
                       LC_MD50"

Network 2: Pomoci DB10 vymaz vsechny hodnoty vsech promennych v DB2.
Pomoci DB10 vymaz vsechny hodnoty vsech promennych v DB2.

                SFC20
              Copy Variables
                "BLKMOV"
               EN          ENO
  P#DB10.
  DBX0.0
  BYTE 10 -SRCBLK    RET_VAL-#RetVal
                             P#DB2.
                             DBX0.0
                    DSTBLK-BYTE 10
```

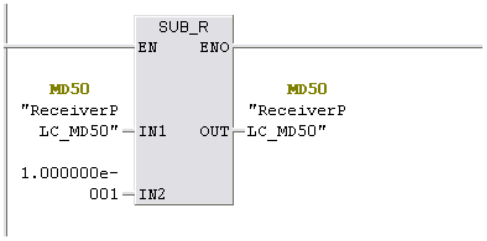
OB35:

OB35 : Call Every 100 ms

OB35 je volán každých 100ms.

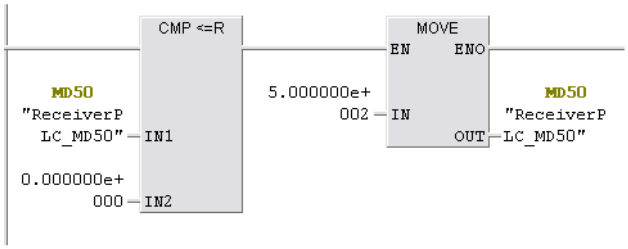
Network 1: Kazdych 100ms dekrementuj hodnotu MD50 o 0.1.

Kazdych 100ms dekrementuj hodnotu MD50 o 0.1.



Network 2 : Pokud je hodnota MD50 mensi nebo rovna 0, pak do ni dej 500.

Pokud je hodnota MD50 mensi nebo rovna 0, pak do ni dej 500.

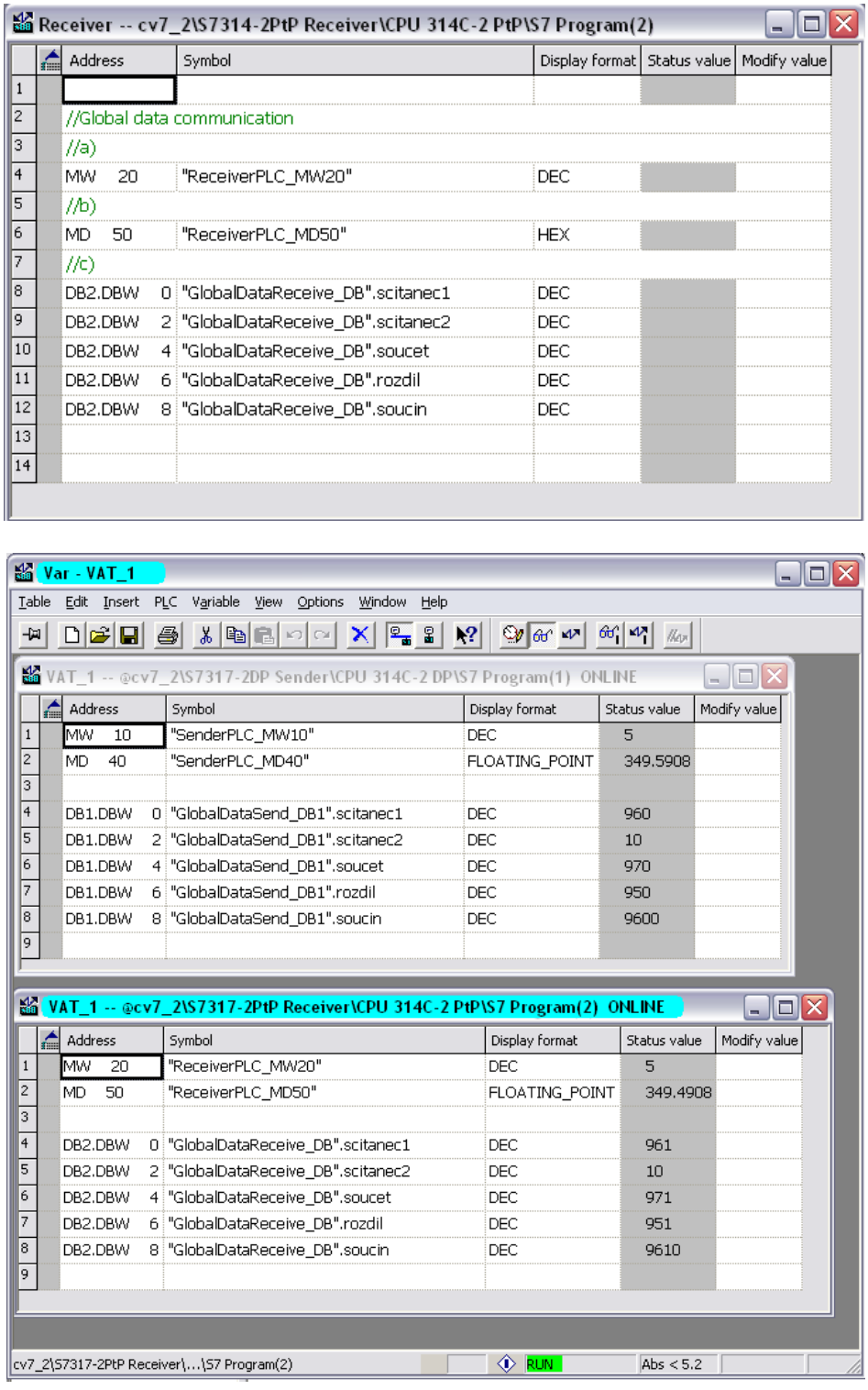


DB2:

DB2 -- "GlobalDataReceive_DB" -- cv7_2\S7314-2PtP Receiver\CPU 314C-2 PtP\...\DB2

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	scitanec1	INT	0	
+2.0	scitanec2	INT	0	
+4.0	soucet	INT	0	
+6.0	rozdil	INT	0	
+8.0	soucin	INT	0	
=10.0		END_STRUCT		

VAT tabulka:



Receiver -- cv7_2\S7314-2PtP Receiver\CPU 314C-2 PtP\S7 Program(2)

	Address	Symbol	Display format	Status value	Modify value
1					
2	//Global data communication				
3	//a)				
4	MW 20	"ReceiverPLC_MW20"	DEC		
5	//b)				
6	MD 50	"ReceiverPLC_MD50"	HEX		
7	//c)				
8	DB2.DBW 0	"GlobalDataReceive_DB".scitanec1	DEC		
9	DB2.DBW 2	"GlobalDataReceive_DB".scitanec2	DEC		
10	DB2.DBW 4	"GlobalDataReceive_DB".soucet	DEC		
11	DB2.DBW 6	"GlobalDataReceive_DB".rozdil	DEC		
12	DB2.DBW 8	"GlobalDataReceive_DB".soucin	DEC		
13					
14					

Var - VAT_1

Table Edit Insert PLC Variable View Options Window Help

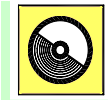
VAT_1 -- @cv7_2\S7317-2DP Sender\CPU 314C-2 DP\S7 Program(1) ONLINE

	Address	Symbol	Display format	Status value	Modify value
1	MW 10	"SenderPLC_MW10"	DEC	5	
2	MD 40	"SenderPLC_MD40"	FLOATING_POINT	349.5908	
3					
4	DB1.DBW 0	"GlobalDataSend_DB1".scitanec1	DEC	960	
5	DB1.DBW 2	"GlobalDataSend_DB1".scitanec2	DEC	10	
6	DB1.DBW 4	"GlobalDataSend_DB1".soucet	DEC	970	
7	DB1.DBW 6	"GlobalDataSend_DB1".rozdil	DEC	950	
8	DB1.DBW 8	"GlobalDataSend_DB1".soucin	DEC	9600	
9					

VAT_1 -- @cv7_2\S7317-2PtP Receiver\CPU 314C-2 PtP\S7 Program(2) ONLINE

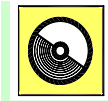
	Address	Symbol	Display format	Status value	Modify value
1	MW 20	"ReceiverPLC_MW20"	DEC	5	
2	MD 50	"ReceiverPLC_MD50"	FLOATING_POINT	349.4908	
3					
4	DB2.DBW 0	"GlobalDataReceive_DB".scitanec1	DEC	961	
5	DB2.DBW 2	"GlobalDataReceive_DB".scitanec2	DEC	10	
6	DB2.DBW 4	"GlobalDataReceive_DB".soucet	DEC	971	
7	DB2.DBW 6	"GlobalDataReceive_DB".rozdil	DEC	951	
8	DB2.DBW 8	"GlobalDataReceive_DB".soucin	DEC	9610	
9					

cv7_2\S7317-2PtP Receiver\...\S7 Program(2) RUN Abs < 5.2



DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI7\



DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI7\

8. PROFIBUS

Čas ke studiu: 3 hodiny

Cíl Po prostudování této kapitoly budete umět

- Popsat základní vlastnosti sběrnice Profibus.
- Popsat varianty typy sběrnice Profibus.
- Popsat vlastnosti sběrnice Profibus DP.
- Popsat vlastnosti sběrnice Profibus PA.
- Praktická výuka je zaměřena na komunikaci po MPI u programovatelného automatu Simatic S7 300, komunikace pomocí funkcí GET, PUT, SEND a RECEIVE.

Výklad

8.1. Profibus

Průmyslová komunikační síť Profibus představuje v současné době jeden z velmi rozšířených komunikačních standardů v oblasti promyslové automatizace. Vychází z otevřeného komunikačního modelu ISO/OSI a je určena pro všechny oblasti automatizace, tj. řízení technologií, řízení procesů a automatizaci budov. Historie sítě Profibus spadá do poloviny 80. let, kdy se firmy Bosch, Klockner & Moller a Siemens dohodly na společném projektu pro vývoj promyslové sběrnice označené jako Profibus (PROces Field BUS). Cílem bylo vytvořit architekturu komunikačního systému, který by na jedné straně respektoval potřebu připojit na sběrnici malá zařízení a současně vytvořil otevřené rozhraní pro komunikaci různých automatizačních zařízení (programovatelné automaty, operátorské panely, snímače, akční členy atd.). Norma Profibus je nezávislá na výrobci a její otevřenost je garantována normou EN 50170. Komunikační systém Profibus je rovněž zakotven v mezinárodních standardech IEC61158 a IEC61784 [1].

Profibus je otevřený, digitální komunikační systém pro širokou řadu aplikací, zvláště při řízení technologických procesů. Je vhodný pro rychlé (časově kritické) aplikace i pro komplexní komunikační úlohy. Rozšířenost komunikačního systému Profibus je dána hlavně množstvím komponent, se kterými je možno pomocí Profibusu komunikovat a které vyrábí velké množství výrobců.

Architektura systému Profibus

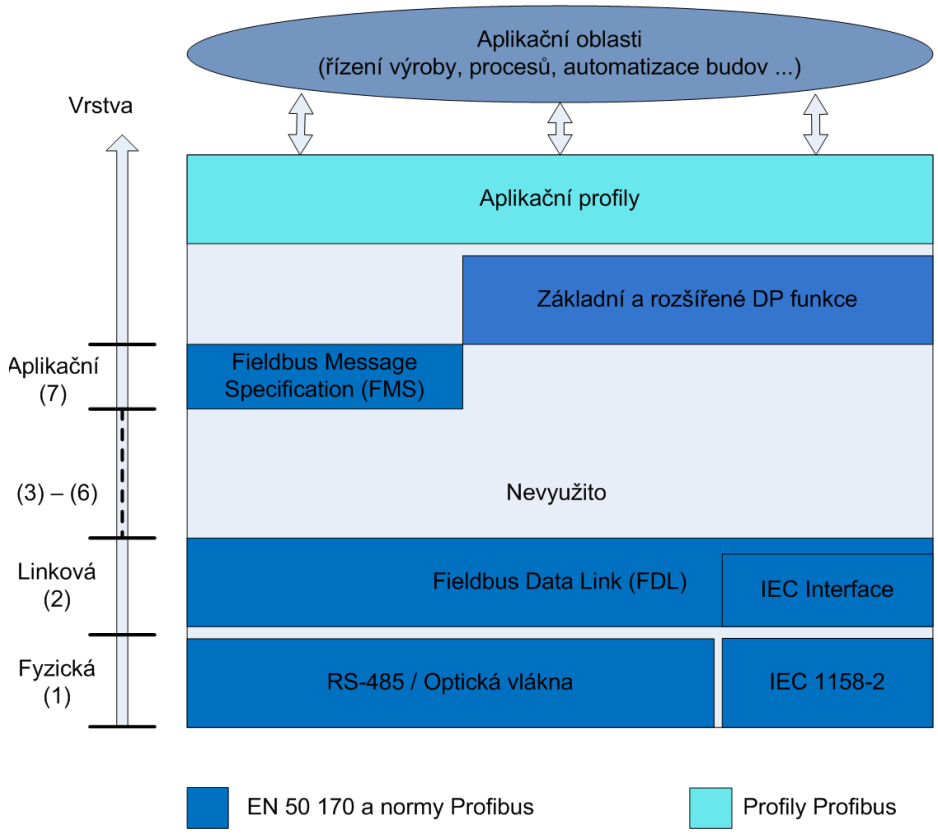
Norma Profibus vyšla z modelu ISO/OSI. Z důvodu časové optimalizace definuje z tohoto modelu pouze vrstvy fyzickou, linkovou a aplikační:

- Fyzická vrstva definuje fyzické spojení mezi zařízeními včetně mechanických a elektrických vlastností tohoto spojení a současně je v této vrstvě definována topologie sítě; Profibus podporuje přenos po sběrnici RS-485, optickém vláknu a pro výbušné prostředí po proudové smyčce IEC 1158-2.

- Linková vrstva (Fieldbus Data Link) definuje mechanismus přístupu účastníka na přenosové médium (token passing, master-slave) a zabezpečuje tvorbu zprávy na úrovni bitového řetězce včetně generování kontrolních částí.
- Aplikační vrstva je nejvyšší vrstvou v referenčním modelu ISO/OSI, poskytuje jednotlivé služby nezbytné pro realizaci komunikace z hlediska uživatele.

Pro každou oblast automatizace existují určité požadavky na vlastnosti komunikační sítě. Tyto požadavky jsou shrnuty v tzv. profilech zařízení definovaných nad aplikační vrstvou pro každý typ protokolu. V současné době existují tři varianty komunikačního standardu Profibus [1]:

- Profibus-DP -komunikační síť pro rychlou komunikaci typu master-slave. Uživatelská vrstva nabízí jednoduché funkce pro komunikaci, konfigurování a řízení provozu na síti. Komunikačním médiem je buď kroucená dvojlinka (standard RS-485), nebo optické vlákno. Tato komunikační síť je nasazována na nižší systémové úrovni ke komunikaci s distribuovanými zařízeními, kde jsou kladeny vysoké nároky na rychlost přenosu a dobu odezvy, nejsou však zapotřebí složité komunikační funkce.
- Profibus-FMS -nabízí komunikační standard pro komunikaci v heterogenním prostředí a s velkou množinou služeb pro práci s daty, programy a alarmy. Komunikačním médiem je podobně jako u varianty Profibus-DP buď kroucená dvojlinka (standard RS-485), nebo optické vlákno. Je určen pro komunikaci na vyšší úrovni řízení. Na této úrovni mezi sebou komunikují řídicí systémy (PLC, NC) a systémy vizualizace a sběru dat (operátorské panely, PC). Cílem této komunikační sítě není dosažení minimální doby reakce, ale především komunikace v heterogenním prostředí (komunikace v prostředí různých výrobců). Dnes už se v nových aplikacích nenasazuje, je nahrazen Ethernetem.
- Profibus-PA -používá rozšířenou normu Profibus-DP a je určen pro sběr dat ze snímačů v automatizaci procesů (tlak, teplota apod.). Aby bylo možné síť využít také v prostředí s nebezpečím výbuchu a tím aby vyhovovala požadavkům na jiskrovou bezpečnost, je použita i speciální fyzická vrstva - proudová smyčka podle standardu IEC 1158-2.



Obr. 8.1 Architektura Profubusu (upraveno z [1]).

Fyzická vrstva sběrnice Profibus

Vlastnosti fyzické vrstvy komunikačního systému bývají nezřídka určující pro oblast použití té které komunikační sítě. Mimo obecných parametrů (bezpečnost přenosu, přenosová rychlost či maximální rozlehlost sítě) je zajímavá i jednoduchost instalace, cena, popř. realizace některých speciálních požadavků (napájení zařízení prostřednictvím komunikačního kabelu atd.). Protože je nemožné vyhovět současně všem požadavkům uživatelů, nabízí standard Profibus použití následujících tří variant fyzické vrstvy [1]:

- Sběrnici RS-485 pro DP a FMS.
- Smyčku podle IEC 1158-2 pro PA.
- Optické vlákno (FO).

Přenosová cesta na bázi sběrnice RS-485

Nejčastěji používanou variantou přenosové vrstvy sítě Profibus je rozdílová napěťová sběrnice podle standardu RS-485 (v souvislosti se sítí Profibus se též můžeme setkat s označením H2). Aplikační oblast této varianty tvoří instalace Profibus-DP nebo FMS s požadavkem na jednoduchou, levnou síť s velkou přenosovou rychlostí. Pro RS-485 je použito stíněného kabelu s jedním měděným krouceným párem. U instalací, kde lze vyloučit vliv elektromagnetického rušení, je možné použít kabel nestíněný. Doporučené parametry kabelu pro síť Profibus se svými hodnotami včetně zakončení odlišují od standardu RS-485 [1]:

- Impedance: 135 Ω až 165 Ω.
- Kapacita: < 30 pF/m.
- Odpor smyčky: 110 Ω/km.
- Minimální průřez vodiče: > 0,34 mm2.

Co do topologie, jedná se o sběrnicovou (liniovou) strukturu sítě. Povolená délka odbočky je 0,3 m. Na jeden segment sběrnice RS-485 je možné připojit až 32 účastníků sítě Profibus (aktivních, pasivních nebo opakovačů). Pro připojení účastníků na sběrnici je doporučeno použít devítikolíkový konektor D sub. Segment sběrnice musí být na obou svých koncích ukončen sběrnicovým terminátorem. Terminátor obsahuje mimo přizpůsobovacího odporu konce vedení Rt (220 Ω) ještě odpory Rd a Ru (390 Ω), pomocí nichž je definován stav vedení v době, kdy žádné zařízení nevysílá. Pro zajištění správné funkce musí být oba terminátory napájeny. Většina výrobců dodává připojovací síťové konektory pro Profibus s integrovaným odpínatelným terminátorem nebo instalují odpínatelné terminátory přímo do jednotlivých zařízení. Zároveň je velmi výhodné použít konektory, ve kterých je propojen kabel přicházející k zařízení s kabelem vycházejícím ze zařízení. Při použití takovýchto konektoru je možné odpojit a připojit účastnická zařízení bez rozpojování segmentu. Maximální délka segmentu sítě závisí na použité přenosové rychlosti. Závislost je samozřejmě nepřímá, a proto nabízí Profibus v této variantě stupňovitě volitelnou přenosovou rychlost v hodnotách uvedených v Tab. 8.1. To umožňuje téměř vždy na1ézt vhodný kompromis mezi požadovanou rozlehlostí sítě a přenosovou rychlostí. Pokud je třeba připojit větší počet účastníků než 32 nebo je třeba zvětšit rozlehlost sítě při zachování přenosové rychlosti, je nutné pokračovat dalším segmentem.

Tab. 8.1 Závislost maximální délky vedení na přenosové rychlosti u komunikační sběrnice Profibus

Přenosová rychlost v kb/s	9,6	19,2	45,45	93,75	187,5	500	1500	3000	6000	12000
Maximální délka vedení v m	1200	1200	1200	1200	1000	400	200	100	100	100

K propojování segmentů slouží opakovače (repeater). Opakovač galvanicky odděluje segmenty a regeneruje signál procházející opakovačem z jednoho segmentu do druhého. Pomocí opakovačů je možné realizovat jak sériové řazení segmentů, tak i odbočení. Jediným hlediskem pro spojování segmentů je čas potřebný pro přenos signálu mezi nejvzdálenějšími stanicemi. V praxi se sériově řadí maximálně 10 segmentů. Celkově však nesmí být překročen maximální počet účastníků připojených k jedné síti daný adresovacími možnostmi standardu Profibus, tj. 127 účastníků (aktivních nebo pasivních).

Přenosová cesta na bázi sběrnice IEC 1158-2 pro Profibus-PA

Sběrnice podle standardu IEC 1158-2 splňující požadavky aplikací v chemickém a petrochemickém průmyslu nese někdy označení H1 (neplést se starším označením sítě Industrial Ethernet firmy Siemens -SINEC H1). Tato varianta zaručuje tzv. jiskrovou bezpečnost a zároveň podporuje napájení zařízení po sběrnicovém kabelu. Proto se předpokládá použití převážně ve výbušných prostředích. Jako komunikační médium se pro tuto fyzickou vrstvu používá kabel s jedním měděným krouceným párem (stíněným nebo nestíněným) s následujícími doporučenými vlastnostmi [1]:

- Impedance při 31,25 kHz: 100 Ω ±20 %.
- Kapacitní nesouměrnost: < 2 nF/km.
- Odpor smyčky: 44 Ω/km.
- Minimální průřez vodiče: > 0,88 mm2.
- Útlum při 39 kHz: 3 dB/km.

Přenos dat je zde založen na následujících principech:

- Každý segment má pouze jeden zdroj proudu.
- Při vysílání nedodává zařízení do sítě žádný proud.
- V klidovém stavu odebírá každé zařízení konstantní proud.
- Každé účastnické zařízení pracuje jako pasivní proudový spotřebič.
- Segment je na obou koncích zakončen pasivním terminátorem.

Pro modulaci se předpokládá klidový proud minimálně 10mA pro napájení každého zařízení na síti. Logické úrovně komunikačního signálu jsou generovány vysílajícím zařízením modulací ±9mA ke klidovému proudu. U této varianty fyzické vrstvy je použito synchronního bitově orientovaného protokolu s přenosovou rychlostí pevně nastavenou na 31,25 kHz.

Přenos optickým vláknem - FO

Světlovody se v instalacích sítě Profibus používají pro aplikace v prostředí s vysokou úrovní elektromagnetického rušení a zároveň umožňují zvětšit maximální vzdálenosti pro velké přenosové rychlosti. Pro přenos optickým vláknem jsou používány jak levné plastové (délka až 50 m), tak i skleněné (délka až 2 km) světlovodné kabely. Existují však i varianty pro skleněné světlovody s délkou 15 km. Většina výrobců dodává speciální konektory s integrovaným převodníkem RS-485 na optické rozhraní a opačně. To umožňuje jednoduše kombinovat metalický a optický rozvod v jedné síti.

8.2. Linková vrstva - přístup na sběrnici

Druhá vrstva referenčního modelu ISOIOSI, linková, zabezpečuje mimo služeb pro blokový přenos dat především řízení přístupu na sběrnici. U standardu Profibus se tato vrstva nazývá Fieldbus Data Link (FDL) a je nejnižší vrstvou, ke které je v některých speciálních případech realizován přístup aplikačních programů [1].

Metoda řízení přístupu na sběrnici stanovuje, kdy je zařízení oprávněno vysílat na sběrnici. Musí být zajištěno, že v danou chvíli má právo na vysílání dat pouze jedno zařízení. Metoda řízení přístupu na sběrnici použitá u sítě Profibus byla navržena tak, aby uspokojovala následující dva požadavky:

- Pro komunikaci mezi složitějšími automatizačními zařízeními musí být zajištěno, že každému z těchto zařízení je přidělován dostatečný prostor na provádění jeho komunikačních úloh.
- Pro komunikaci mezi automatizačním zařízením a jemu přiřazenými jednoduchými vstupně/výstupními zařízeními je třeba zajistit co nejjednodušší a nejrychlejší cyklickou výměnu dat.

Proto v sobě Profibus kombinuje dvě základní metody řízení přístupu na sběrnici: metodu token passing (předávání pověření v logickém kruhu) pro komunikaci mezi aktivními zařízeními a metodu master-slave (centrálně řízené dotazování) pro komunikaci mezi aktivním a jemu přidělenými pasivními zařízeními. Pak je možné implementovat jak konfigurace používající pouze jednu z metod, tak i konfigurace s tzv. hybridním řízením přístupu na sběrnici (kombinace obou metod).

Protože metoda token passing patří k decentralizovaným metodám řízení přístupu na sběrnici, musí každé aktivní zařízení připojené na sběrnici realizovat mechanismus předávání pověření k přístupu na sběrnici. Jedním ze základních požadavků kladených na průmyslové komunikační sběrnice je možnost připojovat a odpojovat jednotlivé účastníky ke sběrnici, aniž by to mělo vliv na činnost

ostatních zařízení. Proto nemůže uvedený mechanismus vycházet ze statických dat. Logický kruh, ve kterém dochází k předávání pověření, je tvořen aktivními stanicemi uspořádanými vzestupně podle jejich adresy. V ustáleném stavu zná tedy každá stanice v logickém kruhu svého předchůdce, od kterého dostane pověření (token) a svého následníka, kterému pověření zasílá.

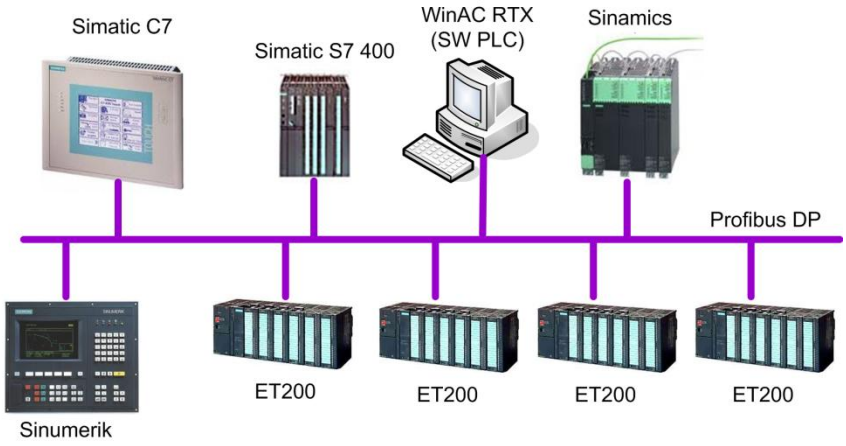
Typické pro deterministické metody přidělování přístupu na sběrnici, k nimž token passing patří, je existence parametru definujícího maximální dobu, za níž každá stanice získá právo vysílat. U standardu Profibus je to právě žádaná doba oběhu pověření označovaná TTR (Target Rotation Time). Měření skutečné doby oběhu pověření TRR (Real Rotation Time) provádí každá aktivní stanice zařazená do logického kruhu, která v době, kdy vlastní pověření, porovnává doby, TTR a TRR. Pokud je TRR menší než TTR realizuje stanice své komunikační požadavky v pořadí, v jakém vznikly a s ohledem na jejich prioritu. Pokud nemá žádné další požadavky nebo hodnota TRR dosáhla hodnoty TTR, odešle stanice pověření svému následníkovi v logickém kruhu a vynuluje časovač pro měření doby TRR. V případě, že by došlo k situaci, kdy v době přijetí pověření stanicí bude hodnota TRR větší než TTR, má stanice právo odvysílat jednu zprávu s vysokou prioritou. Za účelem detekce nově připojených zařízení prohledává každé zařízení v rámci tzv. režijních činností na sběrnici adresní prostor.

Adresní prostor zařízení v logickém kruhu, za který je dané zařízení "zodpovědné", začíná adresou o jedničku větší než vlastní adresa zařízení a končí adresou o jedničku menší, než je adresa jeho následníka v kruhu. Adresní prostor je uzavřen tak, že se po adrese 126 pokračuje adresou 0. Parametrem zvaným GAP-Factor je možné specifikovat, jak často se má adresní prostor prohledávat. Protože prohledávání adresního prostoru patří k časově nejnáročnějším akcím (je prováděno pokusem o získání tzv. statusu stanice FDL), je možné adresní prostor shora omezit hodnotou parametru HSA (Highest Station Address). V případě odpojení zařízení nepřijde potvrzení o přijetí pověření následníkem a pověření je zasláno dalšímu nalezenému zařízení. Zároveň jsou připraveny mechanismy reagující na ztrátu pověření apod.

8.3. Profibus-DP

Protokol Profibus-DP je navržen pro rychlou cyklickou výměnu dat na nejnižší (technologické) úrovni komunikačního modelu CIM, tzn. pro komunikaci mezi programovatelnými řídicími automaty a jejich decentralizovanými vstupy a výstupy (v/v).

Jedním ze speciálních požadavků kladených na komunikační systémy pro tuto úroveň řízení je zaručit kratší komunikační cyklus, než je cyklus zpracování řídicího algoritmu programovatelným automatem tak, aby nedocházelo ke zpoždění vlivem komunikace. Výměna dat probíhá mezi programovatelným automatem (řídicí, nadřízené zařízení -master) a jednotlivými v/v zařízeními (řízenými -slave) cyklicky. Avšak pro speciální účely (náběh komunikace, konfigurování zařízení, diagnostika atd.) jsou k dispozici acyklické služby. Typická architektura řídicího systému se sběrnicí Profibus DP je uvedena na obr. 8.2.



Obr. 8.2 Typická architektura řídicího systému se sběrnicí Profibus DP.

Typy zařízení a konfigurace systému

Zařízení podporující komunikaci Profibus-DP je možné rozdělit do následujících tří skupin [1]:

- DP Master Class 1 (DPM1) - řídicí zařízení realizující cyklickou komunikaci s podřízenými zařízeními: nejčastěji realizováno pomocí programovatelného automatu (Programmable Logic Controller -PLC), počítače PC atd.
- DP Master Class 2 (DPM2) - řídicí zařízení pro realizaci diagnostických a monitorovacích funkcí používaných při uvádění sítí Profibus-DP do provozu nebo při provozu pro monitorovací účely.
- DP Slave - periferní zařízení (v/v zařízení, pohony, ventily, operátorské panely atp.) získávající vstupní data pro řídicí zařízení a poskytující výstupní data od řídicího zařízení (množství vstupních a výstupních dat závisí na typu zařízení: maximálně může zařízení poskytovat 246 bajtů vstupních dat a požadovat 256 bajtů výstupních dat).

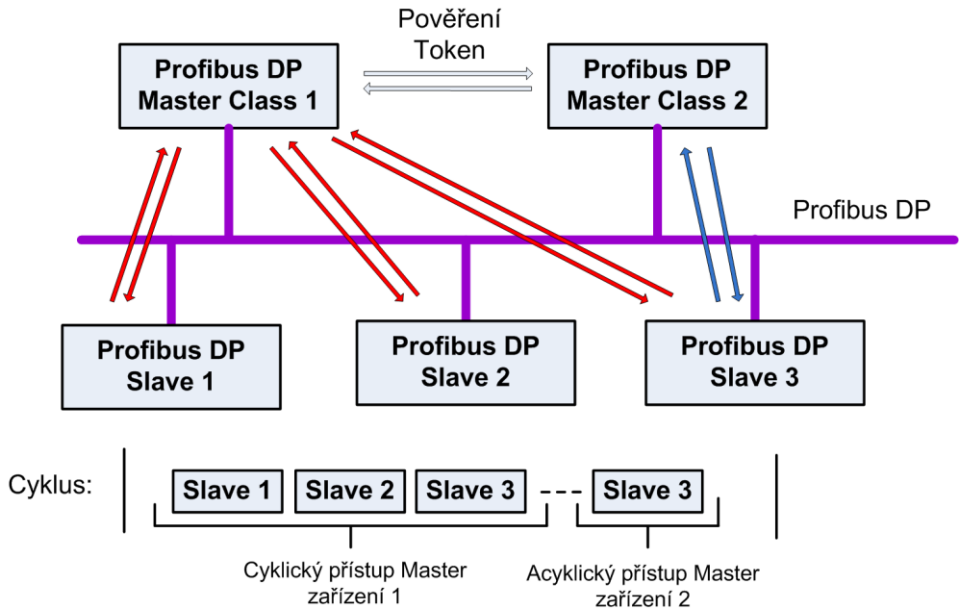
Z hlediska konfigurace sítě je možné provozovat konfiguraci buď monomaster, nebo multimaster. V konfiguraci monomaster je na sběrnici pouze jedno aktivní zařízení typu DPM1. Komunikace mezi tímto zařízením a pasivními zařízeními typu DP Slave je realizována metodou master-slave. Toto řešení zaručuje nejkratší doby trvání komunikačního cyklu. Při konfiguraci multimaster se na sběrnici nachází několik aktivních řídicích zařízení. Potom můžeme na celý systém pohlížet jako na několik podsystémů vždy s jedním DPM1 zařízením, jemu přidělenými zařízeními DP Slave a případné diagnostické zařízení typu DPM2. Norma samozřejmě připouští i sdílení zařízení typu DP Slave několika řídicími zařízeními, ale pouze v případě vstupních zařízení typu DP Slave. Možnost zapisovat na výstupy má pouze zařízení DPM1, které konfigurovalo dané výstupní zařízení DP Slave. Mezi jednotlivými řídicími zařízeními dochází k předávání pověření k přístupu na sběrnici metodou token passing a v době, kdy řídicí zařízení vlastní právo přístupu na sběrnici, realizuje cyklickou výměnu dat se svými zařízeními DP Slave. Tato varianta vykazuje z hlediska jednotlivých podsystémů delší časy komunikačního cyklu.

Verze Profibusu DP

Základní verze Profibusu DP je DP-V0, v současné době jsou již vyvinuty dvě rozšiřující verze DP-V1 a DP-V2 [1].

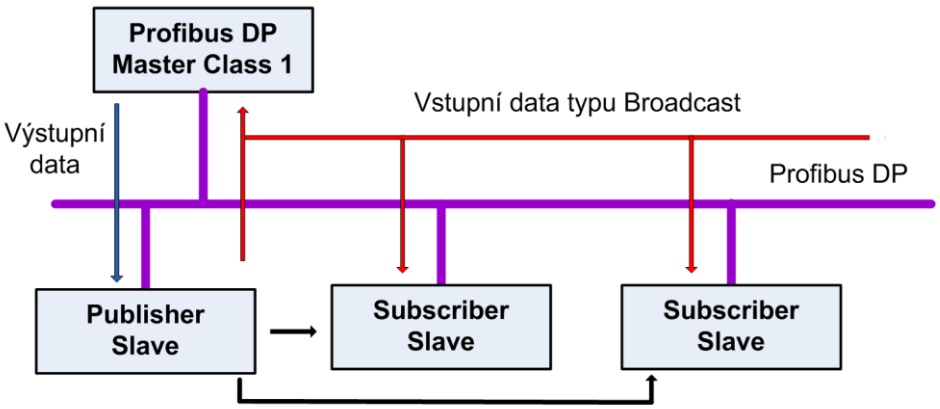
- DP-V0 – Verze DP-V0 poskytuje základní funkčnost DP, cyklickou výměnu dat, diagnostické funkce modulů a kanálu.

– DP-V1 – Verze DP-V1 obsahuje rozšíření směrem k procesní automatizaci. Přináší acyklickou komunikaci pro nastavování parametrů, vizualizaci, alarmy apod., která běží současně s cyklickou komunikací. Umožňuje tím parametrizaci a kalibraci zařízení na komunikační síti při běhu systému.



Obr. 8.3 Acyklická komunikace verze DP-V1 (upraveno z [1]).

– DP-V2 – Verze DP-V2 přináší další rozšíření, které je směřováno primárně do oblasti pohonů. Umožňuje isochronní slave mód a komunikaci slave-slave. Isochronní mód umožňuje časově synchronizované řízení v master a slave zařízeních. Umožněno je tak přesné pozicování s odchylkou měnší než 1 mikrosekunda. Všechna zařízení na síti jsou synchronizována na cyklus master zařízení pomocí globální zprávy typu broadcast. Slave-slave komunikace je přímá a časově úsporná komunikace mezi slave zařízeními prostřednictvím broadcast komunikace. Zpráva nejde přes master, ale vysílá ji tzv. Publisher a přijímá ji tzv. Subscriber. Tato komunikace umožňuje slave zařízením číst data jiného slave zařízení, což může zredukovat čas odezvy sběrnice až o 90%.



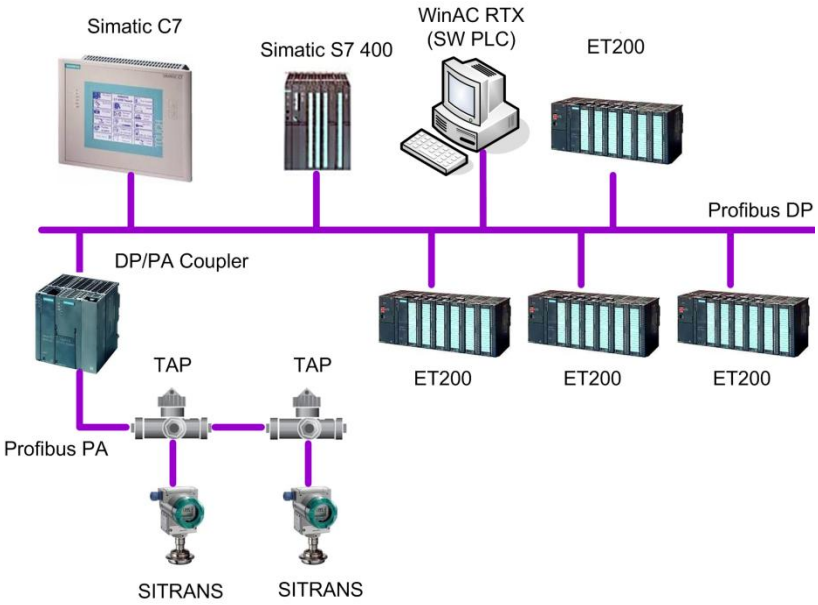
Obr. 8.4 Ukázka komunikace slave-slave (upraveno z [1]).

8.4. Profibus PA

Profibus-PA je navržen pro přístrojovou instrumentaci v bezpečném i nebezpečném prostředí Zóna 0,1 a 2. Profibus PA povoluje pružnou topologii sběrnice s délkou větve do 120m pro výbušná prostředí do 30m. Standardizované funkce Profibus PA přes profily. Profily popisují funkční bloky, zařízení a volitelné parametry. Zařízení s Profibus PA Profil III není jen univerzální, ale také vyměnitelný bez dalších potřebných technických úprav [1].

Až 31 procesních zařízení může být připojeno do každého DP/PA Link. Každý DP/PA Link může číst a psát 244 bytů informací po síti. Teoreticky je možné do jednoho Profibus-DP lze zapojit více než 3800 procesních přístrojů.

Maximální délka Profibus PA při dodržení konfiguračních pravidel je 1900m. Typická architektura řídicího systému se sběrnicí Profibus PA je uvedena na obr. 8.5.



Obr. 8.5 Typická architektura řídicího systému se sběrnicí Profibus PA.

8.5. Profily Profibus

Profily se vztahují ke kontrétnímu typu zařízení (řídicí prvky, aktuátory…) a obsahují vhodné nastavení sběrnice a také specifické aplikace daného zařízení [1].
Dělí se na:

- Obecné aplikační profily. Popisují funkce a vlastnosti společné více aplikacím. Mohou být použity rovněž ve spojení se specifickým aplikačním profilem. Příkladem je například profil PROFIsafe, který poskytuje komplexní, otevřené řešení pro aplikace, které mají vyšší bezpečnostní nároky. Definuje, jakým způsobem jsou fail-safe zařízení (kritický stop, bezpečnostní vypínače..) propojena Profibusem. Snaží se řešit všechny možné chyby, které mohou nastat a narušit komunikaci. Dalším příkladem je profil Hart on Profibus, který vznikl proto, aby mohla být HART zařízení integrována do komunikačního systému Profibus.
- Specifické aplikační profily. Mezi specifické aplikační profily patří například profily PROFIdrive (připojení elektrických pohonů), Encoders (připojení enkodérů),

Dosing/Weighing (připojení zařízení pro dávkování a měření hmostnosti), Panel devices (připojení jednoduchých HMI panelů) a mnoho dalších.

- Master profily. Master profil popisuje jednotlivé třídy master zařízení, kdy každá třída musí podporovat určitou podmnožinu možných funkcí master zařízení (cyklická komunikace, acyklická komunikace, diagnostika, alarmy, řízení času, slave-slave komunikace, isochronní mód, bezpečnost).
- Systémové profily. Systémové profily popisují třídy systémů (včetně mastaer zařízení), možnou funkčnost standardních programových rozhraní (funkční bloky FB podle IEC61131-3) a možnosti integrace (GSD files, …).

Shrnutí pojmů

Profibus DP je komunikační síť pro rychlou komunikaci typu master-slave. Uživatelská vrstva nabízí jednoduché funkce pro komunikaci, konfigurování a řízení provozu na síti. Komunikačním médiem je buď kroucená dvojlinka (standard RS-485), nebo optické vlákno.

Profibus PA používá rozšířenou normu Profibus-DP a je určen pro sběr dat ze snímačů v automatizaci procesů (tlak, teplota apod.). Aby bylo možné síť využít také v prostředí s nebezpečím výbuchu, je použita i speciální fyzická vrstva - proudová smyčka podle standardu IEC 1158-2.

Profibus FMS je určen pro komunikaci na vyšší úrovni řízení. Na této úrovni mezi sebou komunikují řídicí systémy (PLC, NC) a systémy vizualizace a sběru dat (operátorské panely, PC). V současnosti se pro tyto účely používá téměř výhradně Ethernet.

Fyzická vrstva Profibusu je tvořena sběrnicí RS-485 pro DP a FMS, smyčkou podle IEC 1158-2 pro PA nebo optickým vláknem.

Profibus kombinuje dvě základní **metody řízení přístupu na sběrnici** - metodu token passing (předávání pověření v logickém kruhu) pro komunikaci mezi aktivními zařízeními a metodu master-slave (centrálně řízené dotazování) pro komunikaci mezi aktivním a jemu přidělenými pasivními zařízeními.

Otázky

1. Popište architekturu systému Profibus.
2. Popište základní typy systému Profibus.
3. Jaké jsou parametry fyzické vrstvy systému Profibus?
4. Jaké jsou parametry linkové vrstvy systému Profibus?
5. Popište vlastnosti přenosové cesty na bázi sběrnice RS 485.
6. Popište vlastnosti přenosové cesty na bázi sběrnice IEC 1158-2.
7. Popište vlastnosti a použití systému Profibus DP.
8. Jaké metody přístupu ke komunikačnímu médiu se používají u Profibusu DP?

9. Jaké typy zařízení se používají u Profibusu DP?
10. Popište vlastnosti a použití systému Profibus PA.

Použitá literatura a další zdroje

1. Profibus System Description. Profibus Nutzeorgenization, Ocrober 2002.

Řešená úloha 8.1

Zadání: Nastavte komunikaci mezi dvěma PLC (CPU 314C-2DP a CPU 314C-2PtP) po MPI. Pro komunikaci použijte funkce GET a PUT. Adresa PLC CPU 314C-2DP na sběrnici je 6, adresa PLC CPU 314C-2PtP je 9.

Na PLC CPU 314C-2PtP na IB124 připojte přípravek pro simulaci spínání vstupních signálů. Tyto hodnoty pomocí funkce GET vyčítejte v PLC CPU 314C-2DP a zapisujte přímo na výstupy QB124 tohoto PLC.

Z PLC CPU 314C-2PtP zapisujte pomocí funkce PUT paměťovou buňku MW10 do PLC CPU 314C-2DP do oblasti MW20. Hodnotu v paměti MW10 inkrementujte každých 100ms o hodnotu 1. Při dosažení hodnoty 100 ji vynulujte.

Data posílejte v obou případech kontinuálně.

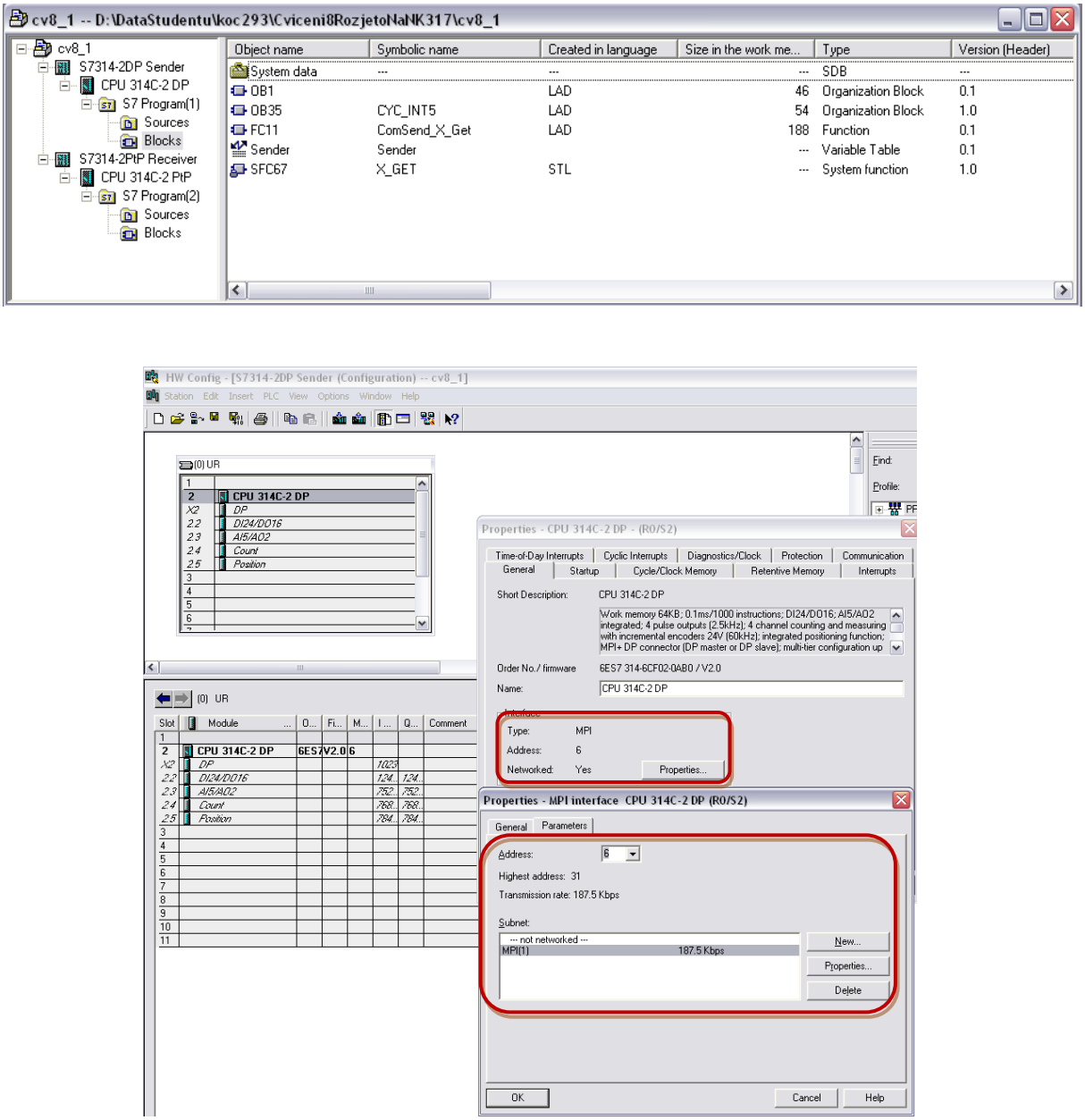
Prvním krokem řešení úlohy je hardwarová konfigurace dvou PLC. Stejně jako v řešené úloze 7.2 v kapitole 7 je pro komunikaci potřeba nastavit každému prvku na sběrnici jinou adresu. CPU 314C-2DP na sběrnici je 6, adresa PLC CPU 314C-2PtP je 9.

Pomocí systémové funkce SFC67 „X_GET“ lze číst data z datové oblasti komunikačního partnera. Žádné odpovídající SFC na straně komunikačního partnera v tomto případě není. Čtení je aktivováno po zavolání SFC s parametrem REQ = 1. Přijímání pokračuje, dokud není indikováno přijetí dat v BUSY = 0 (sestupná hrana). RET_VAL poté obsahuje délku přijatého bloku dat v bytech.

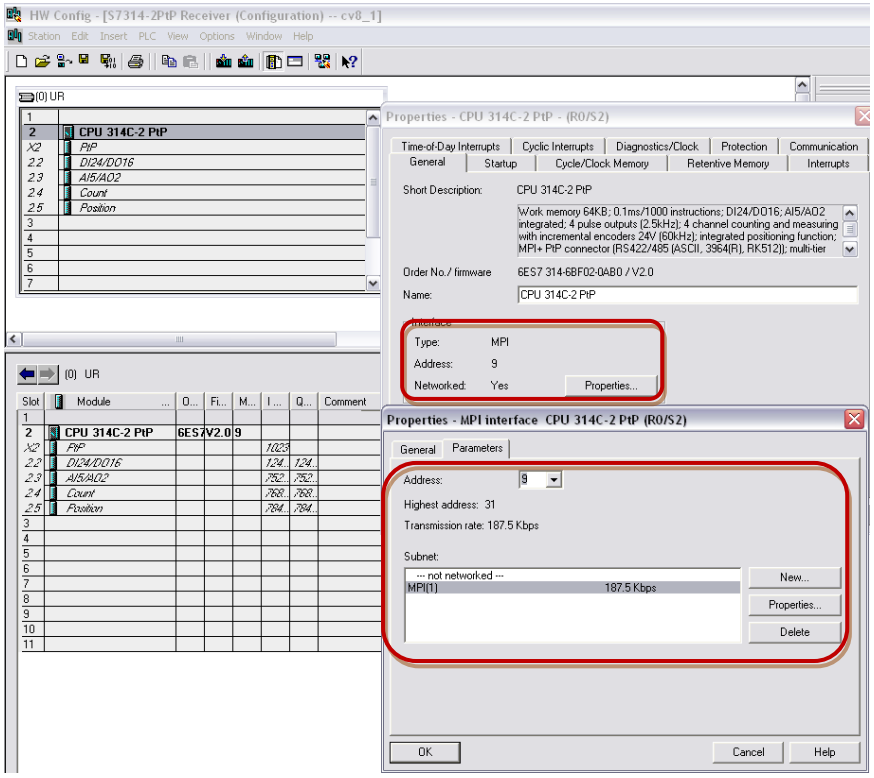
Musí být zajištěno, že přijímací oblast je definována pomocí RD parametru (u přijímacího CPU) a je přinejmenším stejně velká, nebo větší, než čtená oblast definovaná pomocí VAR_ADDR (u komunikačního partnera).

Pomocí systémové funkce SFC68 „X_PUT“ lze zapisovat data do datové oblasti komunikačního partnera. Žádné odpovídající SFC na straně komunikačního partnera v tomto případě není. Zapisování je aktivováno voláním SFC s REQ = 1. Přijímání pokračuje, dokud není indikováno potvrzení přijetí dat v BUSY = 0 (sestupná hrana).

Stejně jako u X_GET musí být zajištěno, že přijímací oblast je definována pomocí SD parametru (u vysílacího CPU) a je přinejmenším stejně velká, nebo větší, než přijímací oblast definovaná pomocí VAR_ADDR (u komunikačního partnera).



Obr. 8.6 Konfigurace MPI.



Obr. 8.7 Konfigurace MPI.

Program v LAD

PLC1: S7314-2DP Sender:

S7 Program(1) (Symbols) -- cv8_1\S7314-2DP Sender\CPU 314C-2 DP

	Status	Symbol	Addres	Data type	Comment
1		ComSend_X_Get	FC 11	FC 11	
2		ContinueX_Get	M 101.2	BOOL	
3		TransferX_Get	M 101.3	BOOL	
4		BusyX_Get	M 101.4	BOOL	
5		BusyX_Get_Nedge	M 101.5	BOOL	
6		X_Get_Cmpltd	M 101.6	BOOL	X Get completed
7		SenderMD20	MD 20	REAL	
8		RetValX_Get	MW 132	INT	
9		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
10		Outputs124thByte	QB 124	BYTE	
11		X_GET	SFC 67	SFC 67	Read Data from a Communication Pa...
12		X_PUT	SFC 68	SFC 68	Write Data to a Communication Partn...
13		Sender	VAT 1		
14					

OB1:

OB1 : "Main Program Sweep (Cycle)"

Comment:

Network 1: Title:

X_Get.

Network 2: Title:

X_Get.

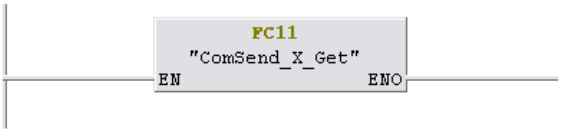
OB35:

OB35 : Block Call Timer-Controlled Every 100 ms

Comment:

Network 1: Title:

Volání funkce FC11.



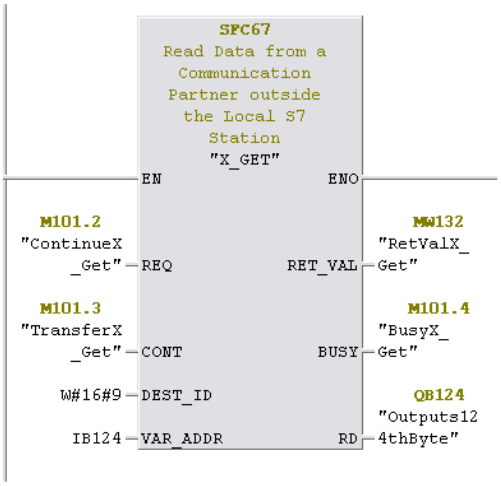
FC11:

FC11 : Title:

```
X_Get funkce.
```

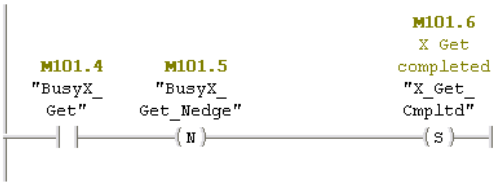
Network 1: Title:

```
Volani systemoveho funkcniho bloku GET.
REQ: Pozadavek na preneseni dat (nastavovano v OB1).
CONT: Parametr pokracovani v prenosu (nastavovano v OB1).
DEST_ID: MPI adresa komunikujiciho partnera.
AR_ADDR: Adresa promenne v pametove oblasti komunikacniho partnera.
RET_VAL: Stav prenosu.
BUSY: BUSY=1: Prijimani dat neni dosud dokonceno. BUSY=0: Prijimani dat je
dokonceno nebo neni zadny pozadavek k prijimani.
RD: Adresa pameti, kde jsou prijimana data zapisovana.
```



Network 2: X Get completed

```
Hlidani hrany vystupu BUSY.
```



Network 3: X Get completed

```
Comment:
```

VAT tabulka:

Sender -- cv8_1\S7314-2DP Sender\CPU 314C-2 DP\S7 Program(1)

	Address	Symbol	Display format	Status value	Modify value
1					
2	//Get				
3	M 101.2	"ContinueX_Get"	BOOL		
4	M 101.3	"TransferX_Get"	BOOL		
5	M 101.4	"BusyX_Get"	BOOL		
6	M 101.5	"BusyX_Get_Nedge"	BOOL		
7	M 101.6	"X_Get_Cmpltd"	BOOL		
8					
9	QB 124	"Outputs124thByte"	BIN		
10					
11	MD 20	"SenderMD20"	FLOATING_POINT		
12					

PLC2 S7314-2PtP Receiver:

S7 Program(2) (Symbols) -- cv8_1\S7314-2PtP Receiver\CPU 314C-2 PtP

	Status	Symbol	Addres	Data type	Comment
1		ComSend_X_Put	FC 31	FC 31	
2		TransferData	M 100.3	BOOL	
3		ContinueX_Put	M 100.4	BOOL	
4		BusyX_Put	M 100.5	BOOL	
5		BusyX_Put_Nedge	M 100.6	BOOL	
6		X_Put_Cmpltd	M 100.7	BOOL	X Put completed
7		ReceiverPLC_MD10	MD 10	REAL	
8		AdresaNaSenderu	MD 20	REAL	
9		RetValX_Put	MW 134	INT	
10		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
11		X_PUT	SFC 68	SFC 68	Write Data to a Communication Partner...
12		Receiver	VAT 1		
13					

OB1:

OB1 : "Main Program Sweep (Cycle)"

Comment:

Network 1: Title:

X_Put.

Network 2: Title:

X_Put.

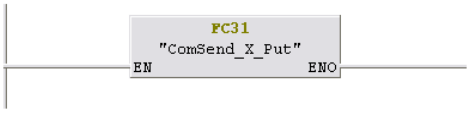
OB35:

OB35 : Call Every 100 ms

Comment:

Network 1: Title:

Volání funkce FC31.



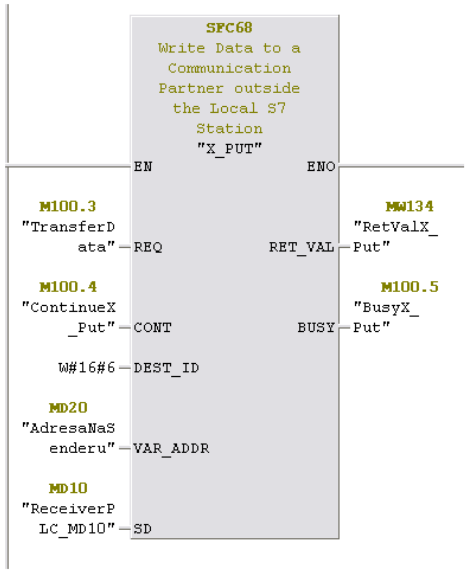
FC31:

FC31 : Funkce X_Put.

Funkce X_Put.

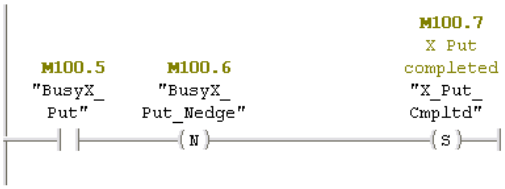
Network 1: Title:

Volani systemoveho funkcniho bloku PUT.
REQ: Pozadavek na preneseni dat (nastavovano v OB1).
CONT: Parametr pokracovani v prenosu (nastavovano v OB1).
DEST_ID: MPI adresa komunikujiciho partnera.
AR_ADDR: Adresa promenne v pametove oblasti komunikacniho partnera.
SD: Adresa pameti, ze ktere se bude kopirovat.
RET_VAL: Stav prenosu.
BUSY: BUSY=1: Prijimani dat neni dosud dokonceno. BUSY=0: Prijimani dat je dokonceno nebo neni zadny pozadavek k prijimani.



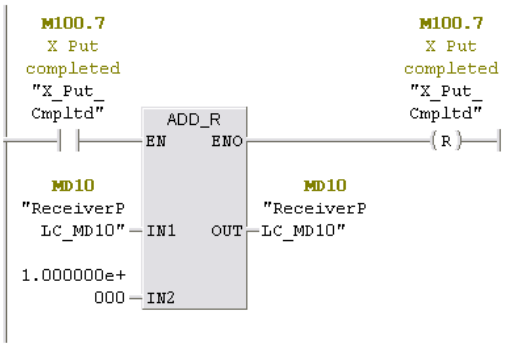
Network 2 : X Put completed

Comment:



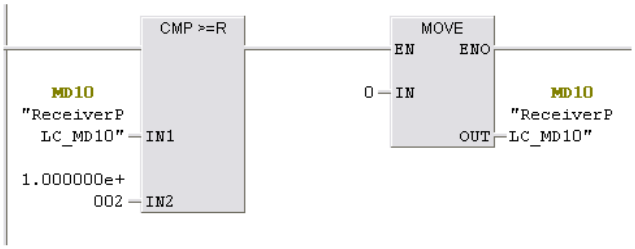
Network 3 : X Put completed

Comment:



Network 4 : Title:

Comment:



VAT tabulka:

Receiver -- cv8_1\S7314-2PtP Receiver\CPU 314C-2 PtP\S7 Program(2)

	Address	Symbol	Display format	Status value	Modify value
1					
2	//Put				
3	M 100.3	"TransferData"	BOOL		
4	M 100.4	"ContinueX_Put"	BOOL		
5	M 100.5	"BusyX_Put"	BOOL		
6	M 100.6	"BusyX_Put_Nedge"	BOOL		
7	M 100.7	"X_Put_Cmpltd"	BOOL		
8					
9	IB 124		BIN		
10	MD 10	"ReceiverPLC_MD10"	FLOATING_POINT		
11					

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI8\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI8\

Řešená úloha 8.2

Zadání: Nastavte komunikaci mezi dvěma PLC (CPU 314C-2DP a CPU 314C-2PtP) po MPI. Pro komunikaci použijte funkce SEND a RECEIVE. Adresa PLC CPU 314C-2DP na sběrnici je 6, adresa PLC CPU 314C-2PtP je 9.

Z PLC CPU 314C-2DP posílejte pět hodnot typu INTEGER do PLC CPU 314C-2PtP. Do první hodnoty datového bloku zapisujte z VAT tabulky, druhou hodnotu ve zvolené časové periodě inkrementujte od 0 100, třetí hodnotu dekrementujte od 100 do 0. Čtvrtá hodnota bude součtem a pátá součinem druhé a třetí hodnoty.

Data posílejte kontinuálně.

Prvním krokem řešení úlohy je hardwarová konfigurace dvou PLC. Stejně jako v řešené úloze 8.1 je pro komunikaci potřeba nastavit každému prvku na sběrnici jinou adresu. CPU 314C-2DP na sběrnici je 6, adresa PLC CPU 314C-2PtP je 9.

X_Send

Pomocí systémové funkce SFC65 „X_SEND“ lze zasílat data komunikačnímu partnerovi mimo lokální S7 stanici. Data jsou přijímána v komunikačním partneru pomocí systémové funkce SFC66 „X_RCV.“

Přenášená data lze identifikovat pomocí vstupního parametru REQ_ID. Tento ID je zaslán s přenášenými daty. Data jsou poslána poté, co SFC voláme s REQ = 1.

Před vysláním dat se musíme ujistit, že vysílací oblast (u vysílacího CPU) je definována parametrem SD a je menší nebo maximálně je stejně velká než přijímací oblast definovaná pomocí parametru RD (u komunikačního partnera).

Parametr REQ_ID na konci přijímání dat je důležitý zejména v následujících situacích:

Pokud voláme více než jeden SFC65 „X_SEND“ blok s rozdílnými REQ_ID parametry u vysílacího CPU a zasíláme data jednomu komunikačnímu partneru.

Pokud zasíláme data jednomu komunikačnímu partneru z více než jednoho vysílacího CPU užitím SFC65 „X_SEND.“

Určením REQ_ID lze uložit přijímaná data do různých paměťových částí.

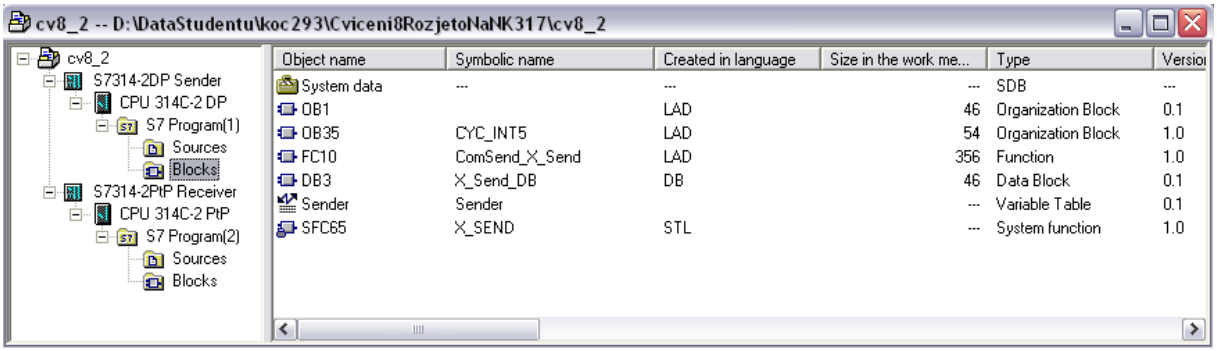
X_Receive

Pomocí systémové funkce SFC66 „X_RCV“ můžeme přijímat data zasílaná od jednoho nebo více komunikačních partnerů umístněných mimo lokální S7 stanici. Tato dada jsou vysílána pomocí SFC65 „X_SEND.“

Pomocí SFC66 „X_RCV“:

Lze kontrolovat, zda data byla zaslána a zdali čekají, než budou zkopírována.

Lze zkopírovat nejstarší data z fronty do určené přijímací oblasti.



Program v LAD

PLC1: S7314-2DP Sender:

S7 Program(1) (Symbols) -- cv8_2\S7314-2DP Sender\CPU 314C-2 DP

	Status	Symbol	Addres	Data type	Comment
1		X_Send_DB	DB 3	DB 3	
2		ComSend_X_Send	FC 10	FC 10	
3		ActivateX_Send	M 102.2	BOOL	
4		ContinueX_Send	M 102.3	BOOL	
5		BusyX_Send	M 102.4	BOOL	
6		BusyX_Send_Nedge	M 102.5	BOOL	
7		X_Send_Cmpltd	M 102.6	BOOL	X Send completed
8		RetValX_Send	MW 134	INT	
9		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
10		X_SEND	SFC 65	SFC 65	
11		Sender	VAT 1		
12					

OB1:

OB1 : "Main Program Sweep (Cycle)"

Comment:

Network 1: Title:

X_Send.

Network 2: Title:

X_Send.

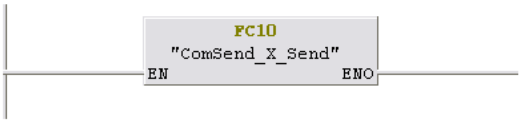
OB35:

OB35 : Block Call Timer-Controlled Every 100 ms

Comment:

Network 1: Title:

Volání funkce FC10.



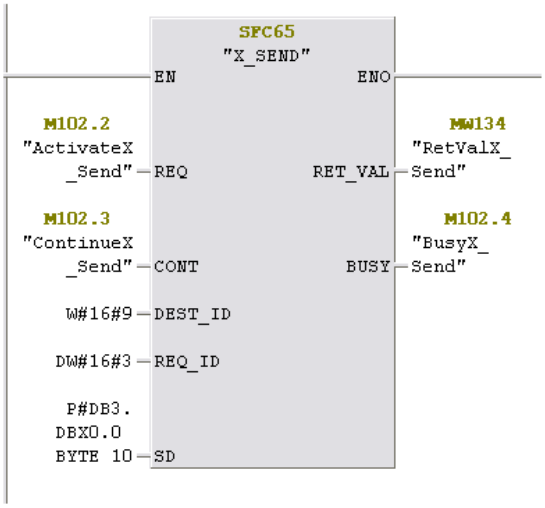
FC10:

FC10 : Communicating with Both Servers

Communication with Server MPI 9.

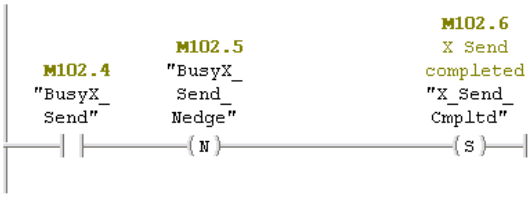
Network 1: Title:

Volani systemoveho funkcniho bloku X_SEND.
REQ: Pozadavek na preneseni dat (nastavovano v OB1).
CONT: Parametr pokracovani v prenosu (nastavovano v OB1).
DEST_ID: MPI adresa komunikujiciho partnera.
REQ_ID: Identifikatr: cislo 3.
SD: Ukazatel na posilana data.
RET_VAL: Stav prenosu.
BUSY: BUSY=1: Prijimani dat neni dosud dokonceno. BUSY=0: Prijimani dat je dokonceno nebo neni zadny pozadavek k prijimani.



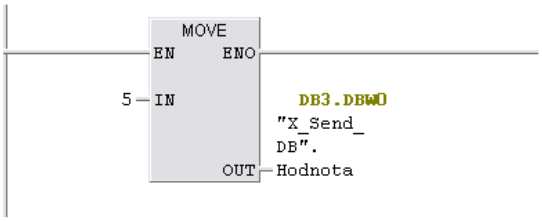
Network 2 : X Send completed

Comment:



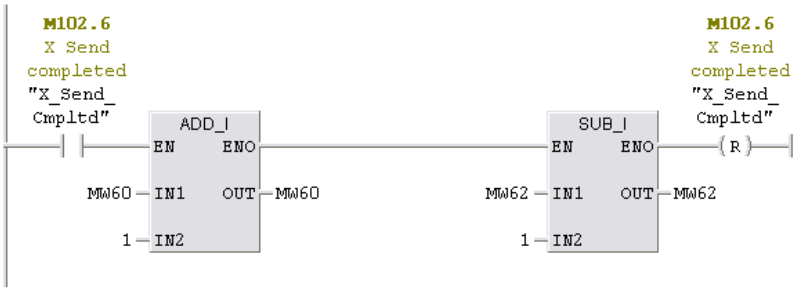
Network 3 : Title:

"X_Send_DB".Hodnota: Hodnota 5.



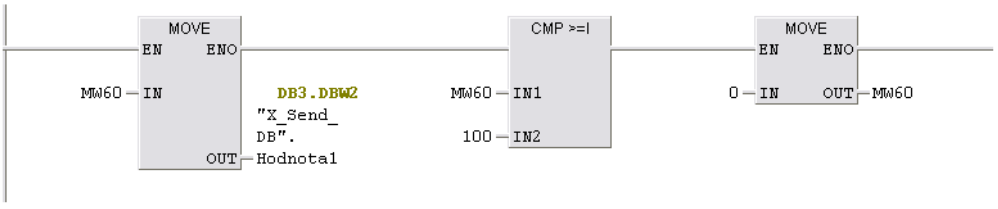
Network 4 : X Send completed

Jestli ze je prenos dat dokoncen, pak inkrementuj MW60 a dekrementuj MW62.



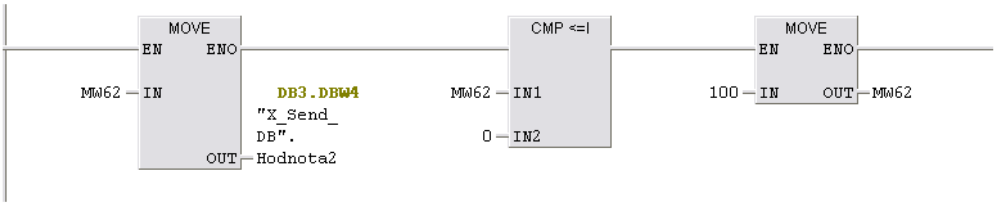
Network 5 : Title:

"X_Send_DB".Hodnota1: inkrementovaná data.



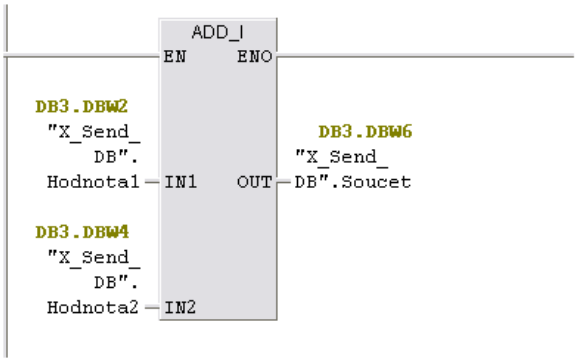
Network 6 : Title:

"X_Send_DB".Hodnota2: dekrementovaná data.



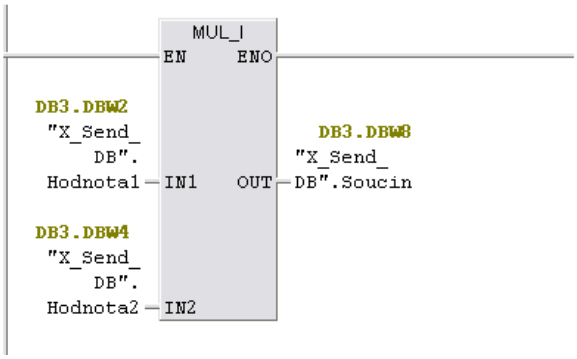
Network 7 : Title:

```
"X_Send_DB".Soucet = "X_Send_DB".Hodnota1 + "X_Send_DB".Hodnota2.
```



Network 8 : Title:

```
"X_Send_DB".Soucin = "X_Send_DB".Hodnota1 * "X_Send_DB".Hodnota2.
```



DB3:

DB3 -- "X_Send_DB" -- cv8_2\S7314-2DP Sender\CPU 314C-2 DP\...\DB3

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	Hodnota	INT	0	
+2.0	Hodnota1	INT	0	
+4.0	Hodnota2	INT	0	
+6.0	Soucet	INT	0	
+8.0	Soucin	INT	0	
=10.0		END_STRUCT		

VAT tabulka:

Sender -- cv8_2\S7314-2DP Sender\CPU 314C-2 DP\S7 Program(1)

	Address	Symbol	Display format	Status value	Modify value
1					
2	//Send - Receive communication				
3	M 102.2	"ActivateX_Send"	BOOL		
4	M 102.3	"ContinueX_Send"	BOOL		
5	M 102.4	"BusyX_Send"	BOOL		
6	M 102.5	"BusyX_Send_Nedge"	BOOL		
7	M 102.6	"X_Send_Cmpltd"	BOOL		
8					
9	DB3.DBW 0	"X_Send_DB".Hodnota	DEC		
10	DB3.DBW 2	"X_Send_DB".Hodnota1	DEC		
11	DB3.DBW 4	"X_Send_DB".Hodnota2	DEC		
12	DB3.DBW 6	"X_Send_DB".Soucet	DEC		
13	DB3.DBW 8	"X_Send_DB".Soucin	DEC		
14					

PLC2 S7314-2PtP Receiver:

S7 Program(2) (Symbols) -- cv8_2\S7314-2PtP Receiver\CP...

	Status	Symbol	Addres	Data type	Comment
1		X_Receive_DB	DB 3	DB 3	
2		ComSend_X_Rec...	FC 30	FC 30	
3		AcceptRcvData	M 100.2	BOOL	
4		NewDataX_Rcv	M 101.5	BOOL	
5		JobIdentifierX_Rcv	MD 120	DWORD	
6		RetValX_Receive	MW 132	INT	
7		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
8		X_RCV	SFC 66	SFC 66	
9		Receiver	VAT 1		
10					

OB1:

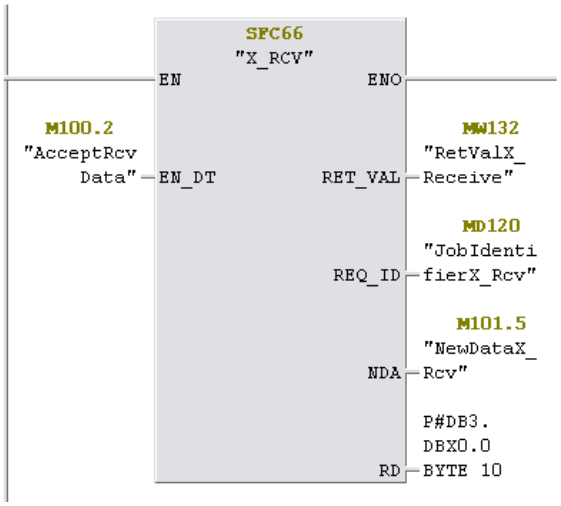
```
OB1 :  "Main Program Sweep (Cycle)"
Comment:
Network 1: Title:
Set EN_DT (parametr SFC66) pro akceptovani prijatych dat.
```

OB35:

```
OB35 : Call Every 100 ms
Comment:
Network 1: Title:
Volání funkce FC30.
```

FC30:

```
FC30 : Title:
Comment:
Network 1: Timer-Controlled Call of SFC X_RCV
Call X_RCV system function block.
EN_DT: Povoleni prenosu dat.
RET_VAL: Return value.
REQ_ID: Identifikator prijimanych dat.
NDA: Prisla nova data ke zpracovani.
RD: Oblast pameti, kde budou data zapsana.
```



DB3:

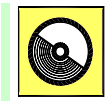
DB3 -- "X_Receive_DB" -- cv8_2\S7314-2PtP Receiver\CPU 314C-2 PtP\...\DB3

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	PolePro5Integeru	ARRAY[1..50]	0	
*2.0		INT		
=100.0		END_STRUCT		

VAT tabulka:

Receiver -- cv8_2\S7314-2PtP Receiver\CPU 314C-2 PtP\S7 Program(2)

	Address	Symbol	Display format	Status value	Modify value
1					
2	//Send - Receive communication				
3	DB3.DBW 0	"X_Receive_DB".PolePro5Integeru[1]	DEC		
4	DB3.DBW 2	"X_Receive_DB".PolePro5Integeru[2]	DEC		
5	DB3.DBW 4	"X_Receive_DB".PolePro5Integeru[3]	DEC		
6	DB3.DBW 6	"X_Receive_DB".PolePro5Integeru[4]	DEC		
7	DB3.DBW 8	"X_Receive_DB".PolePro5Integeru[5]	DEC		
8	DB3.DBW 10	"X_Receive_DB".PolePro5Integeru[6]	DEC		
9	DB3.DBW 12	"X_Receive_DB".PolePro5Integeru[7]	DEC		
10	DB3.DBW 14	"X_Receive_DB".PolePro5Integeru[8]	DEC		
11	DB3.DBW 16	"X_Receive_DB".PolePro5Integeru[9]	DEC		
12	DB3.DBW 18	"X_Receive_DB".PolePro5Integeru[10]	DEC		
13	MD 120	"JobIdentifierX_Rcv"	DEC		
14					



DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI8\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI8\

9. ETHERNET

Čas ke studiu: 3 hodiny

Cíl Po prostudování této kapitoly budete umět

- Popsat základní vlastnosti Ethernetu.
- Rozlišit klasický a průmyslový Ethernet.
- Popsat fyzickou vrstvu Ethernetu.
- Popsat linkovou vrstvu Ethernetu.
- Praktická část kapitoly se věnuje komunikaci programovatelných automatů přes Ethernet – nahrávání aplikace, komunikace pomocí ISO-on-TCP a S7 funkcí.

Výklad

Historie Ethernetu sahá do počátku sedmdesátých let, kdy byl vyvinut v laboratořích firmy Xerox. Vycházel ze systému Aloha, kde byl poprvé použit náhodný přístup ke komunikačnímu médiu. Tým firmy Xerox vylepšil přístup ke komunikačnímu médiu použitý u systému Aloha tím, že přidal mechanizmy pro detekci kolize, pro „poslouchání“ provozu na komunikačním médiu. Tím vznikl základ metody CSMA/CD, která se na dlouhou dobu stala zákaldním mechanizmem pro přístup ke komunikačnímu médiu u sítí Ethernet [1].

První experimentální verze Ethernetu dosahovaly přenosové rychlosti 2,94 Mb/s a prokázal svoji funkčnost. Do vývoje tohoto komunikačního systému se zapojila řada firem, včetně DEC, Intel aj. a v roce 1980 vznikla verze označována jako DIX Ethernet (DEC, Intel, Xerox), která již pracovala na rychlosti 10Mb/s.

Ethernet byl posléze standardizován v rámci IEEE802, podskupině 3 (IEEE 802.3), nicméně v mírně pozměněné podobě. Původní DIX Ethernet některé z těchto modifikací také implementoval, ale tím byl jeho vývoj ukončen. Standard IEEE byl poprvé publikován v roce 1985 s názvem *IEEE 802.3 Carrier Sense Multiple Access (CSMA/CD) Method and Physical Layer Specification*. V názvu sice chybí pojem Ethernet, jelikož tento pojem byl zaregistrován firmou Xerox, ale vývoj tohoto standardu už probíhal pouze pod organizací IEEE. Ethernet je dnes standardizován i normou organizace ISO, a to ISO 8802-3.

Od roku 1985 vznikaly další dílčí části IEEE 802.3, jako například [1]:

- 802.3a 10Base2: médium tenký koaxiální kabel (BNC).
- 802.3i 10Base-T: 10 Mb/s, kroucený pár vodičů, topologie hvězda.
- 802.3u 100Base-TX (2 kroucené páry), 100Base-T4 (4 kroucené páry), 100Base-FX (dvě několikavidová optická vlákna): 100Mb/s „Fast Ethernet“.
- 802.3x úplný duplex, řízení toku.
- 802.3ab 1000Base-T: 1 Gb/s, kroucený pár vodičů.
- 802.3ae 10GBase, 10 Gb/s, optické vlákno.
- 802.3af napájení po Ethernetu.

9.1. Ethernet a model ISO/OSI

Fyzická vrstva (Physical Layer)

Fyzická média používaná v Ethernetu se dají rozdělit do několika skupin podle rychlosti a použitého propojovacího média. Vbraná přenosová média jsou popsána níže [1, 2, 3] :

Ethernet s přenosovou kapacitou 10 Mbit/s:

10Base-5

- Jedná se o původní přenosové médium Ethernetu.
- Přenosové médium - pětkrát stíněný koaxiální kabel s impedancí 50 ohm. Je označovaný jako Thick Ethernet neboli Yellow Cable.
- Maximální délka kabelu segmentu je 500 m. Pro připojování stanic jsou používány transceivery, maximální vzdálenost stanice od transceiveru je 50 m.
- Transceivery musí být připevňovány ve vzdálenostech násobku 2,5 m, na kabelech bývá označení. Segmenty jsou ukončované terminátory.

10Base-2

- Přenosové médium - dvakrát stíněný koaxiální kabel s impedancí 50 ohm. Je označovaný jako Thin Ethernet.
- Maximální délka kabelu segmentu je 185 m.
- Maximálně 25 stanic na jednom segmementu, segmenty jsou ukončované terminátory.

10Base-T

- Přenosové médium – stíněný nebo nestíněný kroucený pár s impedancí 100 ohm (Cathegory 3 nebo lepší).
- Maximální délka kabelu mezi uzly a aktivním prvkem je maximálně 100 m.

10Base-FL

- Přenosové médium – obvykle multimodový optický kabel (v některých případech i singlemodový kabel).
- Maximální délka kabelu mezi uzly je 2 km.

Fast Ethernet s přenosovou kapacitou 100 Mbit/s:

100Base-TX

- Přenosové médium – stíněný nebo nestíněný kroucený pár s impedancí 100 ohm (Cathegory 5 nebo lepší).
- Maximální délka kabelu mezi uzly a aktivním prvkem je maximálně 100 m.

100Base-T4

- Přenosové médium – stíněný nebo nestíněný kroucený pár s impedancí 100 ohm (Cathegory 3 nebo lepší), využívá všechny 4 páry v kabelu.
- Maximální délka kabelu mezi uzly a aktivním prvkem je maximálně 100 m.

100Base-FX

- Přenosové médium – multividový optický kabel (v některých případech i singlemodový kabel).
- Maximální délka kabelu mezi uzly v případě plně duplexního provozu je 2 km.

Gigabit Ethernet s přenosovou kapacitou 1000 Mbit/s:

1000Base-SX

- Přenosové médium – multimodový optický kabel.
- Maximální délka kabelu mezi uzly a aktivním prvkem je dána parametry kabelu.

1000Base-LX

- Přenosové médium – multimodový optický kabel nebo singlemodový optický kabel.
- Maximální délka kabelu mezi uzly a aktivním prvkem je dána parametry kabelu.

1000Base-T

- Přenosové médium – stíněný nebo nestíněný kroucený pár s impedancí 100 ohm (Cathegory 5 nebo lepší).
- Maximální délka kabelu mezi uzly a aktivním prvkem je maximálně 100 m.
- Používá specifický způsob kódování signálů, který umožňuje dosáhnout této komunikační rychlosti.

10 Gigabit Ethernet s přenosovou kapacitou 10 Gbit/s:

10GBase-SR („short range“)

- Přenosové médium – multimodový optický kabel.
- Maximální délka kabelu mezi uzly je 26m.

10GBase-LR („long range“)

- Přenosové médium – singlemodový optický kabel.
- Maximální délka kabelu mezi uzly je 10km.

10GBase-T

- Přenosové médium – stíněný nebo nestíněný kroucený pár s impedancí 100 ohm (Cathegory 6a).
- Maximální délka kabelu mezi uzly je maximálně 100 m.

Původní Ethernet využíval jako přenosové médium koaxiální kabel. Na začátku 90 let vyl vyvinut standard využívající krouceného páru. Toto přenosové méduim umožnilo budování rozsáhlých sítí, přičemž byly využívány ověřené postupy a techniky známé z telekomunikačních sítí. V roce 1995 byl přijat standard pro Fast Ethernet s přenosovou rychlostí 100Mb/s. Místo hubů se začínají používat switche. V roce 1998 byl standard přepracován tak, aby umožňoval přenos rychlostí 1Gb/s. Je založen jak na optických vláknech nebo krouceném páru. Další inovace Ethernetu spočívaly ve vylepšování jeho vlastností, např. umožnění přenosů v plně duplexním režimu. V roce 2002 byl publikován standard 10G Ethernetu. Ten pracuje již výhradně v plně duplexním režimu, poloviční duplex a metoda CSMA/CD již není podporována.

9.2. Linková vrstva (Data Link Layer)

Typickou vlastností standardního Ethernetu dle IEEE 802.3 je použití přístupová metoda CSMA/CD (Carrier Sense Multiple Access/ Collision Detection), což znamená metoda mnohonásobného přístupu k médiu s nasloucháním nosné a detekce kolizí [1]:

- CS (Carrier Sense) – znamená, že stanice před vysíláním poslouchá přenosové médium, zda nějaká jiná stanice nevysílá. Pokud ano, nezačne odesílat svá data. Začne vysílat, až jakmile se médium uvolní.
- MA (Multiple Access) – zkratka znamená, že se jedná o přístupovou metodu pro přenová média pro připojení více uzlů.
- CD (Collision Detection) – znamená, že stanice jsou schopné detekovat koliizi už v průběhu vysílání. Stanice sleduje, zda úrovně signálů, které vysílá, odpovídají úrovním, které přijímá (poslouchá). V případě, že současně vysílá jiná stanice, úrovně neodpovídají. Tak rozpozná, že došlo ke kolizi a vyšle kolizní posloupnost – speciální signál o délce 32b, který informuje rovněž ostatní stanice, že došlo ke kolizi. Po kolizi opakuje stanice vysílání po náhodně zvoleném časovém intervalu. Pokud u pak dojde ke kolizi, časový interval se zdvojnásobuje. Pokud se vysílání nepodaří ani po šestnácti pokusech, vysílá linková vrstva vyšší vrstvě zprávu o neúspěšné vyslání. Vzhledem k tomu, že stanice před vysíláním poslouchá přenosové médium, může kolize nastat pouze v době od počítku vysílání do doby, než signál obsadí celou délku médium. Tomuto časovému intervalu se říká kolizní okénko. Nejkratší rámec musí být delší, něž je doba kolizního okénka, jinak by mohlo docházek k nedetekovaným kolizím.

Přístup ke komunikačnímu médiu pomocí metody CSMA/CD se používá v režimu polovičního duplexu, když je k médiu připojeno více zařízení. Do té doby, než se rozšířily v sítích Ethernet přepínače (switch, multiportový most), byla CSMA/CD typickým způsobem řízení komunikace v těchto sítích. Jakmile je síť postavena zažízeních typu přepínač, komunikující prvky nemusí sdílet jeden společný kanál.

Pokud jsou počítače k přepínačům připojeny pomocí plného duplexu, CSMA/CD je úplně deaktivován, takto propojená zařízení mohou vysílat data kdykoliv.

Kolizní doména – jedná se o segment sítě, ve kterém vznikne kolize, když dvě nebo více zařízení začnou vysílat současně.

Rámec protokolu 802.3

Tab. 14.1. Rámec protokolu Ethernet.

Počet oktetů:	1	6	6	2	46-1500	4
Význam:	Preambule (Synchronizace)	Cílová adresa	Zdrojová adresa	Délka datového pole	Datové pole	Kontrolní součet

Popis prvků rámce Ethernet:

- **Preambule** se skládá ze střídajících se jedniček a nul, přičemž poslední z oktetů má tvar 10101011 a označuje začátek vlastního rámce. U 802.3 se uvádí jako preambule jen prvních sedm oktetů rámce a osmý je tzv. omezovač počátku rámce (starting frame delimiter - SFD).

- **Cílová i zdrojová adresa** jsou fyzické (MAC) adresy o délce 16 nebo 48 bitů (záleží na konkrétní aplikaci, avšak typ MAC adresy musí být stejného typu pro celý segment LAN), kde zdrojová je vždy unikátní a cílová adresa muže být individuální (unicast), skupinová (multicast) nebo všeobecná (broadcast).
- **Délka datového pole** určuje počet oktetů datového pole.
- **Datové pole** se skládá minimálně ze 46 oktetů a maximální velikost je omezena na 1500 oktetů.
- **Kontrolní součet** (frame check sequence) je třicetidvou bitový cyklický kontrolní kód, který se počítá přes všechna pole kromě preambule.

9.3. Popis sítě Ethernet a Industrial Ethernet

V dnešní době je Ethernet rozšířen do tisíců aplikací, s použitím široké škály přenosových protokolů. Rozšiřování technologie Ethernet do řídicích systémů má několik příčin. Především je úzce spjata s nejdůležitějším informačním prostředkem současnosti – sítí Internet. Tím enormně narostl počet ethernetových rozhraní a následně výrazně poklesla jejich cena [6].

Ethernet lze z hlediska deterministočnosti rozdělit na komerční a průmyslový. Klasický komerční Ethernet používá nedeterministické metody přístupu na médium, a proto ho nelze použít v průmyslových aplikacích. Z tohoto důvodu vznikly modifikované protokoly a jistá opatření vedoucí ke zvýšení deterministočnosti této sítě a tím i k možnosti použití v distribuovaných systémech. Síť s těmito modifikacemi se pak nazývá průmyslový (Industrial) Ethernet .

Zde je výčet několika opatření, které vedly ke zlepšení odezvy:

- Strukturovanost topologie, kde namísto sběrnice s rozsáhlou doménou dochází v současných i kancelářských aplikacích k rozbití rozsáhlé domény použitím rozdělovačů (hub) a přepínačů (switch) na Krátké domény s mnohem menší pravděpodobností kolizí, plynoucích z přístupové metody CSMA/CD.
- Vysokou a stále rostoucí rychlostí ethernetových budičů a tím zkrácením doby odezvy na komunikačním kanálu.
- Směrováním zpráv jen do segmentů, pro které jsou tyto zprávy určeny, čímž opět dochází ke zmenšení pravděpodobnosti kolize.
- Segmentací zpráv, pomocí níž jsou odděleny zprávy RT od zpráv non-RT a topologií je zaručeno oddělení segmentů RT a non-RT.
- Aplikací prioritních slotů do metody CSMA/CD (Carrier Sense Multiple Access/Collision Detection), které zaručí definovaný okamžik přístupu k médiu.
- Použití UDP (User Datagram Protocol) místo protokolu TCP (Transmission Control Protocol) pro časově kritické úlohy (tato nespojovaná služba umožňuje poslání zprávy již v dalším taktu po odhalení kolize).
- Použití PTP (Precission Time Protocol) podle standardu IEEE 1588.

Precission time protocol je zatím nejúčinnější a levný mechanismus pro zaručení synchronismu zpráv v komunikaci Ethernet staví na distribuovaných hodinách reálného času v každé komunikující entitě. Dosahuje se tak vyššího stupně synchronizace zpráv (menší jitter) než u stávajících průmyslových sběrnic, které jsou takto navrhovány ze své podstaty.

Shrnutí pojmů

První **standard Ethernetu** vypracovaný organizací IEEE byl publikován v roce 1985 pod označením „IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification“.

Ethernet lze z hlediska deterministočnosti rozdělit na **komerční a průmyslový**. Klasický komerční Ethernet používá nedeterministické metody přístupu na médium, a proto ho nelze použít v průmyslových aplikacích. Z tohoto důvodu vznikly modifikované protokoly a jistá opatření vedoucí ke zvýšení deterministočnosti této sítě a tím i k možnosti použití v distribuovaných systémech. Síť s těmito modifikacemi se pak nazývá průmyslový (Industrial) Ethernet.

Protokol IEEE 802.3 používá metodu přístupu **CSMA/CD** (Carrier Sense Multiple Access/ Collision Detection), což znamená metoda mnohonásobného přístupu k médiu s nasloucháním nosné a detekce kolizí.

Otázky

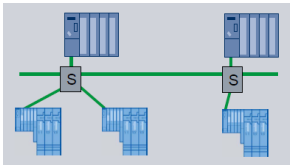
1. Popište základní vlastnosti Ethernetu.
2. Jaký je rozdíl mezi komerčním a průmyslovým Ethernetem.
3. Jaká opatření vedou ke zlepšení odezby Ethernetu?
4. Popište fyzickou vrstvu Ethernetu?
5. Popište druhy přenosových médií používaných v Ethernetu.
6. Popište metodu přístupu ke komunikačnímu médiu používanou u Ethernetu.
7. Popište rámec dle IEEE 802 a jeho části.

Použitá literatura a další zdroje

1. Spurgeon Ch. E. Ethernet. The Definitive Guide. O’Reilly Media, 2000. ISBN 1-56592-660-9.
2. Strukturované kabeláže. [online], [cit. 03-08-2010] http://www.svetsiti.cz
3. Standard pro 10 Gigabit Ethernet. [online], [cit. 03-08-2010] http://www.svetsiti.cz
4. Siemens: SIMATIC Communication with SIMATIC System Manual, 12/2005, EWA 4NEB 710 6075-02 03
5. Siemens: SIMATIC Profinet System Description System Manual, 10/2006 A5E00298288-03
6. Zezulka F.; Hynčica O. Průmyslový Ethernet I-IX. Automa, 2007-2008. ISSN 1210-9592.

Řešená úloha 9.1

Zadání: Seznamte se s možnostmi komunikace po Ethernetu u PLC S7 300/400.



Parametry a vlastnosti komunikace po ethernetu:

- Fyzická vrstva: 100Base-TX, 100Base-FX, …
- Topologie: Linie, strom, hvězda, kruh.
- Maximální vzdálenost port-to-port metalického vedení: 100m.
- Maximální vzdálenost port-to-port optického vedení: 70km.
- Přenosová rychlost:10Mbps, 100Mbps, 1Gbps.
- Maximální počet stanic: >1000.

Tab. 9.1 Protokoly ethernet

Protokol	Adresace	Typ komunikace
Profinet IO	MAC, (Device name)	Cyklická
ISO	MAC	Acyklická
ISO-on-TCP	IP	Acyklická
TCP/IP	IP	Acyklická
UDP/IP	IP	Acyklická

Tab. 9.2 Srovnání datových protokolů

Protokol	Routing	Proměnná délka zprávy	Potvrzování	Ne-Siemens zařízení
ISO	Ne	Ano	Ne	Ne
ISO-on-TCP	Ano	Ano	Ano	Ne
TCP/IP	Ano	Ne	Ano	Ano
UDP/IP	Ano	Ano	Ne	Ano

Příklad MAC adresy:

```
Fyzická Adresa. . . . . : 00-E0-18-2E-7F-66
```

Příklad IP adresy:

```
Adresa IP . . . . . : 10.160.11.208
```

Možnosti komunikace mezi CPU:

Tab. 9.3 Možnosti komunikace mezi CPU

Služba	**Maximální množství přenášených dat**	**Bloky**
S7 komunikace	32 kB S7-300 64 kB S7-400 165 B S7-300 440 B S7-400	BSEND, BRCV BSEND, BRCV USEND, URCV PUT, GET USEND, URCV PUT, GET
Send/Receive komunikace	8 kB Pouze s CP	AG_SEND, AG_RECV, AG_LSEND, AG_LRECV
Otevřená komunikace	8 kB 1460 B Pouze s CPU	TSEND, TRCV, TUSEND, TURCV
Profinet IO	512 IB + 512 QB IO_Device jen s CP	PNIO_SEND, PNIO_RECV

Konkrétní hodnoty maximální velikosti přenášených dat je různý podle použitého CPU.

Komunikace pomocí ethernetu je dostupná nejen pro CPU S7 300, S7 400, ale i pro různé typy operátorských panelů, měničů, vzálených vstupů a výstupů a dalších nejrůznějších zařízení.

Výhody ethernetu:

- I cyklický přenos dat s krátkými dobami odezvy (Profinet IO).
- Výkonná síť, rozlehlá síť, flexibilní topologie, nezávislé části sítě.
- Možnost bezdrátové komunikace.
- IT služby – www, FTP, mail.
- Ethernetové rozhraní má největší množství zařízení.
- Snadná a výkonná komunikace s Profinet CBA.

Řešená úloha 9.2

Zadání: Porovnání různých typů komunikace a jejich použití v řídicích systémech.

Možnosti komunikace mezi CPU:

1) Kterou síť lze použít
- MPI
- Profibus
- Ethernet, Profinet

2) Jaký typ komunikace lze použít
- Global data
- S7 basic komunikace
- S7 komunikace
- DP komunikace
- TCP/IP, UDP/IP, ISO, ISO-on-TCP
- Profinet IO
- Profinet CBA

Datová komunikace – co a kdy použít?

1) Komunikace mezi Simatic S7 PLC
- S7 komunikace (Profibus, ethernet)
- Profinet CBA
- S7 basic komunikace (MPI)

2) Komunikace Simatic S7 <-> ne-Siemens HW zařízení
- Otevřená komunikace TCP/UDP (ethernetové rozhraní S7 CPU)
- Send/Receive komunikace TCP/UDP (ethernet CP)

3) Komunikace s krátkou dobou obnovy dat (1 ms, 10 ms,..)
- Profinet CBA (ethernet)
- Profibus DP
- Profinet IO

4) Synchronizace více PLC mezi sebou (start/stop atd.)
- Profinet CBA
- UDP multicast/broadcast (ethernet přes CP)
- Global data (MPI)

5) Přenos velkého množství dat
- S7 komunikace BSEND/BRCV (ethernet, profibus) – až 64 kB dat
- Otevřená komunikace TCP/UDP (ethernetové rozhraní S7 CPU) – až 8/32 kB dat
- Send/Receive komunikace TCP/UDP (ethernet CP) – až 8 kB dat

6) Komunikace mezi mnoha PLC
- Profinet CBA – až 32 PLC, cyklicky i acyklicky, modularita
- S7 komunikace (ethernet/profibus) – počet spojení podle konkrétního CPU
- Otevřená komunikace či Send/Receive (ethernet) – počet spojení podle konkrétního CPU

Řešená úloha 9.3

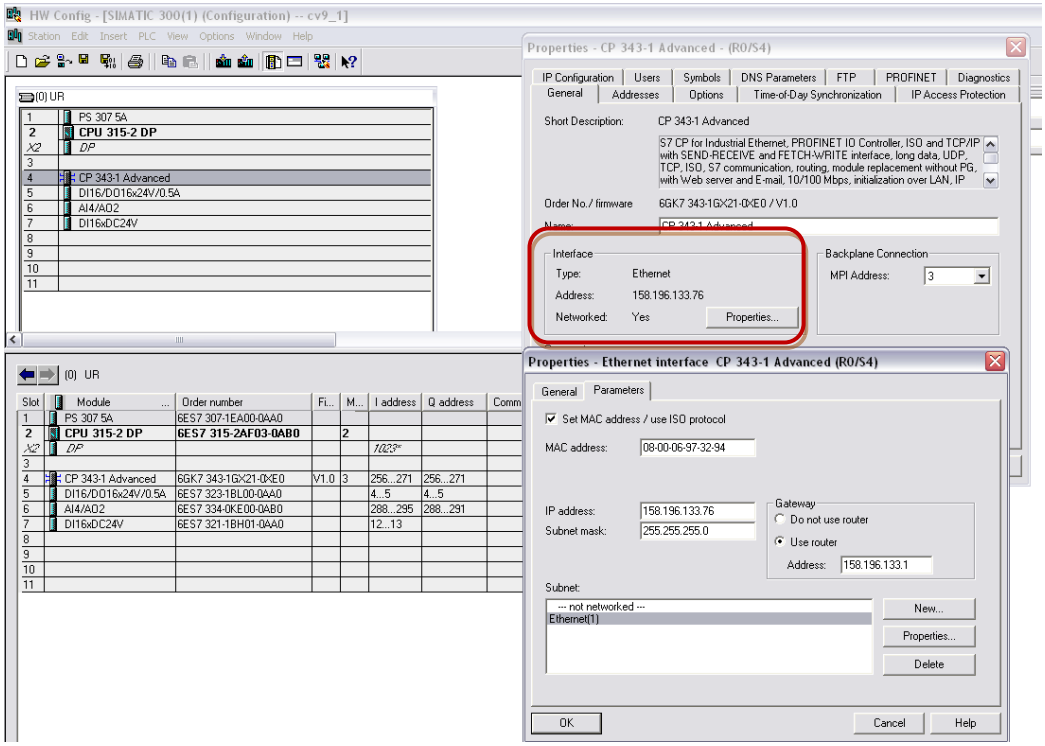
Zadání: Vytvořte komunikaci pomocí sítě ethernet mezi PC a PLC Siemens S7-300. Jako programovatelný automat použijte CPU 315-2DP (6ES7 315-AF03-0AB0) a jako ethernetový modul použijte komunikační procesor CP 343-1 Advanced (6GK7 343-1GX21-0XE0).

Komunikace mezi PLC a PC se nastaví v hardwarové konfiguraci. Po vložení lišty RACK, zdroje a CPU 315-2DP se do slotu č.4 vloží komunikační procesor (CP), který lze nalézt v katalogu ve složce CP300 – Industrial Ethernet – CP343-1 Advanced-IT – 6GK7 343-1GX21-0XE0, verze 1.2.

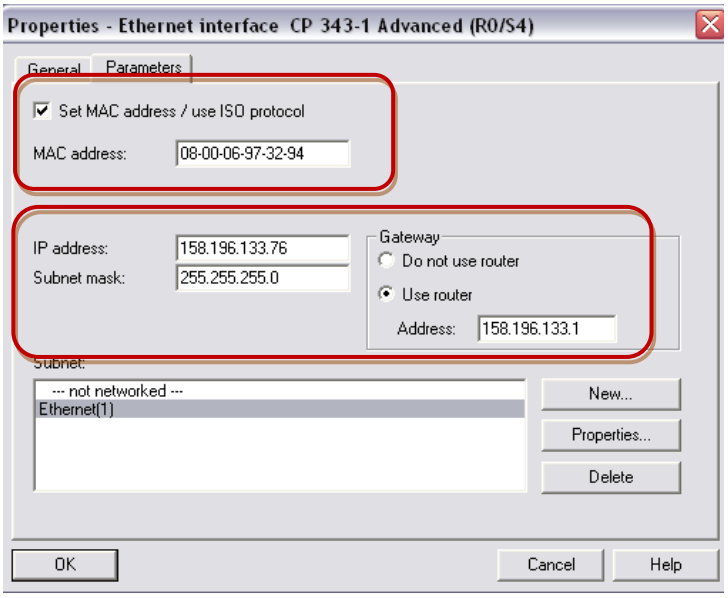
Ihned po vložení komunikačního procesoru do slotu č.4 vyskočí dialogové okno, kde se vyplní MAC a IP adresa komunikačního procesoru. Je žádoucí zkontrolovat, zda je zatrhnuta volba Set MAC address/use ISO protocol. MAC adresa zařízení je specifikována již při výrobě a může být změněna. Důrazně se však doporučuje MAC adresu zařízení neměnit. Do editovacího okna vepište MAC adresu (08-00-06-97-32-94), která je zobrazena na zařízení. Následně nastavte masku podsítě (255.255.255.0) a IP adresu (158.196.133.76), která je danému komunikačnímu procesu přidělena a je rovněž napsána na štítku na zařízení. Dále zaškrtněte použití routeru pomocí use router. IP adresa routeru v učebně je 158.196.133.1. Kliknutím na tlačítko New se v projektu vytvoří síť Ethernet. Kliknutím na tlačítko OK se dialogové okno nastavení komunikačního procesoru zavře.

Pozn. Pokud PLC ještě nebylo použito s daným komunikačním procesorem, pak nebude PLC ani připojený komunikační procesor znát zapsanou IP adresu. Když pak zvolíte v Set PG/PC interface nastavení komunikace na Ethernet, pak nebude možné konfiguraci do PLC nahrát, ani se k němu po ethernetu připojit. V tom případě je nutno konfiguraci nahrát přes MPI rozhraní. Až po úspěšném nahrání konfiguraci bude možné se k PLC a ke komunikačnímu procesoru připojit přes ethernet.

Obr. 9.1 Konfigurace komunikačního procesoru CP343.



Obr. 9.2 Konfigurace komunikačního procesoru CP343.



Obr. 9.3 Konfigurace komunikačního procesoru CP343.

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI9\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI9\

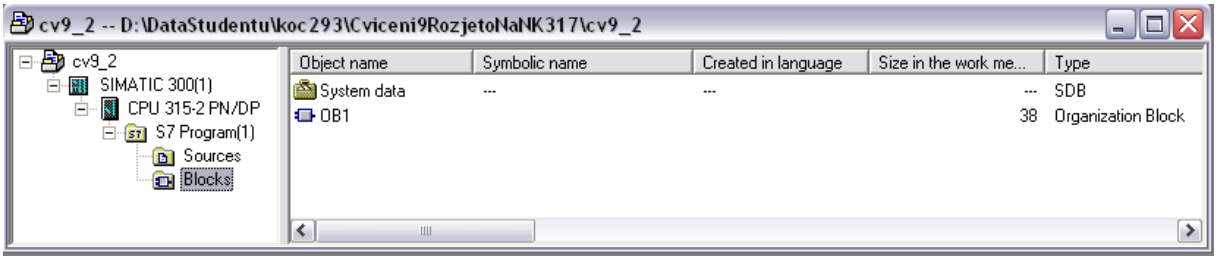
Řešená úloha 9.4

Zadání: Vytvořte komunikaci pomocí sítě ethernet mezi PC a PLC Siemens S7-300. Jako programovatelný automat použijte CPU s integrovaným ethernetovým rozhraním 315PN/DP.

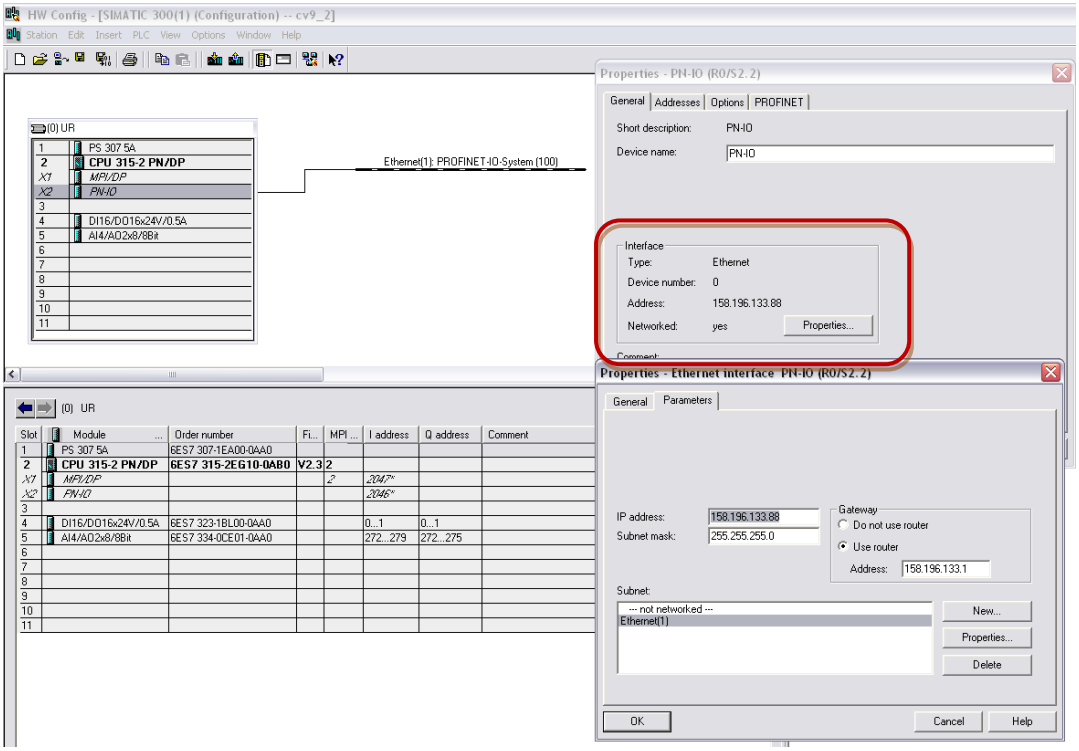
Komunikace mezi PLC a PC se nastaví v hardwarové konfiguraci. Po vložení lišty RACK, zdroje a CPU 315PN/DP (6ES7 315-2EG10-0AB0) vyskočí podobné dialogové okno jako v řešené úloze 9.3. V okně se vyplní maska podsítě (255.255.255.0) a IP adresa (158.196.133.), která je danému programovatelnému automatu přidělena a je rovněž napsána na štítku na zařízení. Dále zaškrtněte použití routeru pomocí use router. IP adresa routeru v učebně je 158.196.133.1. Kliknutím na tlačítko New se v projektu vytvoří síť Ethernet. Kliknutím na tlačítko OK se dialogové okno nastavení komunikačního procesoru zavře. Kliknutím na tlačítko OK se dialogové okno nastavení komunikačního procesoru zavře.

Následně vložte do dalších slotů příslušné karty vstupů a výstupů podle konfigurace zapojení PLC v učebně.

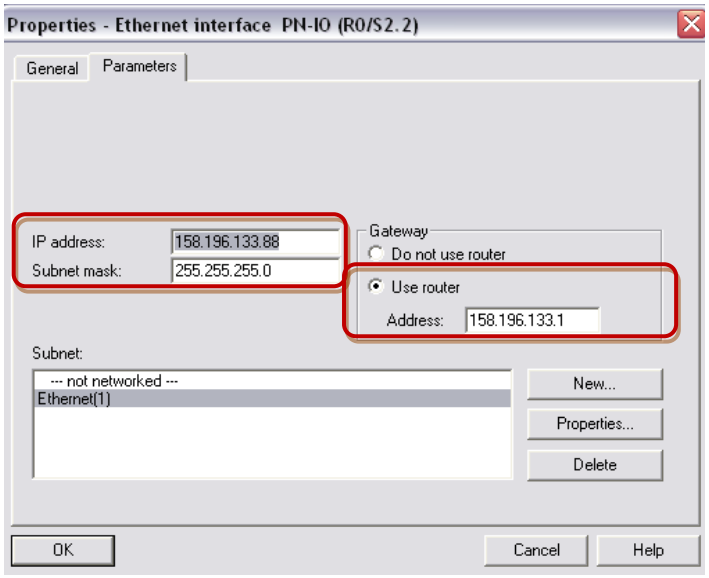
Pozn. Platí stejná poznámka jako v řešeném příkladu 9.3. Tedy pokud PLC ještě nebylo použito s daným komunikačním procesorem, pak nebude PLC ani připojený komunikační procesor znát zapsanou IP adresu. Když pak zvolíte v Set PG/PC interface nastavení komunikace na Ethernet, pak nebude možné konfiguraci do PLC nahrát, ani se k němu po ethernetu připojit. V tom případě je nutno konfiguraci nahrát přes MPI rozhraní. Až po úspěšném nahrání konfiguraci bude možné se k PLC a ke komunikačnímu procesoru připojit přes ethernet.



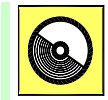
Obr. 9.4 Konfigurace komunikačního procesoru CPU 315PN/DP.



Obr. 9.5 Konfigurace komunikačního procesoru CPU 315PN/DP.

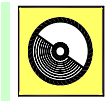


Obr. 9.6 Konfigurace komunikačního procesoru CPU 315PN/DP.



DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI9\



DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI9\

10. RT MODIFIKACE ETHERNETU

Čas ke studiu: 2 hodiny

Cíl Po prostudování této kapitoly budete znát základní vlastnosti čtyř často používaných variant průmyslového Ethernetu:

- Profinet
- Ethernet Powerlink
- EtherNET/IP
- EtherCAT

Výklad

V současnosti je velký požadavek ze strany zákazníků na plně integrovanou automatizaci s možnosti využití ať již stávajících komunikačních sběrnic nebo jejich doplnění a rozšíření o nové sběrnice s vyšší flexibilitou. Často zákazníci mají požadavky na vzdálenou diagnostiku modulů připojených na danou sběrnici stejně tak, jako sběr naměřených dat z jednotlivých částí výroby a jejich archivace na všech úrovních výroby. Za tímto účelem se vyvíjejí a využívají průmyslové sběrnice typu non-real time (NRT) a real time (RT) sběrnice.

Tato kapitola je věnována přehledu části průmyslových real-time sběrnic, kde nejvýznamnějšími zástupci z této kategorie jsou sběrnice: Ethernet Powerlink, Profinet, EtherNET/IP a EtherCAT.

10.1. Profinet

Sběrnice Profinet využívá standardy používané v ethernetové komunikaci. Se sběrnicí Profinet přišla na trh firma Siemens, která mezi prvními ve spolupráci s firmou ANF Data uvedla na trh tuto sběrnici. Ve spolupráci s mezinárodní organizací Profibus International byl definován rozsáhlý standard nazvaný Profinet, který vycházel ze standardu Ethernet a umožňoval další možnosti, které nebyly do této doby možné s využitím sběrnice Ethernet, jak ji dnes známe [6].

Byla vyvinuta za účelem:

- Plné integrace s IT na vyšších úrovních.
- Zvýšení flexibility distribuované automatizace.
- Využití bezdrátových technologií v průmyslu.
- Zajištění odezvy v reálném čase.

Profinet se dělí na dvě skupiny Profinet RT a Profinet IRT. Se sběrnicí Profinet RT se setkáte na úrovni řídicích systémů, které neřídí časově kritické procesy. Typickým použitím sběrnice Profinet RT je ve spojení s programovatelnými automaty. Naproti tomu Profinet IRT, jak již z názvu vyplývá izochronní real time, se využívá pro časově kritické procesy. Tímto procesem mohou být více osé aplikace, kde je nutné využívat synchronizaci pohonů. Tyto aplikace naleznete v papírenském průmyslu, hutním průmyslu a také i v divadelní technice.

Sběrnice Profinet se ještě dále dělí na Profinet IO a Profinet CBA.

V oblasti řízení pohonů se ještě setkáte s pojmem - označením Profinet PN2.1, Profinet PN2.2. Pro řízení pohonů a jejich vzájemné synchronizace mezi jednotlivými měniči byl až do konce roku 2008 používán standard komunikace PN2.1. Označení PN2.1 v sobě skrývá především strukturu komunikace mezi účastníky s přesně definovaným telegramem. Přibližně od začátku roku 2009 přišly na trh zařízení podporující standard komunikace PN2.2. Výhoda použití standardu PN2.2 oproti PN2.1 je především v optimalizaci rychlosti přenosu a navýšení rychlosti na sběrnici díky tomu, že byly optimalizovány přenosové rámce. Nyní se vyrábí již všechna zařízení s podporou verze PN2.2, která jsou většinou i zpětně kompatibilní s verzí PN2.1.

S uvolněním protokolu PROFISafe V2 je možné také na sběrnici Profinet připojovat bezpečnostní moduly a využívat tuto sběrnici jak k přenosu standardních tak bezpečnostních informací anebo v rámci TIA (Totally Integrated Automation), přenášet bezpečnostní informace mezi jednotlivými sběrnicemi [6].

Profinet IO

Profinet IO zavádí vztah IO- Device a IO-Controller.

IO-Device má přímý přístup k jednotlivým vstupně/výstupním signálům a provádí vzorkování těchto vstupně/výstupních dat v pravidelných časových okamžicích.

IO-Controller načítá tyto data nepřímo prostřednictvím obrazu vstupů/výstupů a zajišťuje spojení mezi účastníky za účelem přenosu dat.

Profinet IO se dělí do tří tříd [6]:

- RTclass 1 – cyklus sběrnice 1-4ms. Tuto skupinu využívají zejména programovatelné automaty.
- RTclass 2 (IRTflex) – cyklus sběrnice do 500mikrosekund. Je zde synchronizován příjem a odesílání.
- RTclass 3 (IRTtop) –Tato sběrnice se využívá v oblasti řízení pohonů.

Obě dvě varianty IRTflex a IRTtop využívají ke své činnosti speciálního hardwaru a vztahu SyncMaster, SyncSlave v projektu.

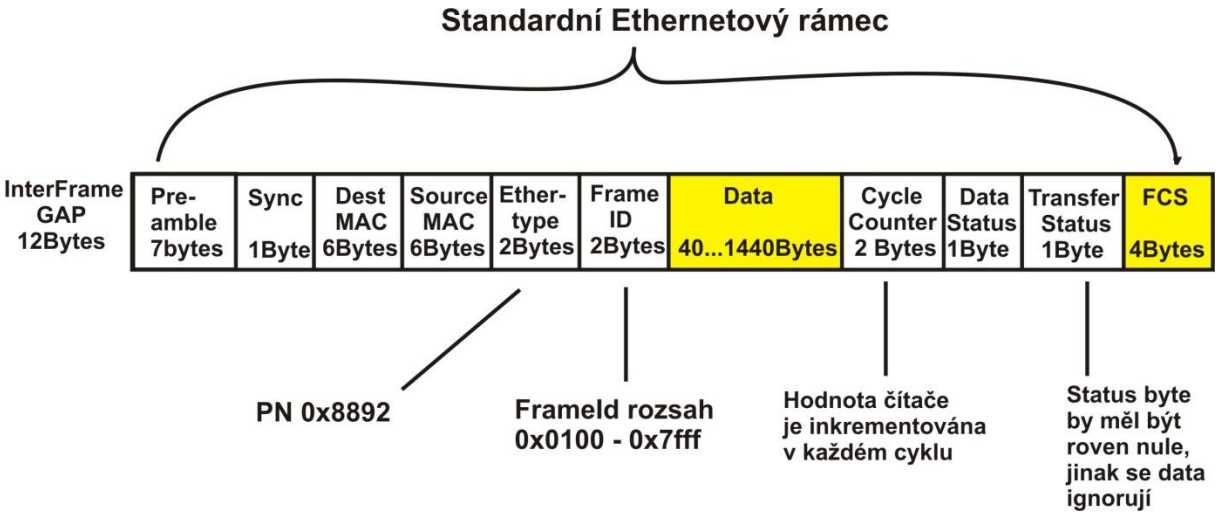
Každé zařízení je popsáno GSDML souborem. Tento GSDML soubor byl vytvořen z GSD souborů (Generic Station Description), které známe ze sběrnice Profibus-DP. GSD soubor byl upraven a vznikl nový standard nazývaný GSDML, který vychází z jazyka XML. XML soubor obsahuje informace o daném zařízení: komunikaci, konfigurační data a jeho možnosti rozšíření. XML soubory jsou editovatelné v jakémkoliv XML editoru a využívají standardizovanou XML strukturu.

Profinet IO s IRTtop

Základní vlastnosti [6]:

- Známá topologie – před uvedením do provozu zařízení využívající Profinet IRT musí tyto zařízení znát vlastní síť. Pokud je nutné sběrnici změnit, znamená to většinou přepis všech konfigurací jednotlivých zařízení.
- Precizní časování – tato vlastnost je velmi důležitá, protože vysílání jednotlivých frame je plánováno.
- Možnost synchronizace dalších zařízení – Profinet IRT dovoluje na sběrnici připojit nejenom řídicí jendotky pro frekvenční měniče např. SIMOTION, ale také je možné na stejnou sběrnici připojit i další zařízení např. jednotky vzdálených vstupů a výstupů, které budou pracovat v izochronním režimu.
- Cyklická výměna dat s dobou cyklu 0,25-4ms.
- 1440 byte pro uživatelská data.

- Komunikační cyklus je rozdělen na intervaly pro IRTtop a NRT.
- IRTtop framy jsou zasílány plánovaně.
- V NRT intervalech jsou framy přepínány jak přichází.
- Velikost každého frame je optimalizována.

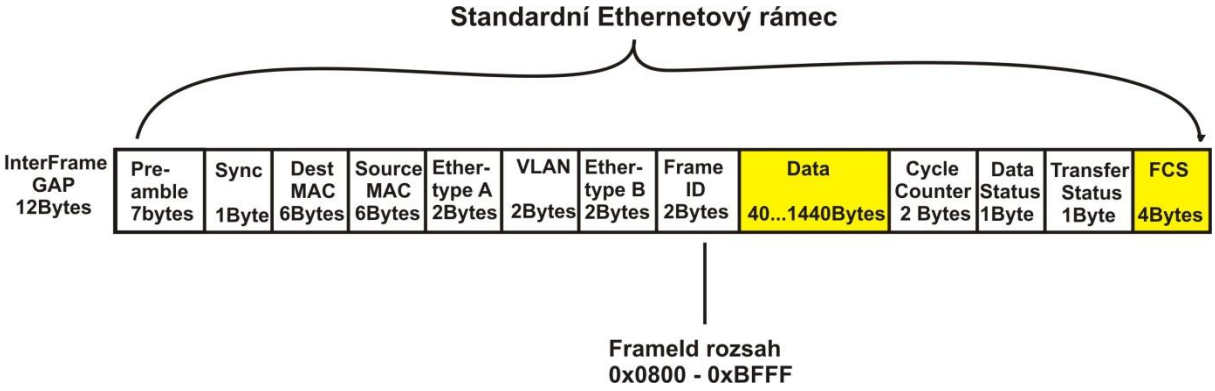


Obr.10.1 Standardní Ethernetový rámce a jeho modifikace pro profinet IRTtop (upraveno z [5]).

Profinet IRTtop využívá při komunikaci pevných cyklů a naplánovaných frame. V těchto komunikačních cyklech se přenáší jak IRT data tak i NRT data.

Profinet IO s IRTflex

- Frame se zasílá pokud jsou známy MAC adresy jednotlivých zařízení.
- IRTflex využívá rezervované časové intervaly.
- Aplikace nejsou synchronizovány.
- Cyklická výměna dat s dobou cyklu 1-4ms.
- 1440 byte pro uživatelská data.
- Komunikační cyklus je rozdělen na IRTflex a NRT intervaly.
- IRTflex framy jsou zasílány v rezerovaných časových intervalech.
- Velikost každého intervalu je rozdělena na 50% délky cyklu.
- IRT flex využívá precizního časování.
- Synchronizační framy jsou zasílány v NRT časových intervalech.
- Pro IRTflex se využívají standardní NRT framy.



Obr.10.2 Standardní ethernetový rámec a jeho modifikace pro profinet IRTflex (upraveno z [5]).

Tab.10.1: Srovnání vlastností jednotlivých verzí Profinet IO.

	RT (Class 1)	IRTflex (Class 2)	IRTtop (Class 3)
Požadavky na využití speciálního HW	NE	IRT switch	IRT switch
Pevná topologie a časové plánování	NE	NE	ANO
Při přenosu dat využití rezerovaných intervalů	NE	ANO	ANO
Rezervované velikosti	NE	ANO – pevná délka 50%	Využití přibližně 15%
Synchronizovaná komunikace	NE	ANO	ANO
Délka periody pro synchronizaci	NE	~30ms	0.25 – 30ms
Délka cyklu	1-128ms	1-4ms	0.25-4ms
Měření zpoždění při přenosu	NE	ANO	ANO

Profinet CBA

Profinet CBA se využívá v procesní automatizaci, kde jednotlivé části procesu se pravidelně opakují je možné je začlenit do komponent, kde tyto komponenty reprezentují nějaký technologický proces.

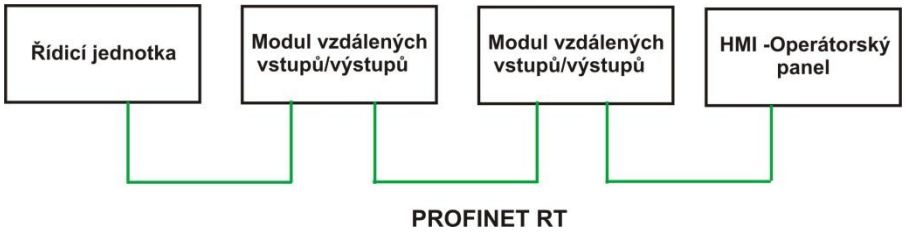
Pro programování se využívá programovací balík SIMATIC iMAP.

Možnosti zapojení sběrnice Profinet

Pro vzájemné propojení všech modulů umístěných na sběrnici se využívají tyto topologie - sběrnicová, kruhová, stromová, zapojení do hvězdy. Každá topologie své výhody a nevýhody. V průmyslu se používají všechny typy topologií. Sběrnicová topologie zajistí minimalizaci nákladů na kabely s přihlédnutím k tomu, že je nutné dbát na to, aby množství použitých switchů nezpomalilo také celkový cyklus sběrnice. Kruhová topologie zajistí zvýšenou spolehlivost [6].

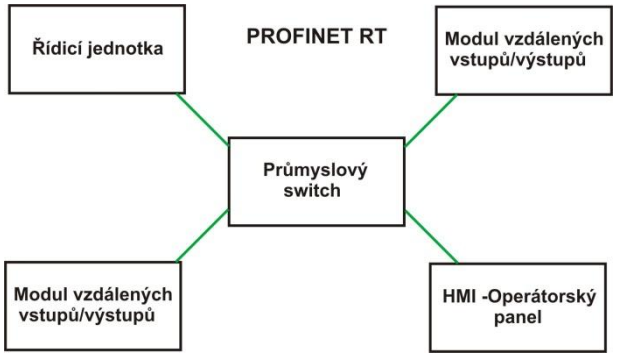
Při návrhu komunikačního systému se musí přihlédnout k tomu, jestli se bude po sběrnici přenášet pouze RT komunikace nebo IRT. Pokud všechny zařízení budou pouze komunikovat s využitím RT komunikace, tak zapojení topologie sběrnice je jednoduché. Je možné využívat jakoukoliv sběrnicovou topologii z výše uvedených. Pokud bude nutné aby někteří z účastníků využívali také IRT komunikaci je nutné k této skutečnosti přihlédnou při návrhu.

Níže je uveden příklad návrhu topologie systému využívající Profinet RT. Většina výrobců vyrábějící komunikační moduly podporující Profinet integrují do svých zařízení také dvouportové switche. V příkladu návrhu je využito této skutečnosti. Jak je vidět, tak zařízení jsou vzájemně propojeny a dokonce může být i k této sběrnici připojen nějaký operátorský panel. Všechny moduly musí mít přidělenu jak IP adresu, tak jednoznačné jméno. Více je uvedeno v řešeném příkladu na konci kapitoly.



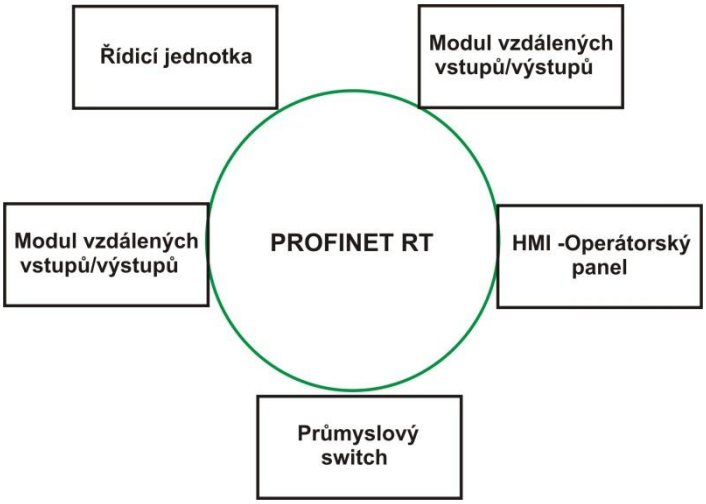
Obr.10.3 Příklad návrhu využívající sběrnicovou topologii.

Někdy se s výhodou využívá topologie typu hvězda zejména, když moduly nemají integrovaný v sobě switch. V tomto okamžiku je nutné využívat průmyslový switch.



Obr. 10.4 Příklad návrhu využívající topologii typu hvězda.

Pro zajištění vyšší spolehlivost se využívá kruhové topologie. V tomto zapojení musí být ale použito nějaké zařízení, které umí směrovat komunikaci. Nejčastěji se za tímto účelem využívá průmyslový switch, který dokáže danou komunikaci v případě ztráty spojení s jakýmkoliv účastníkem jinak přesměrovat. Průmyslový switch přesměruje komunikaci přibližně až za 200ms.



Obr. 10.5 Příklad návrhu využívající kruhovou topologii.

Pokud je nutné využívat komunikaci mezi jednotlivými účastníky Profinet IRT a zároveň komunikovat mezi účastníky s využitím Profinetu RT, tak je nutné dodržet také základní pravidlo, že zařízení podporují Profinet RT nesmí být vloženo mezi dva účastníky komunikující s využitím IRT Profinetu. Zařízení podporující Profinet RT musí být umístěno na konec sběrnice s IRT komunikací.

Návrh sběrnice, na které bude probíhat IRT komunikace, musí také zohlednit zatížení sběrnice, aby v něm byl dostatek časového prostoru, jak pro přenos dalších RT a non RT komunikací apod. Z tohoto důvodu se musí věnovat zvláštní pozornost při konfiguracích více osých aplikací pro polohovací aplikace.

10.2. Ethernet Powerlink

Ethernet Powerlink je další významnou sběrnicí pro řízení v reálném čase. Ethernet Powerlink byl vyvinut firmou Bernecker Rainer a později byl přijat jako standard organizací EPSG (Ethernet Powerlink Standardization Group). Ethernet Powerlink využívá vlastností systému Ethernet a proto nevyžaduje využití speciálního hardware. Ethernet Powerlink využívá především důsledné časové rozdělení přenosového cyklu na část izochronní (cyklický přenos časově kritických dat v reálném čase a asynchronní (přenos časově nekritických dat protokolem IP). Jako další mechanismus směřující k determinismu používá Ethernet Powerlink modifikovaný způsob tvorby bezkolizních domén při použití rozbočovačů hub s opakováním zpráv na místo jinak standardně používaných přepínačů switch, které by zanášely do izochronní rychlé části nežadoucí zpoždění, a dále důsledné oddělení segmentů sítě pracujících v reálném čase od těch, které práci v reálném čase nepodporují. Standard Ethernet Powerlink využívá komunikační model producent/konzument, což opět vede k většímu výkonu a propustnosti sítě. Pro deterministickou synchronizaci izochronních přenosů dále zavádí mechanismy synchronizace prostřednictvím distribuovaných hodin reálného času podle standardu IEEE 1588. Ethernet Powerlink umožňuje vytvořit síť s jakoukoliv topologií, neboť tvorba bezkolizních domén je vyřešena realizací arbitra přenosu a přiřazením časových oken jednotlivým uzlům (stanicím) v síti. Standard EPL koresponduje s odpovídajícími standardy IEEE i EN a členové EPSG jsou pro mezinárodní standardizaci metody EPL členy standardizačních projektů IEC 61784-2 Real-time Ethernet, IEC 61800-7 Power Drive Systems a ISO 15745 XML–based Description. Pro své vynikající vlastnosti z hlediska reálného času je Ethernet Powerlink velmi často používán zejména v oblasti řízení strojů [3].

10.3. EtherNET/IP

EtherNET/IP je dalším velmi rozšířeným standardem používanýn v průmyslu. EtherNET/IP je plně kompatibilní s ethernetem TCP/IP a je určen pro přenos dat v reálném čase. EtherNET/IP byl vyvinut několika výrobci, kteří jsou členy asociace ODVA (Open DeviceNET Vendor Association) a ControlNet International (CI) v čele s firmou Rockwell Automation.

Výhoda sítě EtherNET/IP je využívaný systém pro přenos dat – producent konzument, využití standardního Ethernetu a síťových komponent podporující přenosové rychlosti od 10Mbps do 1Gbps.

Profily zařízení a aplikační vrstva EtherNETu/IP jsou tvořeny protokolem Common Industrial Protocol (CIP). Pro přenos dat v síti EtherNET/IP se využívá vztahu producent konzument, zatímco jedno zařízení vysílá může jedno nebo více zařízení ve stejném časovém okamžiku data přijímat. Hlavní výhoda využívaného vztahu producent-konzument je využívaná šířka pásma. [1]

CIP protokol je využíván kromě EtherNETu/IP také sběrnicí DeviceNet a ControlNet. Každé zařízení na síti je reprezentováno skupinou objektů. Příkaz se skládá z datové části, potřebných služeb a služeb. Existují tři skupiny objektů – povinné, aplikační a objekty definované výrobcem. Povinnými objekty jsou:

- Objekt identifikující zařízení.
- Objekt specifikující předávání zpráv.
- Objekt specifikující předávání zpráv.
- Objekt pro správu spojení.
- Jeden nebo několik objektů s parametry konfigurace komunikační sítě.

Aplikační objekty obsahují data specifická pro komunikující zařízení a jsou vázány na typ a funkci těchto zařízení. Skupina aplikačních objektů tvoří profil zařízení. Výrobci si mohou specifikovat i vlastní zvláštní objekty. Aby bylo zřejmé, které objekty jsou v daném zařízení charakterizovány, jsou pro jednotlivá zařízení sestaveny tzv. elektrické popisy zařízení, které obsahují základní informace potřebné pro konfigurování zařízení pro síť EtherNet/IP.

Pro komunikaci prostřednictvím Ethernetu využívá síť EtherNet/IP standardní porotkoly ze skupiny TCP/UDP/IP. Podle způsobu přenosu existují v síti EtherNet/IP dva způsoby komunikace – explicitní a implicitní. [3]

Na úrovni síťové vrstvy se zprávy CIP zapouzdřují do paketů TCP nebo UDP. Protokol CIP nabízí dva základní mechanismy komunikace – spojovanou a nespojovanou službu.

Komunikační model objektů CIP typu producent-konzument umožňuje lépe využít možnosti komunikačního kanálu. Uzel, který zahajuje spojení, je označován jako žadatel o spojení, cílový uzel spojení je označován jako příjemce spojení. Žadatel nejprve odešle nespojovanou explicitní zprávu s žádostí o vytvoření spojení, která obsahuje navrhované parametry spojení. Jestliže je cílový uzel schopen spojení navázat, odesílá potvrzení s přesnými parametry a navazuje spojení. Mezi parametry spojení patří:

- Identifikátor.
- Způsob přenosu.
- Spouštěcí mechanismus přenosu dat (cyklická data, změna stavu).
- Počet a formát přenášených údajů (každý směr zvlášť).

Každé spojení s CIP je určeno jednoznačným identifikátorem a to jednotlivě pro každý směr přenosu. Typ spojení je závislý na charakteru a způsobu odesílání dat. Spouštěcí mechanismus v síti EtherNet/IP může být pouze cyklický nebo změna stavu. Počet přenášených údajů může být i nulový a tehdy jde o zprávu indikující správnou funkci zařízení. Implicitní zprávy (I/O data) mohou

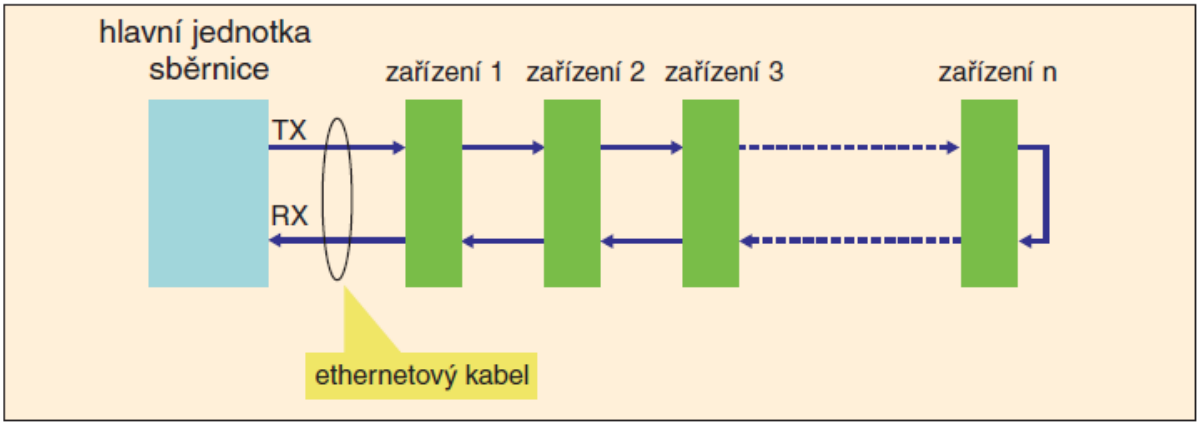
být v síti EtherNet/IP odesílány jednotlivým účastníkům nebo jako hromadné. Jestliže se chce k již existujícímu spojení připojit další zařízení, posílá žádost o příjem a poté zde může poslouchat v modu multicast. Nešlo-li o vysílání typu multicast, je příjemcem spojení vyhrazena nová adresa pro multicast a žádající uzel je o tom informován. Parametry v módu multicast jsou určeny v procesu zřizování spojení. [3]

Standard EtherNet/IP není primárně určen pro úlohy řízení v reálném čase. Pro zajištění vlastností reálného času používá EtherNet/IP pouze základní mechanismy, jako je rozdělení kolizních domén s použitím přepínačů a oddělování segmentů, nebo spoléhá na dostatečnou rychlost Ethernetu. Při každém jeho použití je proto nutné zvážit, zda možná zpoždění nebo ztráty dat jsou přijatelné. V případně náročnějších úloh, jako je např. řízení pohonů při použití objektů CIP Motion, nabízí EtherNet/IP mechanismus objektu CIP Sync. Mechanismus CIP Sync umožňuje řešit synchronizaci na principu distribuovaných hodin podle standardu IEEE1588. [3]

10.4. EtherCAT

EtherCAT (Ethernet for Control Automation Technology) byl vyvinut pro rychlý přenos dat s krátkým cyklem na sběrnici, především pro přenos procesních dat. EtherCAT uvedla na trh skupina dodavatelů EtherCAT Technology Group spolu s firmou Beckhoff, která je autorem sběrnice. EtherCAT využívá standardní Ethernetové framy podle IEEE 802.3.

U standardu EtherCAT není paket rámce Ethernetu přijímán každým účastníkem déle, než jsou zpracovávána a přenášena data. Rámec Ethernetu je zpracováván během příjmu rámce. Zařízení pro EtherCAT jsou většinou konstruována tak, že obsahují dva porty čímž je umožněno, že data prochází skrz zařízení. Hlavní jednotka vyšle data sběrnici. Při průchodu rámce každým zařízením, zařízení pro které jsou data určena, data čte během toho, jak dále rámec prochází na další zařízení. Pokud další zařízení chce nějaká data zaslat dalšímu zařízení, tak ukládá tyto data do rámce při průchodu rozhraním, takže zdržení v každém účastníku síti je velmi malé řádově nanosekundy. Tím je dosaženo velmi vysoké přenosové rychlosti. Pokud je nutné přenést real time data, tak těmto datům jsou přiřazeny vyšší priority, než mají ostatní data např. určená pro diagnostiku apod.



Obr. 10.6 EtherCAT (upraveno z [2]).

V síti EtherCAT je možná komunikace typu Broadcast, Multicast a komunikace mezi slave zařízeními. EtherCAT podporuje téměř všechny topologie. Pro ethernetovou síť, která bude využívána sběrnicí EtherCAT, může být tvořena jak metalickými tak optickými kabely.

EtherCAT může přenášet max. 1486B procesních dat v jednom ethernetovém frame.

Na sběrnici EtherCAT mohou být kromě standardních programovatelných automatů a dalších zařízení připojeny také zařízení pro řízení pohonů, protože sběrnice EtherCAT umožňuje přenášet real time data. [2]

Shrnutí pojmů

Profinet je jednou z nejpoužívanějších variant průmyslového Ethernetu. Dělí se na dvě skupiny **Profinet RT** a **Profinet IRT**. Se sběrnicí Profinet RT se setkáte na úrovni řídicích systémů, které neřídí časově kritické procesy. Typickým použitím sběrnice Profinet RT je ve spojení s programovatelnými automaty. Naproti tomu Profinet IRT, jak již z názvu vyplývá izochronní real time, se využívá pro časově kritické procesy. Tímto procesem mohou být více osé aplikace, kde je nutné využívat synchronizaci pohonů. Další možnosti dělení variant Profinetu jsou Profinet IO a Profinet CBA.

Ethernet Powerlink je další významnou sběrnicí pro řízení v reálném čase. Ethernet Powerlink byl vyvinut firmou Bernecker Rainer a později byl přijat jako standard organizací EPSG (Ethernet Powerlink Standardization Group).

EtherNET/IP je také velmi rozšířeným standardem používanýn v průmyslu. EtherNET/IP je plně kompatibilní s ethernetem TCP/IP a je určen pro přenos dat v reálném čase. EtherNET/IP je podporován firmami v čele s firmou Rockwell Automation. Výhoda sítě EtherNET/IP je využívaný systém pro přenos dat – producent konzument, využití standardního Ethernetu a síťových komponent podporující přenosové rychlosti od 10Mbps do 1Gbps.

EtherCAT byl vyvinut pro rychlý přenos dat s krátkým cyklem na sběrnici, především pro přenos procesních dat. EtherCAT uvedla na trh skupina dodavatelů EtherCAT Technology Group spolu s firmou Beckhoff, která je autorem sběrnice. EtherCAT využívá standardní Ethernetové framy podle IEEE 802.3.

Otázky

1. Popište základní vlastnosti Profinetu.
2. Jaké vatianty Profinetu znáte a kde se používají?
3. Popište Profinet RT a jeho základní vlastnosti.
4. Popište Profinet IRT a jeho základní vlastnosti.
5. Co znamená izochronní režim u komunikační sběrnice?
6. Popište základní vlastnosti Ethernet Powerlinku.
7. Popište základní vlastnosti sběrnice EtherNET/IP.
8. Popište základní vlastnosti sběrnice EtherCAT.

Použitá literatura a další zdroje

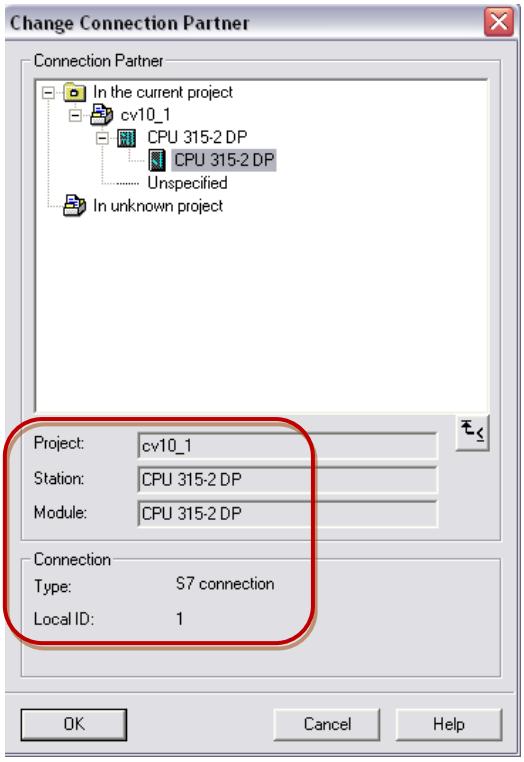
1. EtherNET/IP. [online], [cit. 03-08-2010] www.odva.org
2. EtherCAT. [online], [cit. 03-08-2010] www.ethercat.org
3. Zezulka F.; Hynčica O. Průmyslový Ethernet I-IX. Automa, 2007-2008. ISSN 1210-9592.
4. Siemens: SIMATIC Communication with SIMATIC System Manual, 12/2005, EWA 4NEB 710 6075-02 03
5. Siemens: SIMATIC Profinet System Description System Manual, 10/2006 A5E00298288-03

Řešená úloha 10.1

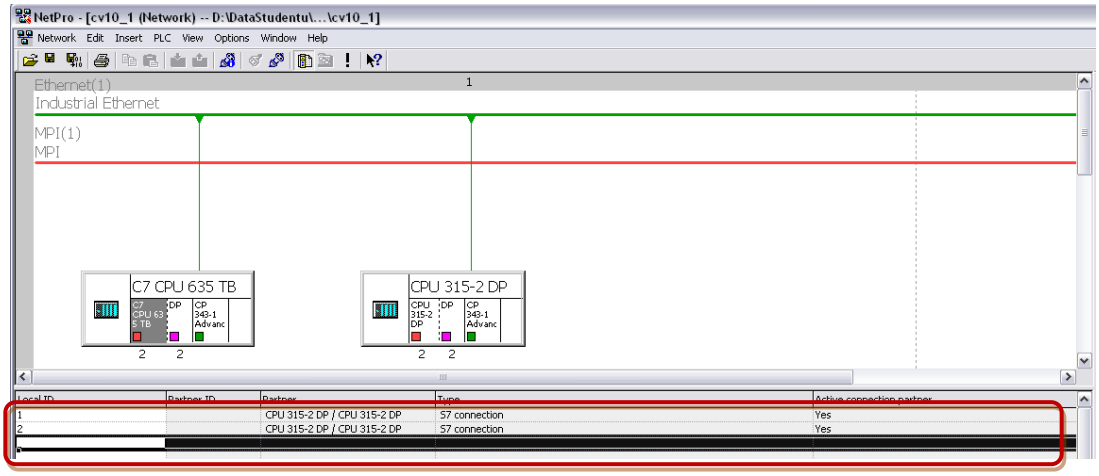
Zadání: Nastavte komunikaci mezi dvěma PLC (CPU 315-2DP a CPU C7 635 TB) po ethernetu (s7 connection). Pro komunikaci použijte funkce PUT a GET.
V PLC CPU C7 635 TB čtěte pomocí funkce GET prvních 5 hodnot datového bloku z PLC CPU 315-2DP. První hodnotu inkrementujte od 0 do 100, druhou inicializujte v OB100, třetí bude součtem, čtvrtá rozdílem a pátá součinem první a druhé hodnoty v datovém bloku.
Z PLC CPU C7 635 TB posílejte pět hodnot typu INTEGER do PLC CPU 315-2DP pomocí funkce PUT. Do druhé hodnoty datového bloku zapisujte z VAT tabulky, první hodnotu ve zvolené časové periodě dekrementujte od 100 do 0. Třetí hodnota bude součtem, čtvrtá hodnota rozdílem a pátá součinem první a druhé hodnoty.

Data posílejte a čtěte kontinuálně.

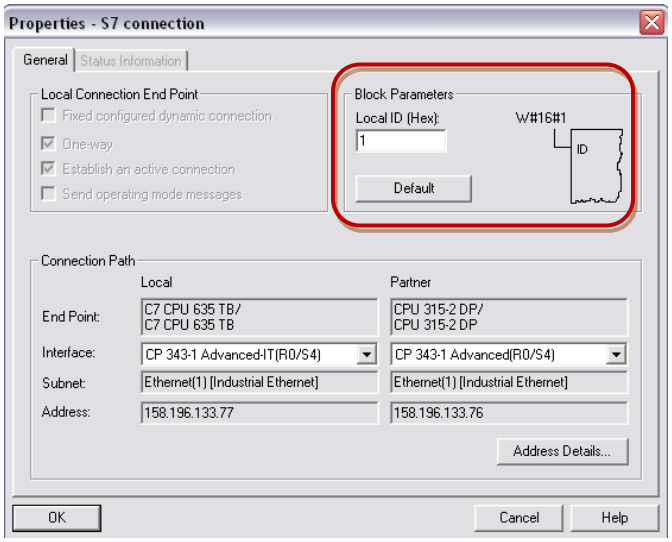
Základním krokem řešení úlohy je hardwarová konfigurace dvou PLC a nastavení komunikace mezi PLC. Konfigurace komunikace probíhá v nástroji NetPro, které se spouští z hlavního okna Simatic Manageru. Klinutím na CPU se dole v okně zobrazí tabulka komunikačních připojení. Pomocí pravého tlačítka vložte nové připojení (Insert New Connection). Definujte, se kterým CPU bude komunikace probíhat a nastavte typ komunikačního spojení (s7 connection). Nastavení potvrďte stiskem tlačítka OK. Objeví se okno Properties, kde nastavte parametry komunikace (ID komunikace). Parametry v ostatních záložkách nechte defaultní. Parametr ID se následně bude používat v programu jako vstupní parametr funkcích bloků GET a PUT. Nastavení v NetPro uložte a zkompilujte.



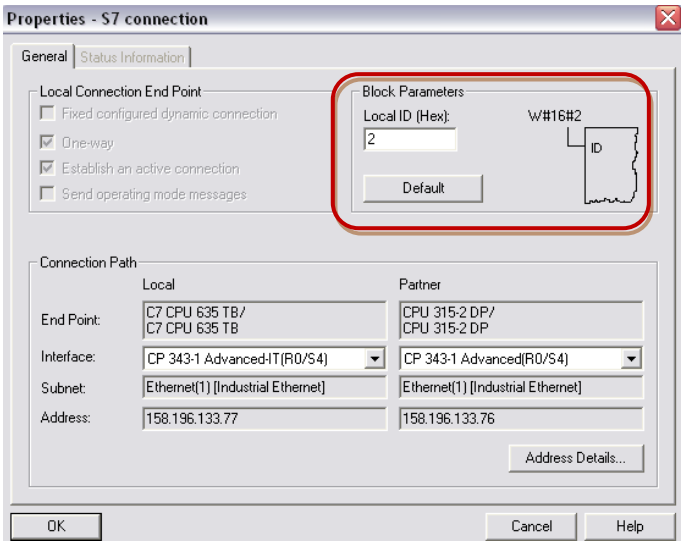
Obr. 10.7 Nastavení S7 komunikace.



Obr. 10.8 Nastavení S7 komunikace.



Obr. 10.9 Nastavení S7 komunikace.



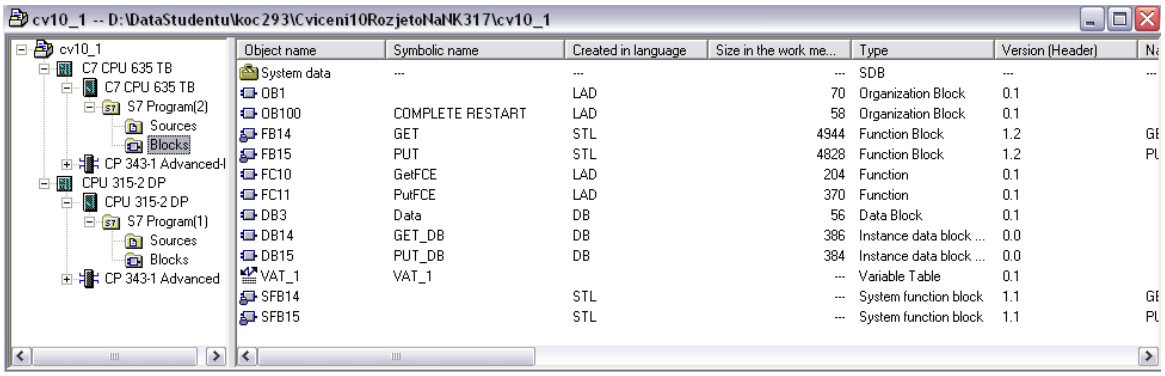
Obr. 10.10 Nastavení S7 komunikace.

Pomocí funkčního bloku FB14 „GET“ lze číst data z komunikačního partnera. Žádné odpovídající FB na straně komunikačního partnera v tomto případě není. Čtení je aktivováno po zavolání FB s parametrem REQ = 1. Přijímání pokračuje, dokud není indikováno přijetí dat v DONE = 1 (náběžná hrana).

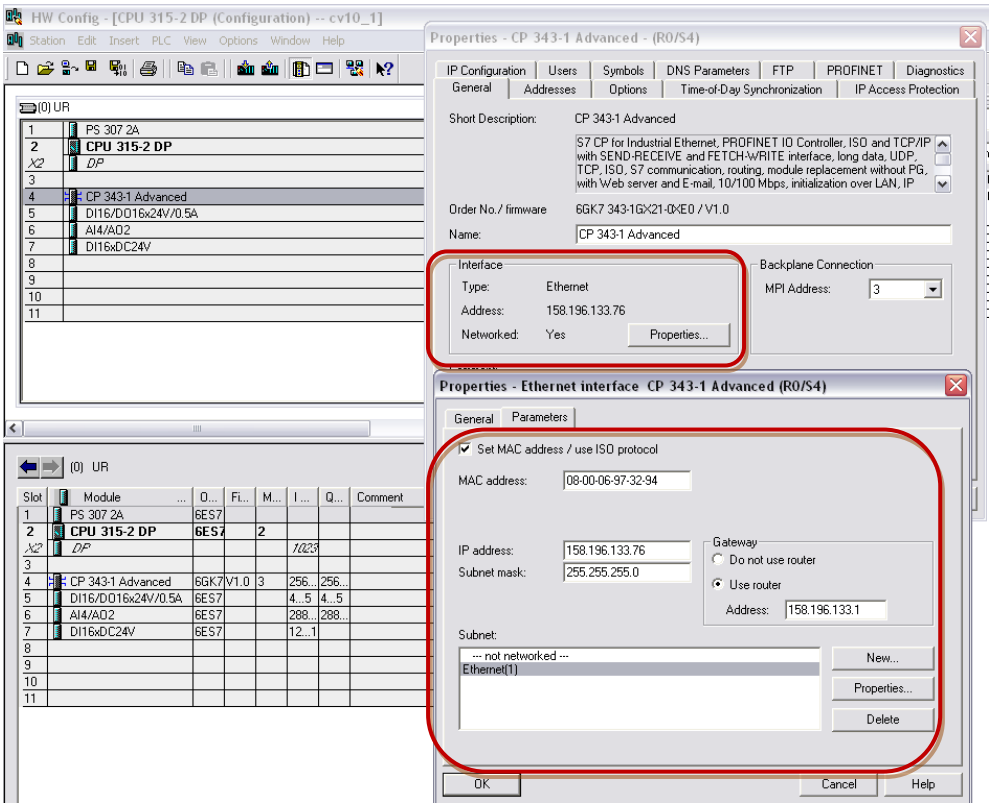
Musí být zajištěno, že přijímací oblast je definována pomocí RD_1 parametru (u přijímacího CPU) a je přinejmenším stejně velká, nebo větší, než čtená oblast definovaná pomocí ADDR_1 (u komunikačního partnera).

Pomocí funkčního bloku FB15 „PUT“ lze zapisovat data do oblasti paměti komunikačního partnera. Žádné odpovídající FB na straně komunikačního partnera v tomto případě není. Zapisování je aktivováno voláním FB s REQ = 1. Přijímání pokračuje, dokud není indikováno potvrzení přijetí dat v DONE = 0 (náběžná hrana).

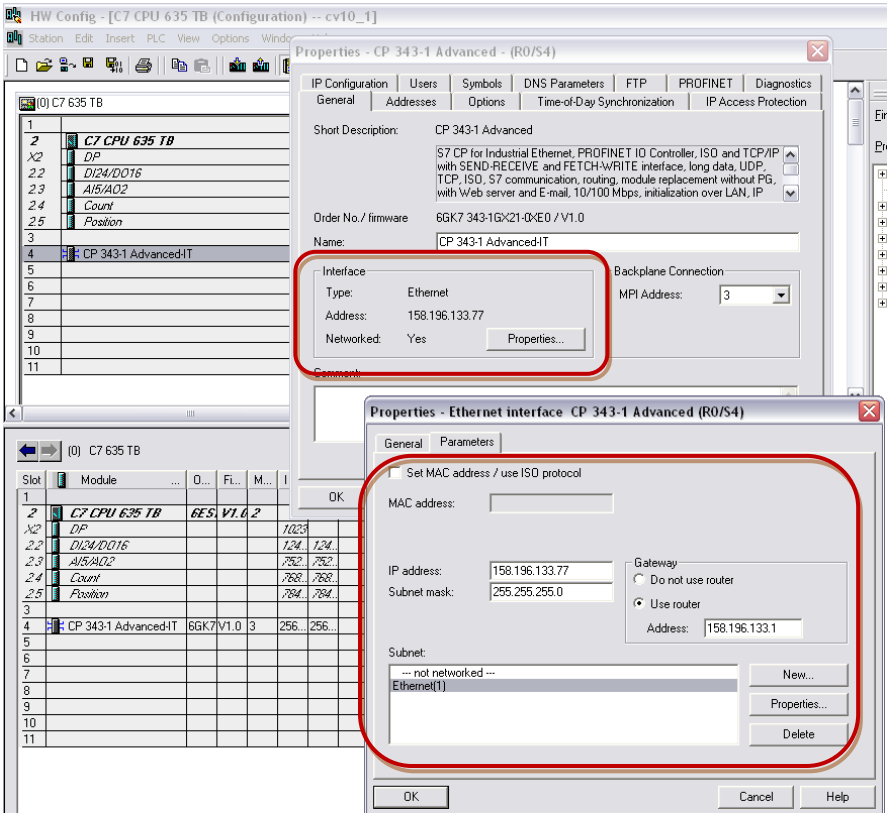
Stejně jako u GET musí být zajištěno, že přijímací oblast je definována pomocí ADDR_1 parametru (u přijímacího CPU) a je přinejmenším stejně velká, nebo větší, než přijímací oblast definovaná pomocí SD_1 (u vysílacího CPU).



Obr. 10.11 Nastavení S7 komunikace.



Obr. 10.12 Nastavení S7 komunikace.



Obr. 10.13 Nastavení S7 komunikace.

Program v LAD

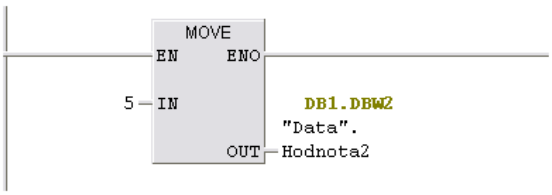
PLC1: S7315-2DP:

S7 Program(1) (Symbols) -- cv10_1\CPU 315-2 DP\CPU 315-2 DP

	Status	Symbol	Address	Data type	Comment
1		COMPLETE REST...	OB 100	OB 100	Complete Restart
2		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
3		Data	DB 1	DB 1	
4		VAT_1	VAT 1		
5					

OB100:

```
OB100 :  "Complete Restart"
Comment:
Network 1: Title:
Comment:
```



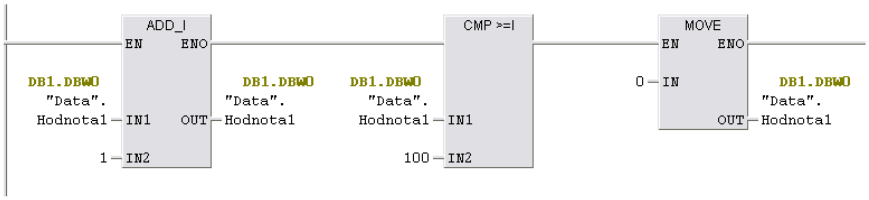
OB35:

OB35 : "Cyclic Interrupt"

Comment:

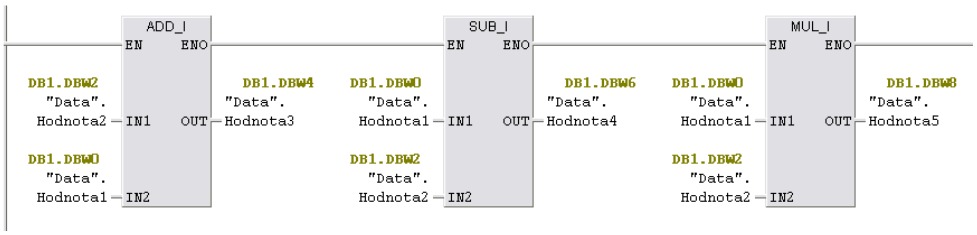
Network 1: Title:

Comment:



Network 2: Title:

Comment:



DB1:

DB1 -- "Data" -- cv10_1\CPU 315-2 DP\CPU 315-2 DP\...\DB1

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	Hodnota1	INT	0	
+2.0	Hodnota2	INT	0	
+4.0	Hodnota3	INT	0	
+6.0	Hodnota4	INT	0	
+8.0	Hodnota5	INT	0	
+10.0	Hodnota6	INT	0	
+12.0	Hodnota7	INT	0	
+14.0	Hodnota8	INT	0	
+16.0	Hodnota9	INT	0	
+18.0	Hodnota10	INT	0	
=20.0		END_STRUCT		

VAT tabulka:

VAT_1 -- @cv10_1\CPU 315-2 DP\CPU 315-2 DP\S7 Pro...

	Address	Symbol	Display format	Status value	Modify value
1	//Data				
2	DB1.DBW 0	"Data".Hodnota1	DEC	18	
3	DB1.DBW 2	"Data".Hodnota2	DEC	5	
4	DB1.DBW 4	"Data".Hodnota3	DEC	23	
5	DB1.DBW 6	"Data".Hodnota4	DEC	13	
6	DB1.DBW 8	"Data".Hodnota5	DEC	90	
7	DB1.DBW 10	"Data".Hodnota6	DEC	24	
8	DB1.DBW 12	"Data".Hodnota7	DEC	10	
9	DB1.DBW 14	"Data".Hodnota8	DEC	34	
10	DB1.DBW 16	"Data".Hodnota9	DEC	14	
11	DB1.DBW 18	"Data".Hodnota10	DEC	240	
12					
13					

PLC2: C7 CPU 635 TB:

Tabulka symbolů:

S7 Program(2) (Symbols) -- cv10_1\C7 CPU 635 TB\C7 CPU 635 TB

	Status	Symbol	Addres	Data type	Comment
1		Data	DB 3	DB 3	
2		GET_DB	DB 14	FB 14	
3		PUT_DB	DB 15	FB 15	
4		GET	FB 14	FB 14	Read Data From a Remote C...
5		PUT	FB 15	FB 15	Write Data to a Remote CPU
6		GetFCE	FC 10	FC 10	
7		PutFCE	FC 11	FC 11	
8		Req_Get	M 10.0	BOOL	
9		StatusParam_Get	M 10.1	BOOL	
10		Error_Get	M 10.2	BOOL	
11		Req_Put	M 20.0	BOOL	
12		DoneParam_Put	M 20.1	BOOL	
13		Error_Put	M 20.2	BOOL	
14		1Hz	M 100.5	BOOL	
15		Status_Get	MW 12	WORD	
16		Status_Put	MW 22	WORD	
17		COMPLETE REST...	OB 100	OB 100	Complete Restart
18		Get_Timer	T 1	TIMER	
19		Put_Timer	T 2	TIMER	
20		VAT_1	VAT 2		
21					

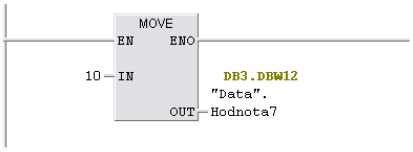
OB100:

OB100 : "Complete Restart"

Comment:

Network 1: Title:

Comment:



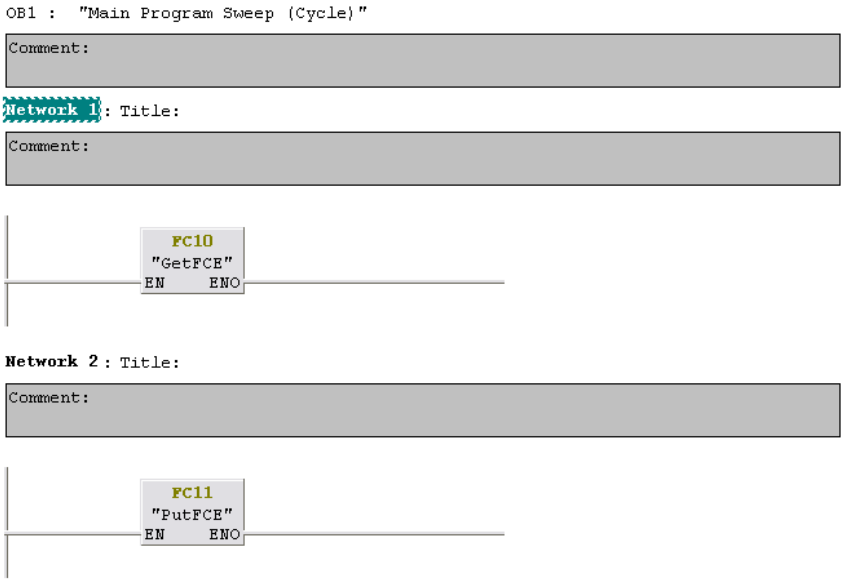
Network 2: Title:

Comment:

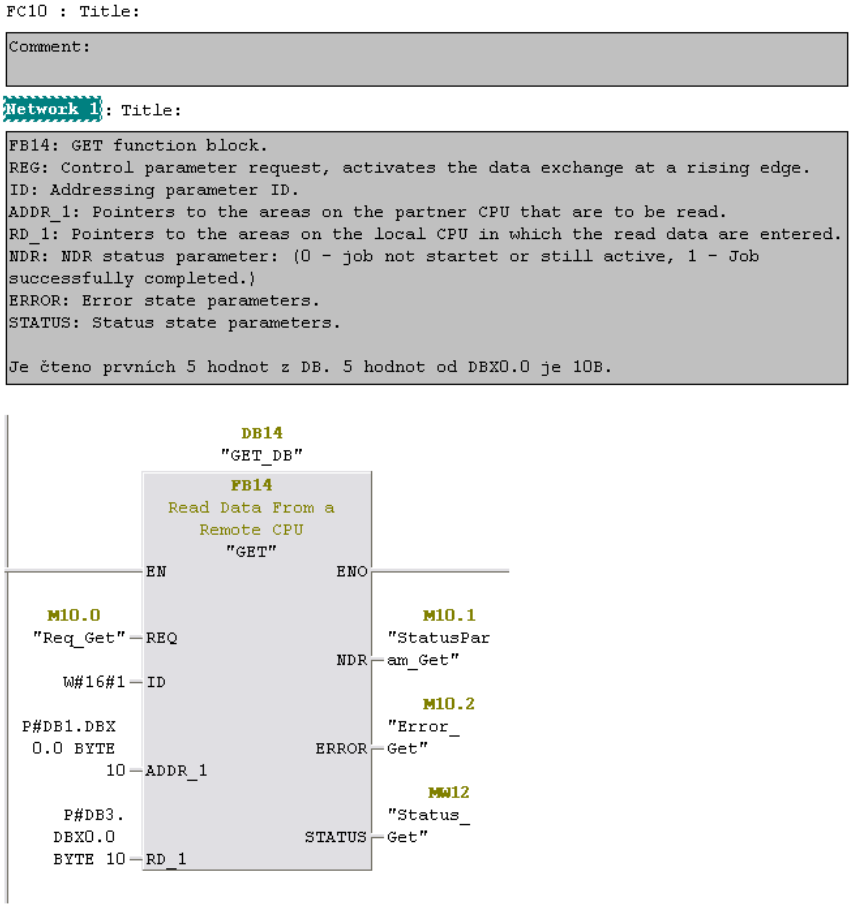
Network 3: Title:

Comment:

OB1:


OB1 : "Main Program Sweep (Cycle)"
Comment:
Network 1: Title:
Comment:
FC10
"GetFCE"
EN ENO
Network 2: Title:
Comment:
FC11
"PutFCE"
EN ENO

FC10:

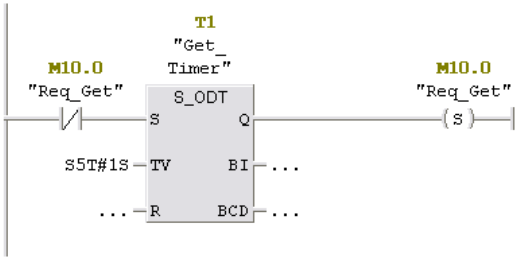

FC10 : Title:
Comment:
Network 1: Title:
FB14: GET function block.
REG: Control parameter request, activates the data exchange at a rising edge.
ID: Addressing parameter ID.
ADDR_1: Pointers to the areas on the partner CPU that are to be read.
RD_1: Pointers to the areas on the local CPU in which the read data are entered.
NDR: NDR status parameter: (0 - job not startet or still active, 1 - Job successfully completed.)
ERROR: Error state parameters.
STATUS: Status state parameters.
Je čteno prvních 5 hodnot z DB. 5 hodnot od DBX0.0 je 10B.
DB14
"GET_DB"
FB14
Read Data From a Remote CPU
"GET"
EN
ENO
M10.0
"Req_Get"
REQ
M10.1
"StatusPar am_Get"
NDR
W#16#1
ID
M10.2
"Error_ Get"
P#DB1.DBX 0.0 BYTE 10
ERROR
ADDR_1
MW12
"Status_ Get"
P#DB3. DBX0.0 BYTE 10
STATUS
RD_1

Network 2 : Title:

Comment:

Network 3 : Title:

Comment:



FC11:

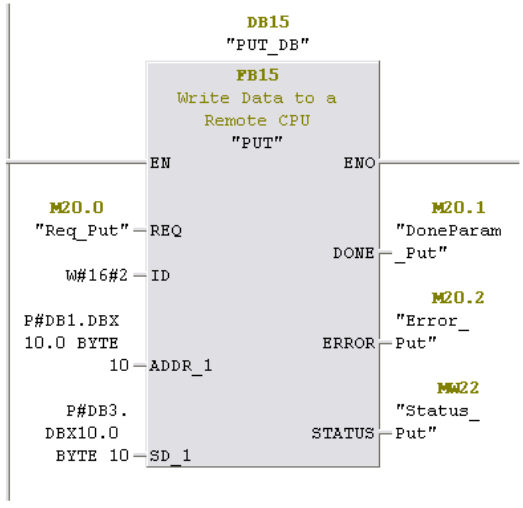
FC11 : Title:

Comment:

Network 1: Title:

FB14: PUT function block.
REG: Control parameter request, activates the data exchange at a rising edge.
ID: Addressing parameter ID.
ADDR_1: Pointers to the areas on the partner CPU in which the data is to be written.
SD_1: Pointers to the areas on the local CPU which contain the data to be sent.
DONE: DONE status parameter (0 - Job not started or still running, 1- Job has been executed error-free.
ERROR: Error state parameters.
STATUS: Status state parameters.

Je zapisováno posledních 5 hodnot z DB. 5 hodnot od DBX10.0 je 10B (od Hodnota6).

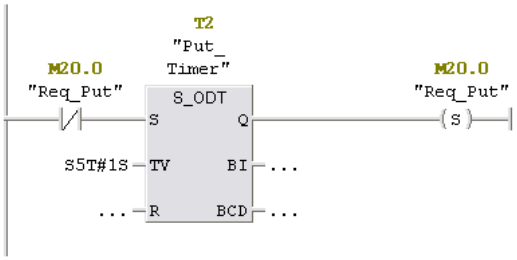


Network 2 : Title:

Comment:

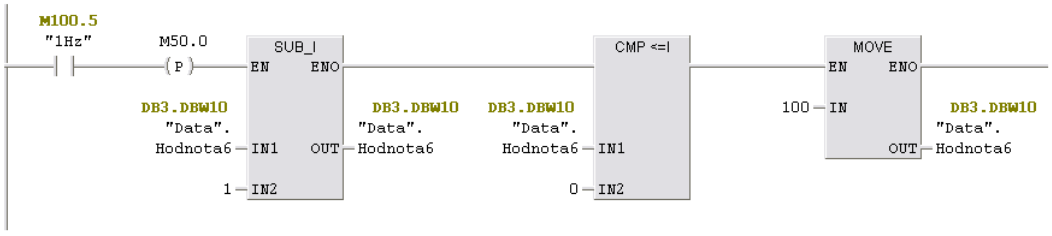
Network 3 : Title:

Comment:



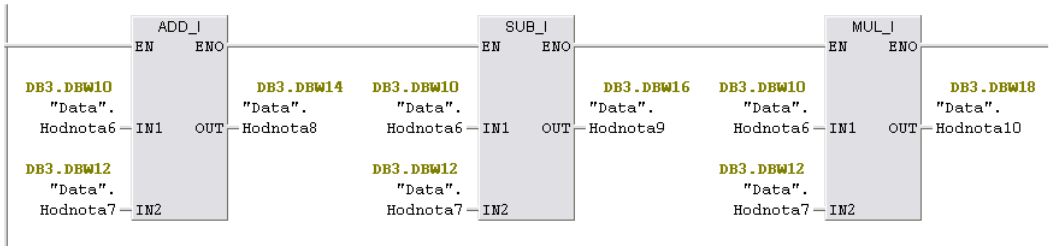
Network 4 : Title:

Dekrementuje Hodnota6 pro posilani.



Network 5 : Title:

Comment:



DB3:

DB3 -- "Data" -- cv10_1\C7 CPU 635 TB\C7 CPU 635 TB\...\DB3

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	Hodnota1	INT	0	
+2.0	Hodnota2	INT	0	
+4.0	Hodnota3	INT	0	
+6.0	Hodnota4	INT	0	
+8.0	Hodnota5	INT	0	
+10.0	Hodnota6	INT	0	
+12.0	Hodnota7	INT	0	
+14.0	Hodnota8	INT	0	
+16.0	Hodnota9	INT	0	
+18.0	Hodnota10	INT	0	
=20.0		END_STRUCT		

VAT tabulka:

Var - VAT_1

Table Edit Insert PLC Variable View Options Window Help

VAT_1 -- @cv10_1\C7 CPU 635 TB\C7 CPU 635 TB\S7 Program(2) ONLINE

	Address	Symbol	Display format	Status value	Modify value
3	M 10.1	"StatusParam_Get"	BOOL	false	
4	M 10.2	"Error_Get"	BOOL	false	
5	MW 12	"Status_Get"	DEC	0	
6					
7	//S7 Put				
8	M 20.0	"Req_Put"	BOOL	false	
9	M 20.1	"DoneParam_Put"	BOOL	false	
10	M 20.2	"Error_Put"	BOOL	false	
11	MW 12	"Status_Get"	HEX	W#16#0000	
12					
13	//Data				
14	DB3.DBW 0	"Data".Hodnota1	DEC	1	
15	DB3.DBW 2	"Data".Hodnota2	DEC	5	
16	DB3.DBW 4	"Data".Hodnota3	DEC	6	
17	DB3.DBW 6	"Data".Hodnota4	DEC	-4	
18	DB3.DBW 8	"Data".Hodnota5	DEC	5	
19					
20	DB3.DBW 10	"Data".Hodnota6	DEC	55	
21	DB3.DBW 12	"Data".Hodnota7	DEC	10	
22	DB3.DBW 14	"Data".Hodnota8	DEC	65	
23	DB3.DBW 16	"Data".Hodnota9	DEC	45	
24	DB3.DBW 18	"Data".Hodnota10	DEC	550	
25					

cv10_1\C7 CPU 635 TB\...\S7 Program(2) RUN Abs < 5.2

VAT tabulky obou PLC:

VAT_1 -- @cv10_1\C7 CPU 635 TB\C7 CPU 635 TB\S7 Program(2) ONLINE

	Address	Symbol	Display format	Status value	Modify value
1	//S7 Get				
2	M 10.0	"Req_Get"	BOOL	false	
3	M 10.1	"StatusParam_Get"	BOOL	false	
4	M 10.2	"Error_Get"	BOOL	false	
5	MW 12	"Status_Get"	DEC	0	
6					
7	//S7 Put				
8	M 20.0	"Req_Put"	BOOL	false	
9	M 20.1	"DoneParam_Put"	BOOL	false	
10	M 20.2	"Error_Put"	BOOL	false	
11	MW 12	"Status_Get"	HEX	W#16#0000	
12					
13	//Data				
14	DB3.DBW 0	"Data".Hodnota1	DEC	82	
15	DB3.DBW 2	"Data".Hodnota2	DEC	5	
16	DB3.DBW 4	"Data".Hodnota3	DEC	87	
17	DB3.DBW 6	"Data".Hodnota4	DEC	77	
18	DB3.DBW 8	"Data".Hodnota5	DEC	410	
19					
20	DB3.DBW 10	"Data".Hodnota6	DEC	77	
21	DB3.DBW 12	"Data".Hodnota7	DEC	10	
22	DB3.DBW 14	"Data".Hodnota8	DEC	87	
23	DB3.DBW 16	"Data".Hodnota9	DEC	67	
24	DB3.DBW 18	"Data".Hodnota10	DEC	770	
25					
26					

VAT_1 -- @cv10_1\CPU 315-2 DP\CPU 315-2 DP\S7 Progra...

	Address	Symbol	Display format	Status value	Modify value
1	//Data				
2	DB1.DBW 0	"Data".Hodnota1	DEC	87	
3	DB1.DBW 2	"Data".Hodnota2	DEC	5	
4	DB1.DBW 4	"Data".Hodnota3	DEC	92	
5	DB1.DBW 6	"Data".Hodnota4	DEC	82	
6	DB1.DBW 8	"Data".Hodnota5	DEC	435	
7	DB1.DBW 10	"Data".Hodnota6	DEC	78	
8	DB1.DBW 12	"Data".Hodnota7	DEC	10	
9	DB1.DBW 14	"Data".Hodnota8	DEC	88	
10	DB1.DBW 16	"Data".Hodnota9	DEC	68	
11	DB1.DBW 18	"Data".Hodnota10	DEC	780	
12					
13					

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI10\

DVD-ROM

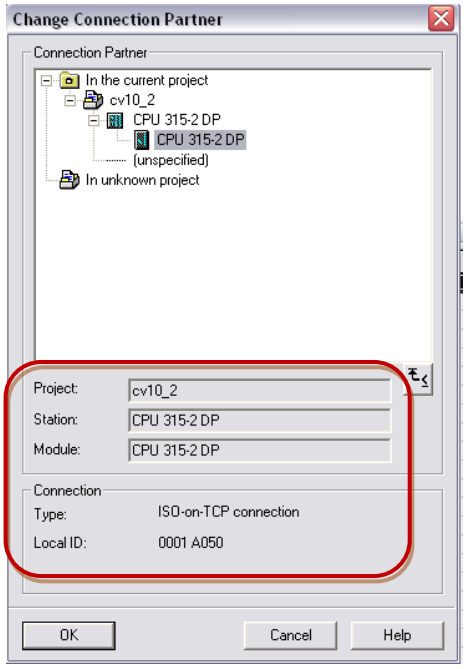
K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI10\

Řešená úloha 10.2

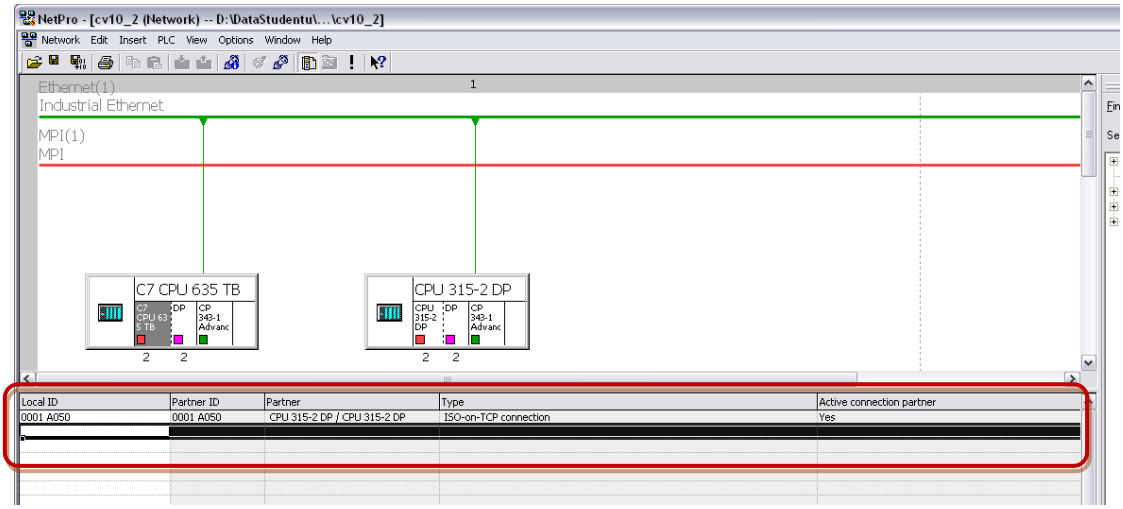
Zadání: Nastavte komunikaci mezi dvěma PLC (CPU 315-2DP a CPU C7 635 TB) po ethernetu (ISO-on-TCP connection). Pro komunikaci použijte funkce AG_SEND a AG_RECEIVE. Vytvořte tři sinusové signály s různými amplitudami (5, 10, 15) a periodami (18s, 36s, 72s). Parametry signálů posílejte z PLC CPU C7 635 TB do CPU 315-2DP.
Vytvořte UDT se čtyřmi hodnotami typu REAL: amplituda, úhel, přepočet a sinus. Pomocí tohoto UDT vytvořte v datovém bloku tři struktury.
Z PLC CPU C7 635 TB posílejte data z vytvořeného datového bloku do PLC CPU 315-2DP. Amplitudu inicializujte v OB100. Hodnota „přepočet“ udává velikost úhlu v radiánech přičítávanou každou periodu vzorkování OB35.

Data posílejte a čtěte kontinuálně.

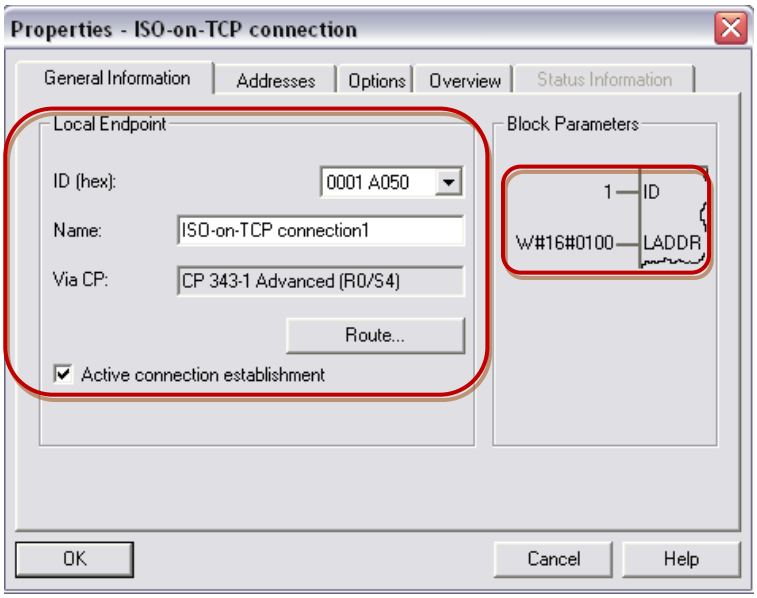
Základním krokem řešení úlohy je hardwarová konfigurace dvou PLC a nastavení komunikace mezi PLC. Konfigurace komunikace probíhá v nástroji NetPro, které se spouští z hlavního okna Simatic Manageru. Klinutím na CPU se dole v okně zobrazí tabulka komunikačních připojení. Pomocí pravého tlačítka vložte nové připojení (Insert New Connection). Definujte, se kterým CPU bude komunikace probíhat a nastavte typ komunikačního spojení (ISO-on-TCP connection). Nastavení potvrďte stiskem tlačítka OK. Objeví se okno Properties, kde nastavte parametry komunikace: ID komunikace, jméno komunikace a zda bude zařízení aktivní (bude navazovat komunikaci) nebo pasivní. Parametry v ostatních záložkách nechte defaultní. Parametr ID se následně bude používat v programu jako vstupní parametr funkcích bloků AG_SEND a AG_RECEIVE. Nastavení v NetPro uložte a zkompilujte.



Obr. 10.14 Nastavení komunikace ISO on TCP.



Obr. 10.15 Nastavení komunikace ISO on TCP.

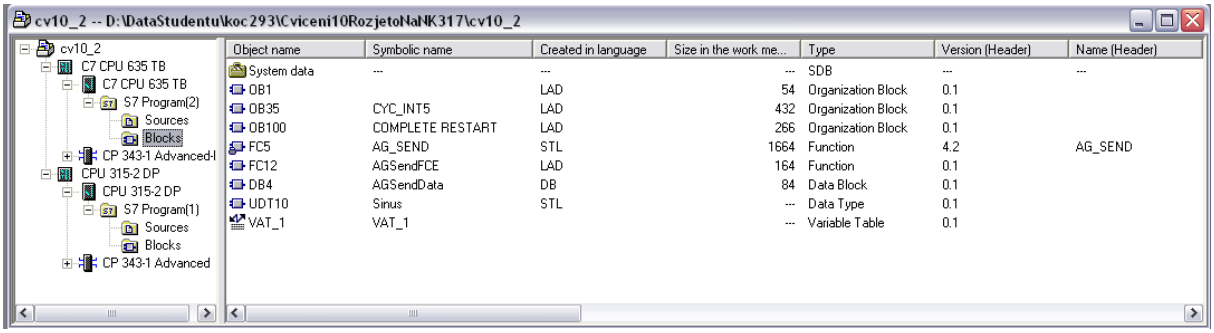


Obr. 10.16 Nastavení komunikace ISO on TCP.

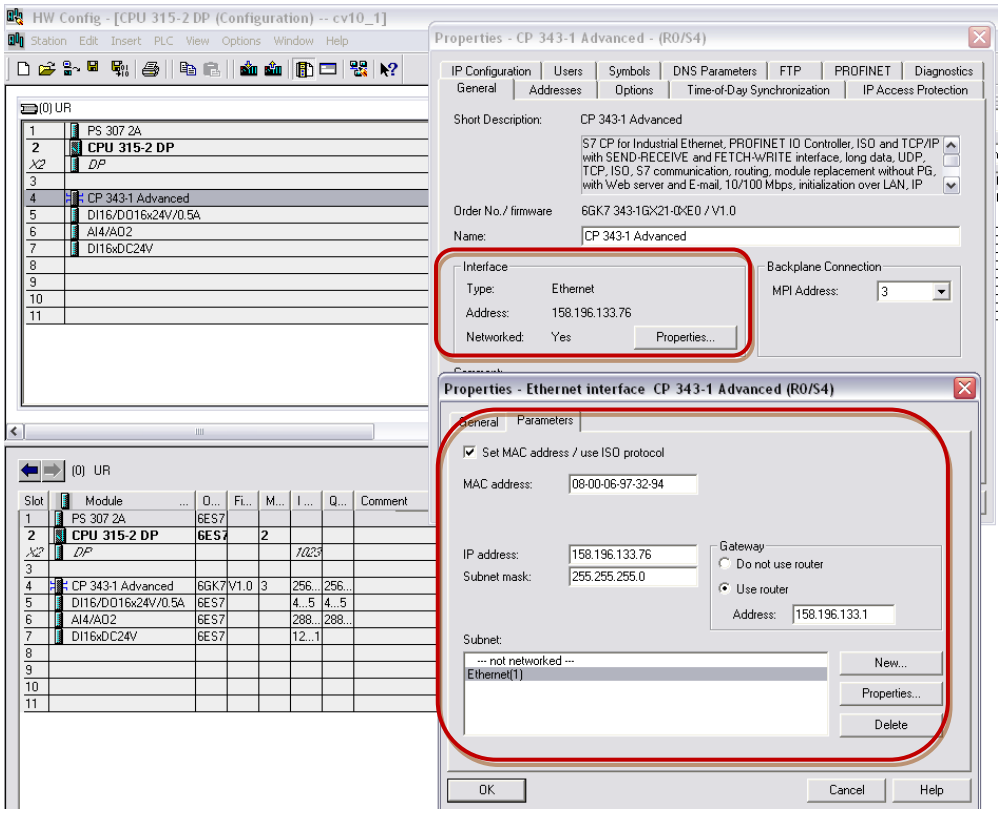
Pomocí funkce FC5„AG_SEND“ a FC6 „AG_RECEIVE“ lze přenášet data mezi programovatelnými automaty. Komunikaci zahajuje aktivní zařízení.

Komunikace začíná požadavkem funkcí FC5 pomocí vstupu ACT = 1. ID udává číslo spojení nakonfigurovaný v nástroji NetPro. LADDR je adresa ethernetového modulu. SEND definuje oblast s daty, která budou vysílána. LEN je pak délka posílané datové oblasti. DONE indikuje, zda byla data odeslána. Pokud má parametr ERROR hodnotu 1, pak při vysílání došlo k chybě. STATUS upřesňuje stav funkce. Popis statusu funkce je možné najít v nápovědě.

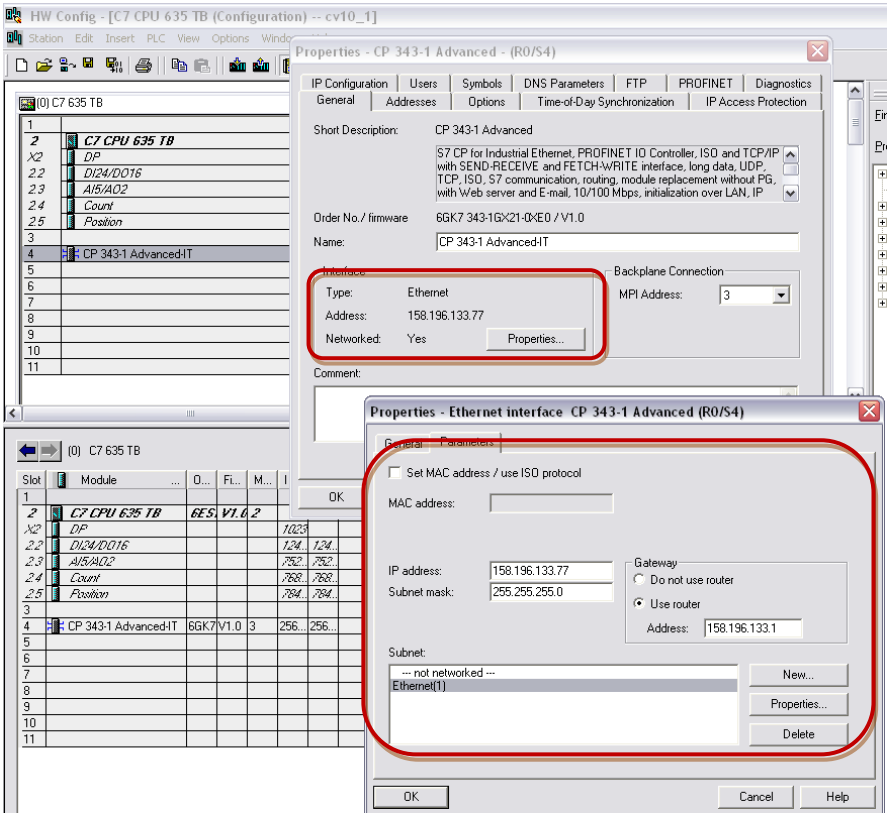
Podobné parametry má i funkce FC6. Parametr ID musí být u obou funkcí stejný.



Obr. 10.17 Nastavení komunikace ISO on TCP.



Obr. 10.18 Nastavení komunikace ISO on TCP.



Obr. 10.19 Nastavení komunikace ISO on TCP.

Program v LAD

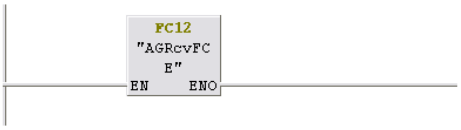
PLC1: S7315-2DP:

S7 Program(1) (Symbols) -- cv10_2\CPU 315-2 DP\CPU 315-2 DP

	Status	Symbol	Addres	Data type	Comment
1		AGRecvData	DB 4	DB 4	
2		AG_RECV	FC 6	FC 6	AG RECEIVE
3		AGRcvFCE	FC 12	FC 12	
4		NDR_AGRcv	M 30.0	BOOL	
5		Error_AGRcv	M 30.1	BOOL	
6		Status_AGRcv	MW 32	WORD	
7		LEN_AGRcv	MW 34	INT	
8		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
9		VAT_2	VAT 2		
10					

OB1:

```
OB1 :  "Main Program Sweep (Cycle)"
Comment:
Network 1: Title:
Comment:
```



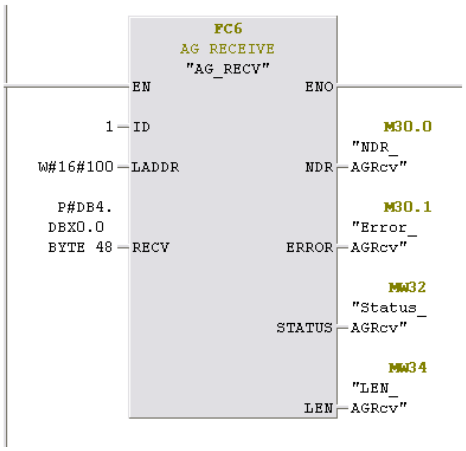
FC12:

FC12 : Title:

Comment:

Network 1: Title:

```
ID: Connection ID acc. to configuration.
LADDR: W#16#0100 (256 dec. in HW Config).
RECV:=P#M 0.0 BYTE 100 (Buffer for received data).
NDR: Receive code.
ERROR: Error code.
STATUS: Status code.
LEN: Received data length.
```



DB4:

DB4 -- "AGRecvData" -- cv10_2\CPU 315-2 DP\CPU 315-2 DP\...\DB4

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	RecvAmplituda1	REAL	0.000000e+000	
+4.0	RecvUhel1	REAL	0.000000e+000	
+8.0	RecvPrepocet1	REAL	0.000000e+000	
+12.0	RecvHodnotaSinus1	REAL	0.000000e+000	
+16.0	RecvAmplituda2	REAL	0.000000e+000	
+20.0	RecvUhel2	REAL	0.000000e+000	
+24.0	RecvPrepocet2	REAL	0.000000e+000	
+28.0	RecvHodnotaSinus2	REAL	0.000000e+000	
+32.0	RecvAmplituda3	REAL	0.000000e+000	
+36.0	RecvUhel3	REAL	0.000000e+000	
+40.0	RecvPrepocet3	REAL	0.000000e+000	
+44.0	RecvHodnotaSinus3	REAL	0.000000e+000	
=48.0		END_STRUCT		

VAT tabulka:

VAT_2 -- @cv10_2\CPU 315-2 DP\CPU 315-2 DP\S7 Program(1) ONLINE

	Address	Symbol	Display format	Status value	Modify value
1	//S7 Receive				
2	M 30.0	"NDR_AGRcv"	BOOL	false	
3	M 30.1	"Error_AGRcv"	BOOL	false	
4	MW 32	"Status_AGRcv"	HEX	W#16#8180	
5	MW 34	"LEN_AGRcv"	DEC	0	
6					
7	//S7 Receive Data				
8	DB4.DBD 0	"AGRecvData".RecvAmplituda1	FLOATING_POINT	5.0	
9	DB4.DBD 4	"AGRecvData".RecvUhel1	FLOATING_POINT	3.717543	
10	DB4.DBD 8	"AGRecvData".RecvPrepocet1	FLOATING_POINT	0.01745329	
11	DB4.DBD 12	"AGRecvData".RecvHodnotaSinus1	FLOATING_POINT	-2.72316	
12	DB4.DBD 16	"AGRecvData".RecvAmplituda2	FLOATING_POINT	10.0	
13	DB4.DBD 20	"AGRecvData".RecvUhel2	FLOATING_POINT	3.717543	
14	DB4.DBD 24	"AGRecvData".RecvPrepocet2	FLOATING_POINT	0.01745329	
15	DB4.DBD 28	"AGRecvData".RecvHodnotaSinus2	FLOATING_POINT	-2.024693	
16	DB4.DBD 32	"AGRecvData".RecvAmplituda3	FLOATING_POINT	15.0	
17	DB4.DBD 36	"AGRecvData".RecvUhel3	FLOATING_POINT	3.717543	
18	DB4.DBD 40	"AGRecvData".RecvPrepocet3	FLOATING_POINT	0.01745329	
19	DB4.DBD 44	"AGRecvData".RecvHodnotaSinus3	FLOATING_POINT	-2.024693	
20					

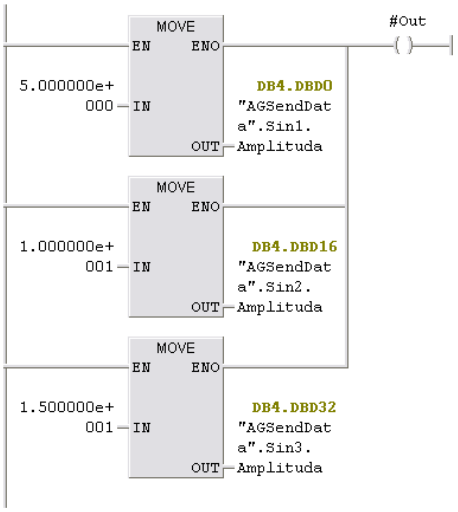
PLC2: C7 CPU 635 TB:

S7 Program(2) (Symbols) -- cv10_2\C7 CPU 635 TB\C7 CPU 635 TB

	Status	Symbol	Addres	Data type	Comment
1		AGSendData	DB 4	DB 4	
2		AG_SEND	FC 5	FC 5	AG SEND
3		AGSendFCE	FC 12	FC 12	
4		Act_AGSend	M 30.0	BOOL	
5		Done_AGSend	M 30.1	BOOL	
6		Error_AGSend	M 30.2	BOOL	
7		1Hz	M 100.5	BOOL	
8		Status_AGSend	MW 32	WORD	
9		CYC_INT5	OB 35	OB 35	Cyclic Interrupt 5
10		COMPLETE REST...	OB 100	OB 100	Complete Restart
11		AGSend_Timer	T 3	TIMER	
12		Sinus	UDT 10	UDT 10	
13		VAT_1	VAT 1		
14					

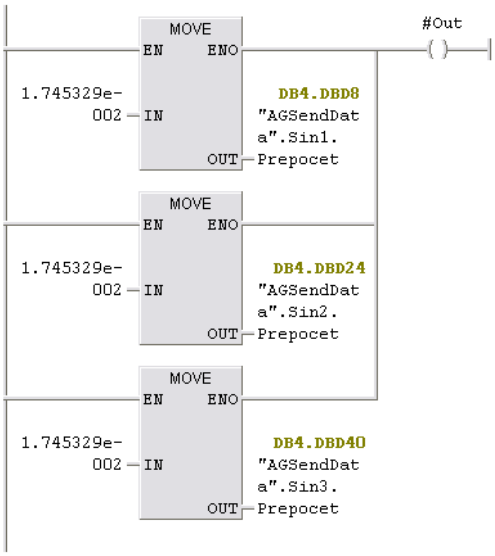
OB100:

```
OB100 :  "Complete Restart"
Comment:

Network 1: Title:
Comment:
```



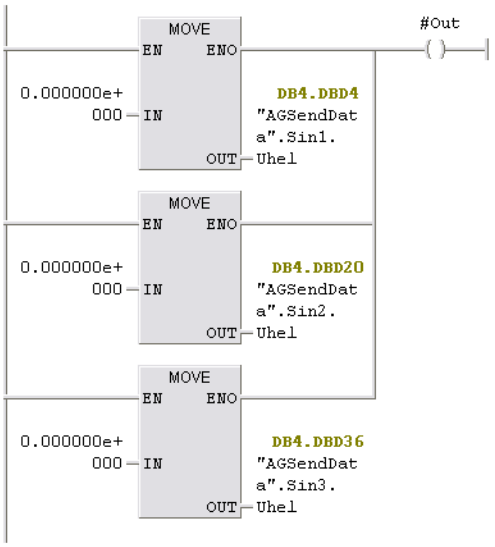
Network 2 : Title:

Comment:



Network 3 : Title:

Comment:



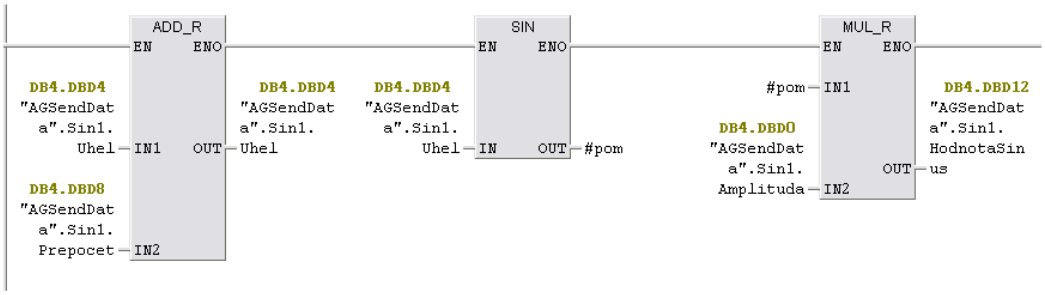
OB35:

```
OB35 :  "Cyclic Interrupt"
```

Comment:

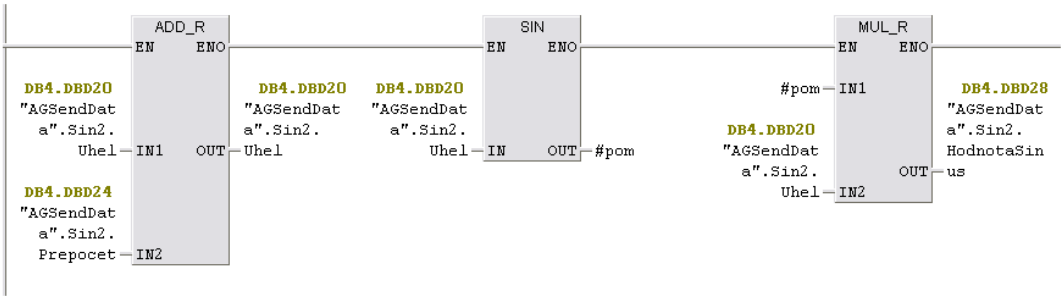
Network 1: Title:

```
Amplituda je: A1 = 5, A2 = 10, A3 = 15.
Perioda je: T1 = 18s, T2 = 36s, T3 = 72s.
Perioda vzorkovani OB35 je 100ms.
Hodnoty prepoctu: P1 = 0.03490658, P2 = 0.01745329, P3 = 0.008726645.

Pr. vypoctu pro periodu 36s:
Prevod stupnu na radiany - uhel ve stupnich se vynasobi hodnotou 0.01745329.
Protoze je perioda vzorkovani 100 ms, perioda je 36 sekund, pak z toho vychazi,
ze v jedne periode se bude vzorkovat 360 krat. Z toho vyplyva, ze kazdou
periodu vzorkovani se bude pricitat 1 stupen uhlu, to znamena ta hodnota
prepoctu: 0.01745329.
```



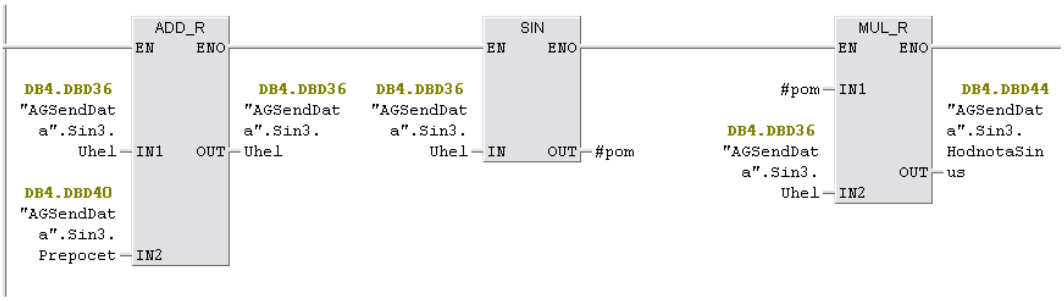
Network 2: Title:

Comment:



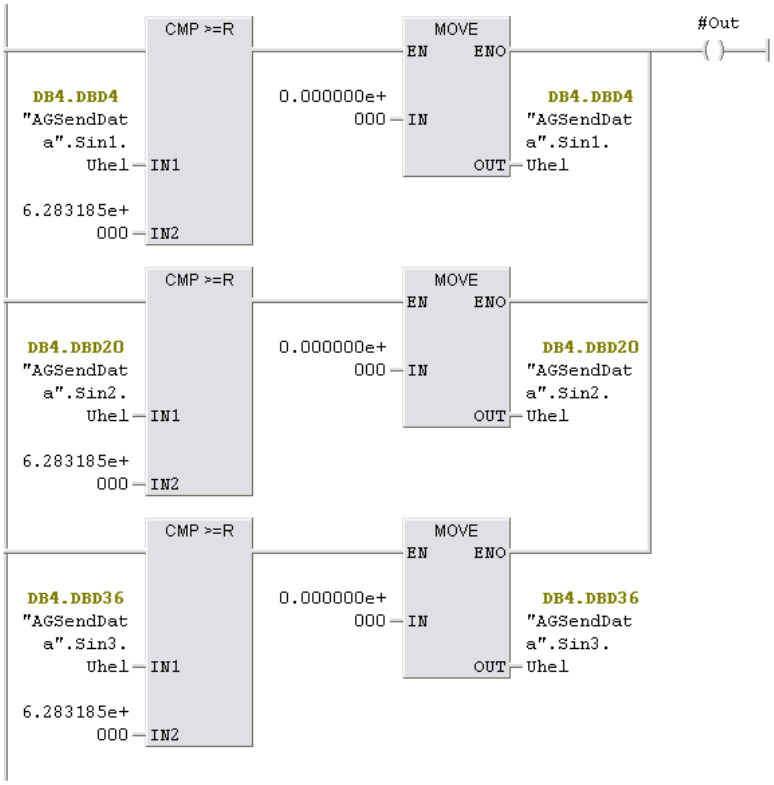
Network 3: Title:

Comment:



Network 4 : Title:

360 krat 0.01745329 = 6.2831844. Vynuluje uhel, pokud je prekroceno 360 stupnu.



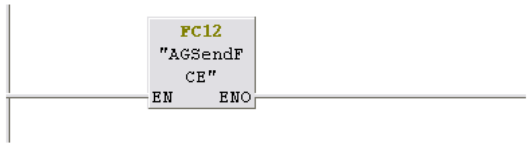
OB1:

OB1 : "Main Program Sweep (Cycle)"

Comment:

Network 1: Title:

FC12



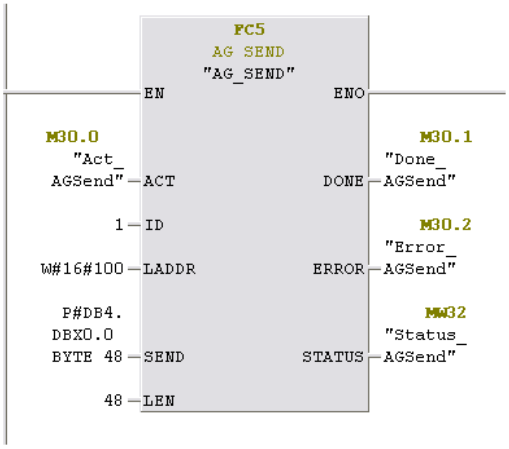
FC12:

FC12 : Title:

Comment:

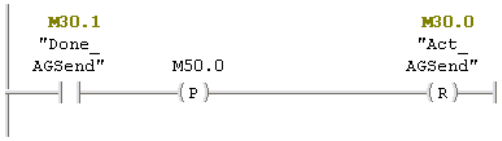
Network 1: Title:

```
Call FC5.
ACT: Job triggered by memory bit.
ID: Connection ID acc. to configuration.
LADDR: W#16#0100 (256 dec. in HW Config).
SEND: Buffer with send data.
LEN: Length for send data.
DONE: Execution.
ERROR: Error code.
STATUS: Status code.
```



Network 2 : Title:

Comment:



Network 3 : Title:

Comment:

DB3:

DB4 -- "AGSendData" -- cv10_2\C7 CPU 635 TB\C7 CPU 635 TB\...\DB4

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	Sin1	"Sinus"		
+16.0	Sin2	"Sinus"		
+32.0	Sin3	"Sinus"		
=48.0		END_STRUCT		

UDT10:

UDT10 -- "Sinus" -- cv10_2\C7 CPU 635 TB\C7 CPU 635 TB\...\UDT10

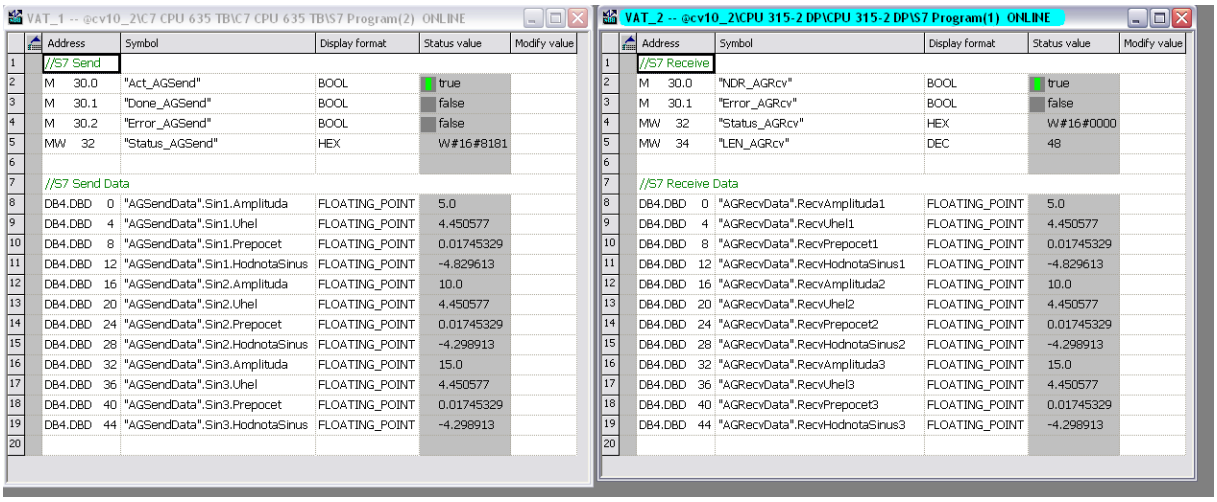
Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	Amplituda	REAL	0.000000e+000	
+4.0	Uhel	REAL	0.000000e+000	
+8.0	Prepocet	REAL	0.000000e+000	
+12.0	HodnotaSinus	REAL	0.000000e+000	
=16.0		END_STRUCT		

VAT tabulka:

VAT_1 -- @cv10_2\C7 CPU 635 TB\C7 CPU 635 TB\S7 Program(2) ONLINE

	Address	Symbol	Display format	Status value	Modify value
1	//S7 Send				
2	M 30.0	"Act_AGSend"	BOOL	true	
3	M 30.1	"Done_AGSend"	BOOL	false	
4	M 30.2	"Error_AGSend"	BOOL	false	
5	MW 32	"Status_AGSend"	HEX	W#16#8181	
6					
7	//S7 Send Data				
8	DB4.DBD 0	"AGSendData".Sin1.Amplituda	FLOATING_POINT	5.0	
9	DB4.DBD 4	"AGSendData".Sin1.Uhel	FLOATING_POINT	4.90436	
10	DB4.DBD 8	"AGSendData".Sin1.Prepocet	FLOATING_POINT	0.01745329	
11	DB4.DBD 12	"AGSendData".Sin1.HodnotaSinus	FLOATING_POINT	-4.90815	
12	DB4.DBD 16	"AGSendData".Sin2.Amplituda	FLOATING_POINT	10.0	
13	DB4.DBD 20	"AGSendData".Sin2.Uhel	FLOATING_POINT	4.90436	
14	DB4.DBD 24	"AGSendData".Sin2.Prepocet	FLOATING_POINT	0.01745329	
15	DB4.DBD 28	"AGSendData".Sin2.HodnotaSinus	FLOATING_POINT	-4.814267	
16	DB4.DBD 32	"AGSendData".Sin3.Amplituda	FLOATING_POINT	15.0	
17	DB4.DBD 36	"AGSendData".Sin3.Uhel	FLOATING_POINT	4.90436	
18	DB4.DBD 40	"AGSendData".Sin3.Prepocet	FLOATING_POINT	0.01745329	
19	DB4.DBD 44	"AGSendData".Sin3.HodnotaSinus	FLOATING_POINT	-4.814267	
20					

VAT tabulky obou PLC:



VAT_1 -- @cv10_2\C7 CPU 635 TB\C7 CPU 635 TB\S7 Program(2) ONLINE

	Address	Symbol	Display format	Status value	Modify value
1	//S7 Send				
2	M 30.0	"Act_AGSend"	BOOL	true	
3	M 30.1	"Done_AGSend"	BOOL	false	
4	M 30.2	"Error_AGSend"	BOOL	false	
5	MW 32	"Status_AGSend"	HEX	W#16#8181	
6					
7	//S7 Send Data				
8	DB4.DBD 0	"AGSendData".Sin1.Amplituda	FLOATING_POINT	5.0	
9	DB4.DBD 4	"AGSendData".Sin1.Uhel	FLOATING_POINT	4.450577	
10	DB4.DBD 8	"AGSendData".Sin1.Prepocet	FLOATING_POINT	0.01745329	
11	DB4.DBD 12	"AGSendData".Sin1.HodnotaSinus	FLOATING_POINT	-4.829613	
12	DB4.DBD 16	"AGSendData".Sin2.Amplituda	FLOATING_POINT	10.0	
13	DB4.DBD 20	"AGSendData".Sin2.Uhel	FLOATING_POINT	4.450577	
14	DB4.DBD 24	"AGSendData".Sin2.Prepocet	FLOATING_POINT	0.01745329	
15	DB4.DBD 28	"AGSendData".Sin2.HodnotaSinus	FLOATING_POINT	-4.298913	
16	DB4.DBD 32	"AGSendData".Sin3.Amplituda	FLOATING_POINT	15.0	
17	DB4.DBD 36	"AGSendData".Sin3.Uhel	FLOATING_POINT	4.450577	
18	DB4.DBD 40	"AGSendData".Sin3.Prepocet	FLOATING_POINT	0.01745329	
19	DB4.DBD 44	"AGSendData".Sin3.HodnotaSinus	FLOATING_POINT	-4.298913	
20					

VAT_2 -- @cv10_2\CPU 315-2 DP\CPU 315-2 DP\S7 Program(1) ONLINE

	Address	Symbol	Display format	Status value	Modify value
1	//S7 Receive				
2	M 30.0	"NDR_AGRcv"	BOOL	true	
3	M 30.1	"Error_AGRcv"	BOOL	false	
4	MW 32	"Status_AGRcv"	HEX	W#16#0000	
5	MW 34	"LEN_AGRcv"	DEC	48	
6					
7	//S7 Receive Data				
8	DB4.DBD 0	"AGRecvData".RecvAmplituda1	FLOATING_POINT	5.0	
9	DB4.DBD 4	"AGRecvData".RecvUhel1	FLOATING_POINT	4.450577	
10	DB4.DBD 8	"AGRecvData".RecvPrepocet1	FLOATING_POINT	0.01745329	
11	DB4.DBD 12	"AGRecvData".RecvHodnotaSinus1	FLOATING_POINT	-4.829613	
12	DB4.DBD 16	"AGRecvData".RecvAmplituda2	FLOATING_POINT	10.0	
13	DB4.DBD 20	"AGRecvData".RecvUhel2	FLOATING_POINT	4.450577	
14	DB4.DBD 24	"AGRecvData".RecvPrepocet2	FLOATING_POINT	0.01745329	
15	DB4.DBD 28	"AGRecvData".RecvHodnotaSinus2	FLOATING_POINT	-4.298913	
16	DB4.DBD 32	"AGRecvData".RecvAmplituda3	FLOATING_POINT	15.0	
17	DB4.DBD 36	"AGRecvData".RecvUhel3	FLOATING_POINT	4.450577	
18	DB4.DBD 40	"AGRecvData".RecvPrepocet3	FLOATING_POINT	0.01745329	
19	DB4.DBD 44	"AGRecvData".RecvHodnotaSinus3	FLOATING_POINT	-4.298913	
20					

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI10\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI10\

11. FUNKČNÍ BEZPEČNOST V KOMUNIKACI

Čas ke studiu: 3 hodiny

Cíl

Po prostudování této kapitoly budete umět znát základní pojmy z funkční bezpečnosti a budete schopni popsat základní principy bezpečnostních komunikačních sběrnic.

Výklad

11.1. Funkční bezpečnost v komunikaci

V současné době se v odborné veřejnosti, zabývající se nejen průmyslovou automatizací, diskutují nejčastěji dvě odborná témata. A to průmyslové řídicí systémy a komunikační sběrnice a jejich bezpečnostní funkce a vlastnosti. To vše v souvislosti s rozšířením všeobecných požadavků na bezpečnost průmyslových technologických systémů. Tato témata jsou nejčastěji řešenou problematikou současného vývoje automatizace ve vyspělých průmyslových zemích. Průmyslové řídicí systémy a jejich komunikační sběrnice, založené na elektrických a elektronických součástech, se již řadu let využívají ve většině aplikačních oblastech pro zajištění bezpečnostních funkcí. Mají-li být technologie, založené na elektronických a počítačových systémech, efektivně a bezpečně využívány, je nutné, aby splňovaly určité úrovně bezpečnosti. Výpadky a chybné funkce technologických zařízení a strojů mohou vést k rizikům pro osoby, životní prostředí a materiální hodnoty. Důsledky poruch a pravděpodobnosti výskytu určují nutná opatření k omezení rizik zabráněním vzniku poruch, rozpoznáním poruch a zvládnutím poruch.

Obecný pojem *bezpečnost* má ve své podstatě více významů. Systém je bezpečný ve smyslu překladu „safety“ pokud není nebezpečný sám o sobě nebo jeho provoz pro svoje okolí. Ve smyslu „security“ je systém bezpečný především v souvislosti se SW vybavením řídicího systému. A to tehdy, pokud je odolný vůči neoprávněným zásahům nepověřených osob. S předchozími dvěma výrazy bývá často dáván do souvislostí také pojem „reliability“, což znamená provozní spolehlivost. Znamená míru dostupnosti systému, tedy pravděpodobnost, že systém úspěšně provedené úlohy/úkoly dříve než selže. Všechny zde doposud uvedené pojmy v souvislosti s bezpečností souvisí přímo či nepřímo a více či méně s HW i SW vybavením průmyslových systémů jako celku včetně komunikačních sběrnic.

Bezpečnost průmyslových systémů ve smyslu výrazu *„safety“* může znamenat ochranu před:

- *Úrazem elektrickým proudem.*
- *Ohněm a žárem.*
- *Nebezpečným zářením*
- *Ohrožením způsobeným selháním korektní funkce systému*

Poslední bod těchto bezpečnostních hledisek je již konkrétněji definován jako tzv.: *„Funkční bezpečnost“*. Pojem *„Funkční bezpečnost“ (Functional Safety)* znamená korektní chování bezpečnostního řídicího systému a jeho částí. Je to část celkové bezpečnosti týkající se rizika řízeného zařízení (*EUC- Equipment Under Control*) a systému řízení EUC. Tato část je závislá na

správném fungování bezpečnostního řídicího systému, systémů založených na jiných technických principech a vnějších prostředcích pro snížení rizika. Pro takovéto požadované chování je nezbytné dosáhnout určitých minimálních úrovní normalizace a funkčnosti těchto systémů.

V průběhu vývoje průmyslových řídicích systémů a s následným nástupem trendu funkční bezpečnosti si většina zemí, na patřičné technické úrovni, vytvořila normy a legislativní ustanovení, specifikující požadavky, funkce, vlastnosti a průběh návrhů systémů splňujících požadavky funkční bezpečnosti. V průběhu tohoto vývoje si každá země zabývající se touto problematikou vytvořila vlastní pohled a určitou metodiku, jak specifikovat a normovat zavádění těchto technologií, mnohdy bez ohledu na vývoj v okolních zemích. S vývojem mezinárodního obchodu a snahou řady společností expandovat se svými produkty do zahraničí, se začalo diskutovat o sjednocení těchto norem a interních standardů každé země do jednotného mezinárodního standardu.

Za nejdůležitější normativní dokumenty, týkající se vysoce funkčního a vysoce bezpečného řízení lze bezesporu považovat mezinárodní normu: **IEC EN 61508-1..7 -** *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností (E/E/PE),* která definuje čtyři úrovně integrity funkční bezpečnosti **SIL 1 – 4** (*Safety Integrity Level*) Nicméně existují i další normy zabývající se funkční bezpečností jako jsou:

- **ČSN EN ISO 13849-1..2** - *Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů*
- **IEC / ČSN EN 61511-1..3** - *Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů*
- **IEC / ČSN EN 62061** - *Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností*
- **ČSN EN ISO 12100-1..2** - *Bezpečnost strojních zařízení – Základní pojmy, všeobecné zásady pro konstrukci*
- **ČSN EN ISO 14121-1** - *Bezpečnost strojních zařízení- Posouzení rizika - Část1: Zásady*

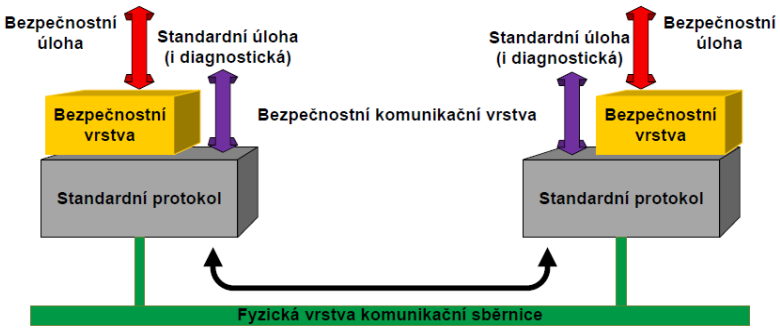
Funkční bezpečnost stále více nabývá na významu především díky mezinárodním standardizačním snahám o minimalizaci rizik souvisejících s provozem průmyslových technologických celků, strojních zařízení apod. Vedle funkční bezpečnosti je nutné brát v úvahu i bezpečnost ve smyslu překladu slova *„security“*. Protože jestliže systémy zajišťující funkční bezpečnost mají minimalizovat rizika spojená s provozem technologických zařízení, pak musí být bezpečná i ve smyslu security pro zabránění neautorizovaného přístupu do sítě, či narušení přenosu dat. Toto ale nemusí platit naopak. V celé řadě průmyslových aplikací jsou provozovány komunikační sběrnice, které jsou sice komunikačně bezpečné (security) – mnohdy bohužel ani to ne – ale není potřeba nebo snaha u nich zajišťovat bezpečnost funkční. [1, 3, 6]

11.2. Princip funkce bezpečnostních komunikačních sběrnic

V oblasti průmyslových komunikací se stala velice oblíbená komunikační technologie tzv. *fieldbus* - jedná se o průmyslové sběrnice primárně určené do oblasti průmyslu a polní instrumentace. Tyto sběrnice jsou definovány normami IEC/ ČSN EN 61158 spolu s IEC/ČSN EN 61784-1 a 61784-2 definující profily komunikačních protokolů pro potřeby distribuovaných systémů řízení spojitých a diskrétních procesů. Nejsou zde zahrnuty všechny běžně používané sběrnice v průmyslu, nicméně je jich většina. Tyto sběrnice se stale častěji začínají také používat v aplikacích s přívlastkem *safety-related*. Musí tedy splňovat požadavky na patřičnou úroveň funkční bezpečnosti. Dříve se pro tyto účely používaly speciální či vyhrazené sběrnice. Dnes se však již vlivem integrace spojily sběrnice pro standardní přenos dat a funkčně bezpečných dat do jedné, rozšířené o bezpečnostní komunikační profil nebo vrstvu. Postupem času vznikla potřeba standardizovat i tyto bezpečnostní

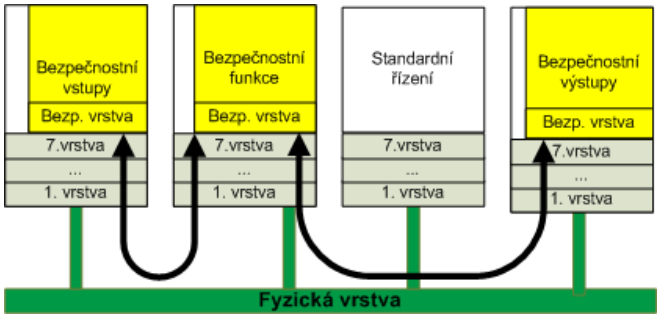
profily. K tomu byla vytvořena norma IEC/ČSN EN 61784-3, která definuje doplňující bezpečnostní komunikační profily pro již definované sběrnice (doposud ne všechny).

Tyto sběrnice fungují na tzv. "*Black Channel*" principu. Jedná se o princip, kdy je funkční bezpečnost vystavěna nad standardním komunikačním kanálem v rámci tzv. SCL (*Safety communication Layer*). Jedná se tedy o vrstvu OSI modelu, která je nadstavbou (profilem) nejvyšší aplikační 7. vrstvy, přičemž může být vestavěna nad nebo do této nejvyšší vrstvy. Přitom není nutné nijak koncepčně zasahovat do existujícího standardu, který nebyl navržen s ohledem na budoucí požadavky funkční bezpečnosti. Potřebné úrovně funkční bezpečnosti, tedy není dosaženo jakoukoli změnou stávající architektury již vyvinuté sběrnice za účelem snížení její poruchovosti, ale jejím rozšířením o další - funkčně bezpečný - komunikační profil. Existují však i sběrnice, jejichž vývoj byl od samotného počátku postaven na zásadách pro zajištění funkční bezpečnosti, a proto jsou s ohledem na tyto požadavky specificky vyvinuty i nižší komunikační vrstvy. Je nezbytné podotknout, že v určitých případech jsou nutná již opatření na úrovni fyzické vrstvy, spočívající např. v redundanci samotného přenosového média komunikační sběrnice či HW komunikačního rozhranní. To ale nesouvisí s bezpečností, ale s pohotovostí (zvýšenou funkčností). Nicméně většina bezpečnostních komunikačních sběrnic byla vyvinuta jako nový profil stávajících sběrnic, a to především pro jejich stávající široké rozšíření a jednodušší vývoj. Nově vyvinutý komunikační profil či sběrnice pro zajištění funkční bezpečnosti by měla eliminovat všechny možné chyby přenosu, které mohou být způsobeny náhodným elektromagnetickým rušením (EMI), které působí na komunikační kanál, poruchami a chybami komunikačního hardware a systematickými chybami některých komponent standardního HW a SW vybavení. Na následujícím obr. 11.1 je zobrazen přístup, jakým je realizována funkčně bezpečná komunikace založená na principu „*Black Chanel*".



Obr. 11.1 Princip „Black Channel" bezpečnostních sběrnic (upraveno ze [7]).

Funkce bezpečné vrstvy (safety layer) spočívá v detekování poruch a provádění opatření pro eliminaci vlivu poruch v komunikačním kanálu v součinnosti s bezpečnostními prvky komunikujících entit (např. zajistit bezpečný stav zařízení). Obrázek dále ukazuje, že standardní komunikace a komunikace související s bezpečností (safety related) běží současně na jednom komunikačním kanálu, přičemž data související s bezpečností jsou použita pro bezpečnostní aplikace a data nesouvisející s bezpečností (standardní data) se používají pro standardní aplikace. Na dalším obr. 11.2 je princip z předchozího obr. 11.1 blíže specifikován pro celý bezpečnostní řetězec. Je z něj patrný i současný provoz standardní a safety komunikace na jednom komunikačním kanálu i to, že safety a non-safety komunikace je navzájem nezávislá. Jednoduchý komunikační kanál by měl být postačující jak pro standardní tak i pro bezpečně orientované aplikace.[2, 4]



Obr. 11.2 Princip současné standardní a bezpečnostní komunikace (upraveno ze [7])

Pokud je v systému, realizovaného s ohledem na funkční bezpečnost, použita pro přenos dat komunikační sběrnice, pak se tato sběrnice stává součástí celého systému. Je třeba zaručit, že i přenos dat mezi jednotlivými účastníky bude funkčně bezpečný stejně jako celý řídicí systém – sběrnice zaručí přenos dat mezi jednotlivými účastníky s garantovanou úrovní integrity bezpečnosti (SIL). SIL je kvantifikovaná faktorem PFH (Probability of Failure per Hour). Ten je dán součtem jednotlivých subčástí celého řídicího systému, včetně komunikační sběrnice.

$$PFH = PFH_{HW} + PFH_{EMI} + PFH_{SW} \tag{12.1}$$

Kde význam dílčích faktorů je následující:

PFH_{HW} - Poruchové stavy v HW přenosového systému. Tato část faktoru PFH je dále složena s následujících subfaktorů:

$$\mathbf{PFH_{HW}} = PFH_{SEN} + PFH_{COM} + PFH_{LOG} + PFH_{COM} + PFH_{ACT} \tag{12.2}$$

Kde: *PFH_{HW} ... PFH celkové hardwarové části řídicího systému včetně sběrnice*
PFH_{SEN} ... PFH použitého senzoru měřící části systémů
PFH_{COM} ... PFH komunikační sběrnice
PFH_{LOG} ... PFH logické části řídicího systému (PLC)
PFH_{ACT} ... PFH akčního členu

Obecně může být zvýšení PFH_{HW} způsobeno např.: zvýšení odporu vodiče (koroze), přerušení vodiče sběrnice, odrazy v důsledku špatně nastavené hodnoty terminátorů, nebo jejich nepřipojení, poruchy v napájecím zdroji a další.

PFH_{EMI} - Poruchové stavy způsobené elektromagnetickým rušením (EMI). Toto rušení může způsobovat poruchové stavy, jako jsou např.: jednoduché (nezávislé) chyby, shluky chyb (závislé), systematické chyby (opakující se vzory chyb), kombinované chyby, chyby způsobené špatnou synchronizací kodéru/dekodéru, maskované chyby způsobené např. špatným výběrem generačního polynomu bezpečnostního kódu (CRC) a další.

PFH_{SW} - Poruchové stavy způsobené špatnou funkcí obslužného SW komunikačního rozhranní komunikujících účastníků, jako jsou např.: chyba v pořadovém čísle přenášených rámců, špatně nastavená hodnotou „timeout“, chyba v adresování účastníků komunikace a další.

Vedle tohoto faktoru rozlišujeme i faktor **PFD** (Probability of Failure on Demand), který označuje střední pravděpodobnost, že zabezpečovací funkce na vyžádání nebude provedena.

Nároky na HW a SW bezpečnostních systémů jsou kladeny tak, aby celkový systém splňoval požadavek na odpovídající úroveň zabezpečení SIL. Z dlouholetých zkušeností z praxe vyplývá, že největší podíl na vzniku poruch a chyb v celém řídicím řetězci mají senzory a akční členy. U snímačů to bývá cca. 35% všech poruch a u akčních členů dokonce až 50%. Jen asi 15% poruch připadá na celý řídicí a komunikační systém. Nicméně i přesto je nutné se touto problematikou zabývat. [5]

11.3. Příčiny a rizika vzniku poruch a chyb průmyslových sběrnic

Poruchy vzniklé při přenosu dat (řídicích i provozních) lze obecně rozdělit do dvou kategorií. A to na poruchy fyzické vrstvy přenosového média sběrnice a na poruchy komunikačního protokolu nebo SW vybavení ŘS a jeho komunikujících komponent. Oba problémy jsou přitom spolu velice úzce spjaty. Porucha fyzické vrstvy, například šum, se může projevovat jako chyba komunikace v podobě ztráty nebo nekonzistence přenášených dat. Chyba samotného komunikačního protokolu se vyskytuje jen zřídka, jelikož ten je během svého vývoje zpravidla řádně odladěn. Chyba však může být v implementaci komunikačního rozhraní mezi ŘS a jednotlivými zařízeními na sítí (data jsou na sběrnici vysílána nebo přijímána ve špatném formátu nebo špatně adresována). To je však problém implementace aplikačního SW. Častěji se však vyskytuje problém bezpečnosti ve smyslu security, kdy jsou přenášená data narušena neautorizovaným zásahem nepověřené osoby – hackerské útoky apod.

Poruchy komponent fyzické vrstvy, jejich detekce a eliminace

Případná porucha některé z komponent fyzické vrstvy sběrnice může vést k přerušení výroby, a tím k poklesu hodnoty jednoho z ostře sledovaných parametrů – koeficientu využití výrobního zařízení. V horším případě pak k materiálním ztrátám, ekologickým haváriím nebo ztrátám na životech. Vyhnout se takové situaci může uživatel pravidelnými kontrolami fyzické vrstvy sběrnice, diagnostickými a predikčními SW algoritmy, nebo už v samém počátku vhodnou volbou typu sběrnice, její fyzické vrstvy nebo topologie. Přestože jsou průmyslové komunikační sběrnice obecně velmi spolehlivé, je seznam možných poruch komponent jejich fyzické vrstvy poměrně obsáhlý:

a) Zkrat stínění – Jedná se o zkrat stínění s kladným nebo záporným vodičem kabelu sběrnice. K nežádoucímu kontaktu může dojít tehdy, jsou-li kabel anebo přístroj špatně nainstalovány, poškozeny, nebo jsou navlhlé. Navenek se může zkrat projevit buď jen zvýšením úrovně šumu ve vedení, nebo až výpadkem segmentu nebo celé sítě. Eliminovat tuto poruchu nebo její vliv je možné už samotnou architekturou fyzické vrstvy sběrnice (galvanické oddělení, vhodné uspořádaní a krytí kabelu).

b) Přerušené vedení - Vodič se může přerušit, popř. se může odpojit od svorky. Porucha tohoto typu vzniká postupně vlivem vibrací, koroze, opotřebení apod. Porušený vodič může po většinu doby vést, občas však může dojít k jeho přerušení a opětnému spojení, a tím i k příležitostné ztrátě zpráv na sběrnici.

c) Šum - Ve sběrnicovém vedení interferuje se signálem přenášeným mezi přístroji. Šum může běžně vzniknout vzájemnou vazbou v případě souběhu sběrnicového kabelu s jinými kabely (i výkonovými), špatným uzemněním stínění kabelu nebo závadou v přístroji připojeném ke sběrnici.

d) Přebytečný, chybějící nebo vadný terminátor - Každý segment sběrnice má být na svém konci opatřen dvěma terminátory (zakončovacími členy). Jestliže je terminátorů víc, je signál utlumený. Chybí-li terminátor, signál na sběrnici je silnější, ale může být v důsledku odrazů deformovaný.

e) Vadný napáječ - Závada na napáječi sběrnice může způsobit výpadek napájení příslušného segmentu sběrnice, nebo celé sítě. Riziko poruchy segmentu sběrnice v důsledku závady na jednom napáječi se snižuje použitím redundantních napáječů.

f) Vniknutí vody - Nekvalitní kabelovou vývodkou nebo při poškození kabelu může do systému vniknout voda. Zpočátku se na sběrnici patrně objeví šum, dále pak může dojít až ke zkratu sběrnice. Je třeba použít komponenty s patřičným krytím (IP). [1]

Poruchy a chyby komunikace, jejich detekce a eliminace

Samotné fyzické médium sice umožňuje přenos dat mezi různými uzly sběrnice, ale nezaručuje doručení dat v přesně stejném tvaru, v jakém byla vyslána. Šum a jiné okolní vlivy působící na sběrnici mohou zasílaná data poškodit. Pro zabezpečení dat proti těmto vlivům se používají dva

přístupy a to detekce (error detection) a korekce chyb (error correction). Algoritmy pro detekci chyb přidávají k původní zprávě určité informace, na základě kterých přijímač zjistí, zda při komunikaci nastaly chyby. Opravy chyb se realizují na principu přidání dostatečného množství dalších dat k zasílané zprávě, tak aby přijímač mohl poškozenou zprávu rekonstruovat (samoopravné kódy). V případě použití komunikačních sběrnic v průmyslu a s potřebou pro zajištění funkční bezpečnosti, již není možné využívat bezpečnostní metody a mechanizmy známé z komerčních sběrnic. Komunikační sběrnice v systémech pro řízení bezpečnostně kritických systémů má svá specifika, na která musí být brán ohled. Mezi rozdíly patří např. časová platnost zpráv, protože jejich pozdní doručení může mít kritický dopad. Proto se zavádí např. mechanismus časové značky (time stamp), ale používají se i jiné jako je identifikace odesilatele a příjemce, potvrzení o doručení a další. Používají se ale i standardní zabezpečovací mechanismy modifikované pro použití v bezpečnostních sběrnicích (32-bitové CRC). Přehled těchto základních mechanismů, definovaných podle normy IEC/ČSN EN 61784-3, je uveden v následující tabulce.

Tab. 111.1 Příčiny chyb komunikačních sběrnic a metody jejich ochrany dle normy IEC 61784-3.

Opatření / Chyba	Sekvenční číslování	Časová známka	Time -out	Auten-tifikace	Potvr-zování	Opatření pro zajištění integrity dat	Redun-dance a crossche cking	Šifrovací techniky
Poškození dat					●	●	●	
Opakování	●	●					●	
Nesprávné pořadí	●	●					●	
Smazání/ ztráta dat	●				●		●	
Zpoždění		●	●					
Vkládání	●			●	●		●	
Maškaráda				●	●			●
Chyba adresování				●				

Význam některých z používaných mechanizmů:

- Identifikace příjemce a odesilatele (Source/Destination Address) - Jednoznačnost identifikátoru, velikost datového pole identifikátorů, kontrola identifikátoru.
- Uplynutí času (Timeout) - Hodnota přijatelného zpoždění, přesnost uplynutého času.
- Sekvenční číslování dat - Délka pořadového čísla, stanovení opatření pro inicializaci pořadového čísla, stanovení opatření pro přerušení sledu zpráv.
- Bezpečnostní kód - Schopnosti detekovat: náhodné chyby, shluky chyb, systematické chyby (opakující se vzory chyb) a kombinované chyby, schopnost detekovat chyby typu: všechny bity mají log. 1, všechny bity mají log. 0 (v případě binárního přenosu), inverzi zprávy, funkční nezávislost použitého kódu s přenosovým kódem, garanci zvýšené chybovosti (pravděpodobnost nedetekované chyby).

Minimálním požadavkem pro bezpečný komunikační protokol je to, aby dokázal eliminovat všechny zmíněné chyby. Protože každá síť má svá specifika a speciální chybové módy, je při tvorbě bezpečného protokolu důležité mít důkladné znalosti o použitém typu a technologii sítě. Podobně jako standardní data jsou doplněna doplňujícími bajty paketu, bezpečná data jsou doplněna bajty použitých bezpečnostních mechanismů z tab. 11.1 a vnořena do datového toku mezi standardní rámce. [1, 4]

Shrnutí pojmů

Základní norma zabývající se problematikou funkční bezpečnosti je **IEC/ČSN EN 61508-1..7**. Tato norma definuje základní úrovně integrity bezpečnosti **SIL 1-4** (Safety Integrity Level). Funkční bezpečnost průmyslových sběrnic je vyvinuta na bázi standardních sběrnic, jež jsou rozšířeny o tzv. **bezpečnostní komunikační profily**. Tyto profily jsou založeny na tzv. „**Black Channel**“ principu, kdy jsou bezpečnostní komunikační mechanizmy vystavěny nad nebo v 7. vrstvě OSI modelu. Není tak nutné nijak zasahovat do stávajících koncepcí již vyvinutých sběrnic. U standardních sběrnic existuje celá řada mechanismů pro zajištění bezpečného přenosu dat. Ty jsou však u bezpečnostních sběrnic ještě rozvinuty, zdokonaleny a doplněny. Jedná se především o techniky jako je **sekvenční číslování dat, potvrzení odesilatele a příjemce, timeout** a speciální bezpečnostní kódy specifického charakteru.

Otázky

1. Co znamená pojem Funkční bezpečnost?
2. Jaký je základní princip bezpečnostních komunikačních sběrnic?
3. Jaké jsou základní příčiny vzniku chyb a poruch komunikačních sítí?
4. Jaké znáte metody pro detekci a eliminaci vzniklých chyb a poruch?

Použitá literatura a další zdroje

1. Láryš, T., Koziorek, J. Význam diagnostiky komunikačních sběrnic v průmyslové automatizaci, *Technická diagnostika z1/2010, ročník XIX*, Ostrava, Asociace technických diagnostiků ČR o.s., 2010, s. 30, ISSN: 1210-311X
2. Láryš, T. Methods and mechanisms for provision safety data transfer at safety fieldbuses, Workshop doktorandů WOEFEX, ročník 2010, Ostrava, VŠB-TU Ostrava - FEI, 2010.
3. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 1998
4. IEC 61784-3 Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial network
5. Franeková, M., Janota A., Rástočný K. Trendy v oblasti komunikačnej bezpečnosti priemyselných sietí. *Advances in Electrical and Electronic Engineering. 2005, vol. 4.* Ostrava 2005. s.253 – 258. ISSN: 1804-3119.
6. Zezulka, F., Úvod do oblasti řídicích počítačů – Část 2, Brno, 2007, VUT Brno – FEEC, [online], [cit. 15-12-2010] http://www.uamt.feec.vutbr.cz/~zezulka/download/LAUP/bezp.pdf
7. Strpf, W., Fieldbus Standard IEC 61158 - Safety Communication Profiles IEC 61784-3, Siemens AG, 2007, Hannover, [online], [cit. 15-12-2010] http://www.dke.de/de/Service/Nachrichten/documents/3stripf.pdf
8. Franeková M., Modelovanie bezpečnostných vlastností priemyselných sietí typu safety fieldbus, Odborný seminář: *„Bezpečnostne relevantné priemyselné a komunikačné systémy*“ sdružení

Profibus.sk, Žilina, 2009, [online], [cit. 15-12-2010]
http://www.profibus.sk/fileadmin/user_upload/prezentacia_modelovanie_Fieldbus_Fra-1.pdf

Řešená úloha 11.1

Zadání: Seznamte se s komunikační sběrnicí Profinet.

Profinet – sběrnice pokrývající požadavky pro komunikaci ve všech vrstvách řídicího systému.

Výhody profinetu:

- Ethernet je výkonná síť.
- Flexibilní topologie sítě, jednoduchá instalace sítě.
- Jednoduché napojení na nadřazený Ethernet, IT služby.
- Lepší diagnostika.
- PROFIsafe–Safety integrated.
- Bezdrátová komunikace.

Nevýhody profinetu:

- Cena.
- Malá znalost Profinetu, užívání zaběhnutých řešení.
- Některá ne-Siemens zařízení nemají Profinet rozhraní.
- Profinet není součástí PCS7.

Diagnostika komunikace:

Základní informace o stavu jednotek je zobrazena pomocí LED diod přímo na zařízení. Pokročilejší diagnostiku nabízí online zobrazení ve Step 7 v hardwarové konfiguraci: on-line pohled s přehledně zobrazenou diagnostikou.

Diagnostiku lze provádět také v uživatelském programu (pomocí error OB). Diagnostické bloky jako rozhraní mezi operačním systémem a uživatelským programem: Čtení pomocí system status lists (SSLs).

Pro diagnostiku lze také použít další nástroje, například Topology editor dostupný přes webové rozhraní.

Řešená úloha 11.2

Zadání: Nastavte komunikaci mezi PLC S7 315PN/DP a modulem ET200S. Programovatelný automat a modul ET200S vzdálených vstupů a výstupů spolu budou komunikovat přes Profinet. Na konektor digitálních vstupů a výstupů připojte přípravek pro simulaci spínání vstupních signálů. Napište program, který přivede logickou hodnotu vstupního signálu na příslušný digitální výstup. Chování programu pozorujte v online režimu a ve VAT tabulce.

Komunikace mezi PLC a modulem ET200S se nastaví v hardwarové konfiguraci. Po vložení lišty RACK, zdroje a CPU 315PN/DP (6ES7 315-2EG10-0AB0) vyskočí dialogové okno, kde se vyplní maska podsítě (255.255.255.0) a IP adresa (158.196.133.88), která je danému programovatelnému automatu přidělena a je rovněž napsána na štítku na zařízení. Dále zaškrtněte použití routeru pomocí

use router. IP adresa routeru v učebně je 158.196.133.1. Kliknutím na tlačítko New se v projektu vytvoří síť Ethernet. Kliknutím na tlačítko „OK“ se dialogové okno nastavení komunikačního procesoru zavře.

Na pozici 4 a 5 na racku jsou moduly vstupů a výstupů SM.

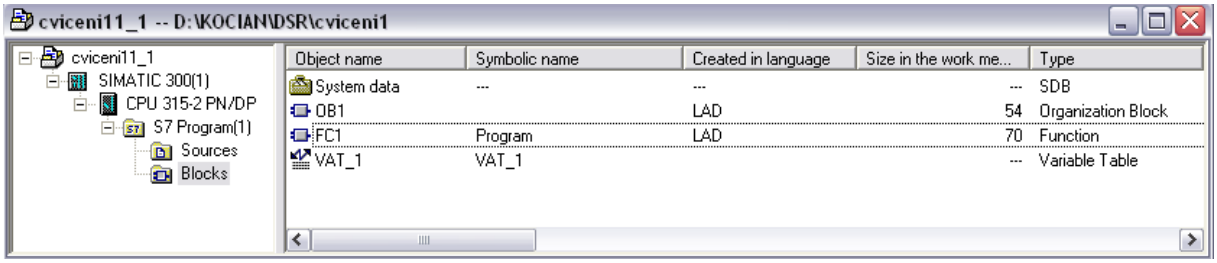
Vložte:

- Pozice 4: SM 323 DI16/DO16x24V/0,5A (6ES7 323-1BL00-0AB0).
- Pozice 5: SM 334 AI4/AO2x8/8Bit (6ES7 334-0CE01-0AB0).

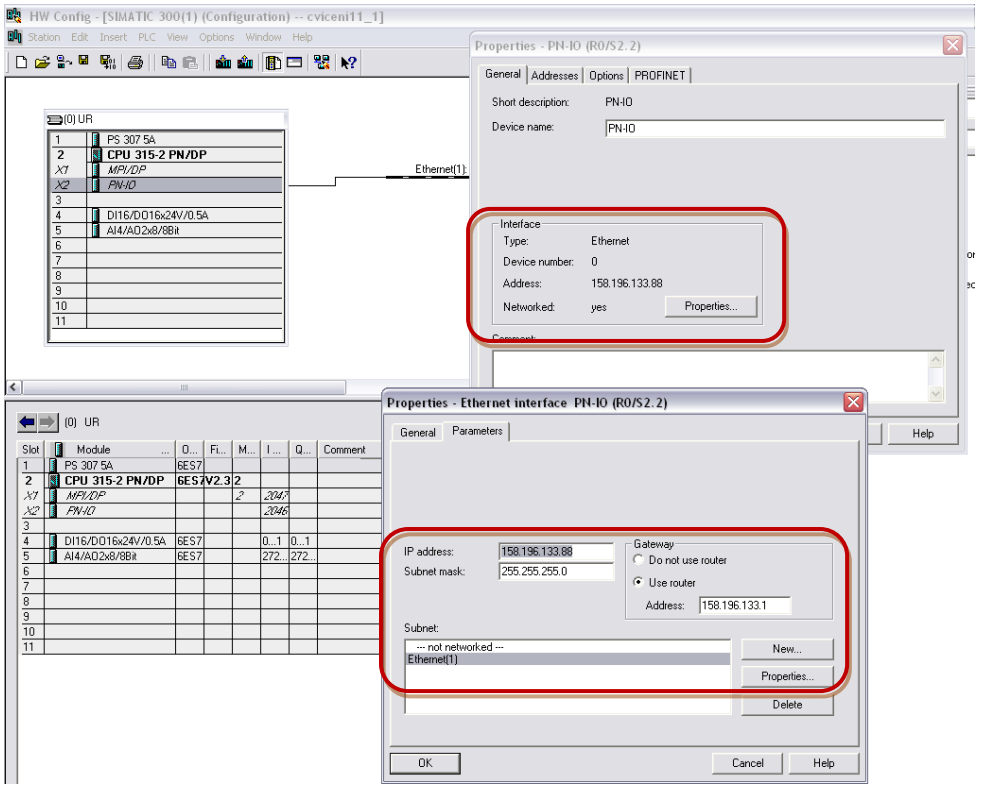
Na vytvořené komunikační ethernetové rozhraní vložte modul vzdálených vstupů a výstupů ET200S (IM 151-3 PN, 6ES7 151-3AA20-0AB0), kterému nastavte IP adresu podobně jako programovatelnému automatu (158.196.133.98). Do slotů modulu vzdálených vstupů a výstupů pak vložte jednotlivé karty digitálních a analogových vstupů a výstupů podle dané konfigurace v učebně.

Vložte:

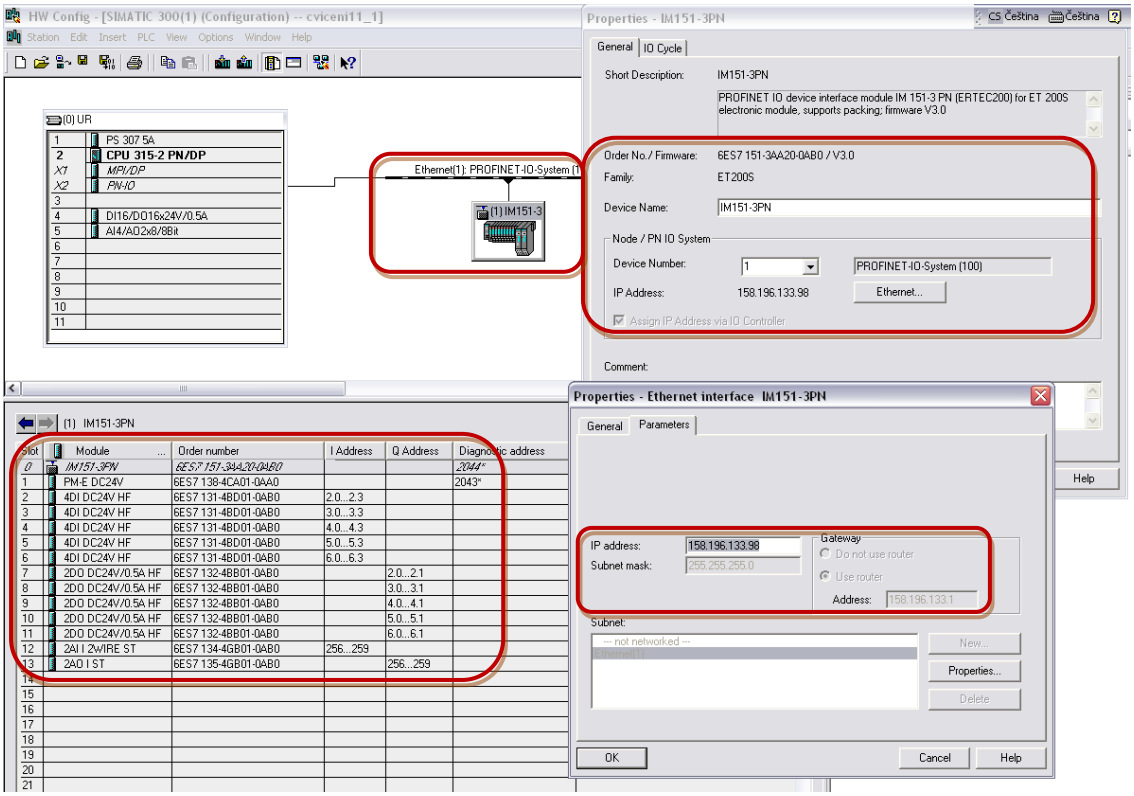
- PM-E DC24V (6ES7 138-4CA01-0AB0).
- 5 x 4DI DC24V HF (6ES7 131-4BD01-0AB0).
- 5 x 2DO DC24V/0,5A HF (6ES7 132-4BB01-0AB0).
- 2AI I 2Wire ST (6ES7 134-4GB01-0AB0).
- 2AO I ST (6ES7 135-4GB01-0AB0).



Obr. 11.3 Nastavení komunikace mezi PLC S7 315PN/DP a modulem ET200S.



Obr. 11.4 Nastavení komunikace mezi PLC S7 315PN/DP a modulem ET200S.



Obr. 11.5 Nastavení komunikace mezi PLC S7 315PN/DP a modulem ET200S.

Program v LAD

Program je napsán ve funkci FC1, která je volána z OB1. Na spínací kontakty jednotlivých vstupů jsou připojeny výstupy.

S7 Program(1) (Symbols) -- cviceni11_1\SIMATIC 300(1)\CPU 315-2 P...

	Status	Symbol	Address	Data type	Comment
1		I1	I 2.0	BOOL	
2		I2	I 2.1	BOOL	
3		I3	I 2.2	BOOL	
4		I4	I 2.3	BOOL	
5		I5	I 3.0	BOOL	
6		I6	I 3.1	BOOL	
7		I7	I 3.2	BOOL	
8		I8	I 3.3	BOOL	
9		Program	FC 1	FC 1	
10		Q1	Q 2.0	BOOL	
11		Q2	Q 2.1	BOOL	
12		Q3	Q 3.0	BOOL	
13		Q4	Q 3.1	BOOL	
14		Q5	Q 4.0	BOOL	
15		Q6	Q 4.1	BOOL	
16		Q7	Q 5.0	BOOL	
17		Q8	Q 5.1	BOOL	
18		VAT_1	VAT 1		
19					

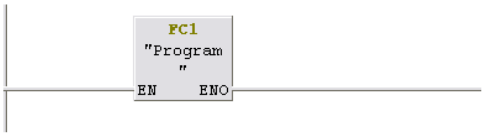
OB1:

OB1 : "Main Program Sweep (Cycle)"

Comment:

Network 1: Title:

Comment:



FC1:

FC1 : Title:

Comment:

Network 1 : Title:

Comment:

Network 2 : Title:

Comment:

Network 3 : Title:

Comment:

Network 4 : Title:

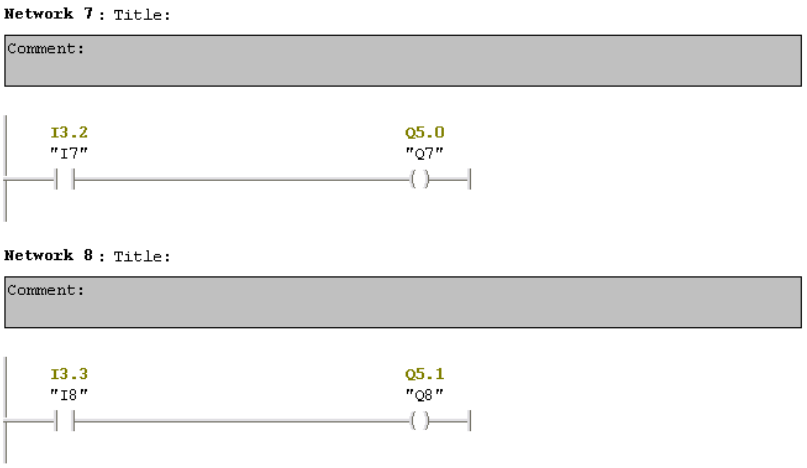
Comment:

Network 5 : Title:

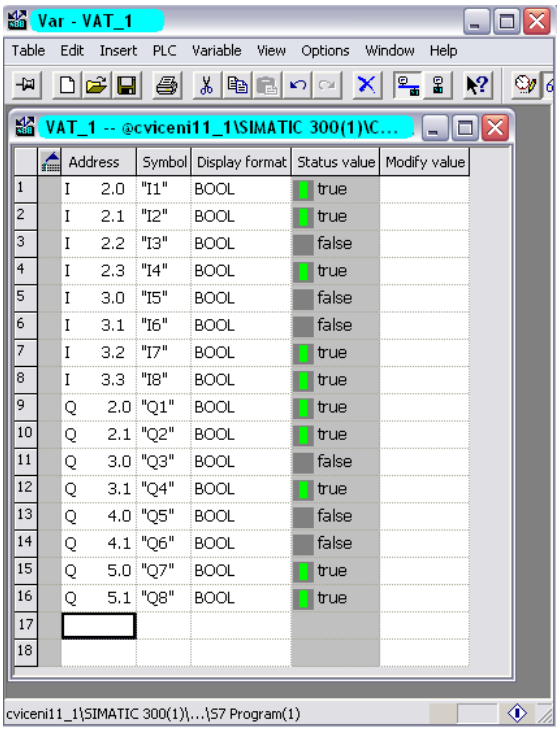
Comment:

Network 6 : Title:

Comment:



VAT tabulka:



	Address	Symbol	Display format	Status value	Modify value
1	I 2.0	"I1"	BOOL	true	
2	I 2.1	"I2"	BOOL	true	
3	I 2.2	"I3"	BOOL	false	
4	I 2.3	"I4"	BOOL	true	
5	I 3.0	"I5"	BOOL	false	
6	I 3.1	"I6"	BOOL	false	
7	I 3.2	"I7"	BOOL	true	
8	I 3.3	"I8"	BOOL	true	
9	Q 2.0	"Q1"	BOOL	true	
10	Q 2.1	"Q2"	BOOL	true	
11	Q 3.0	"Q3"	BOOL	false	
12	Q 3.1	"Q4"	BOOL	true	
13	Q 4.0	"Q5"	BOOL	false	
14	Q 4.1	"Q6"	BOOL	false	
15	Q 5.0	"Q7"	BOOL	true	
16	Q 5.1	"Q8"	BOOL	true	
17					
18					

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI11\

DVD-ROM

K této úloze je vytvořena animace, kterou naleznete na DVD:\CVICENI11\

12. NORMA IEC/ČSN EN 61784-3

Čas ke studiu: 3 hodiny

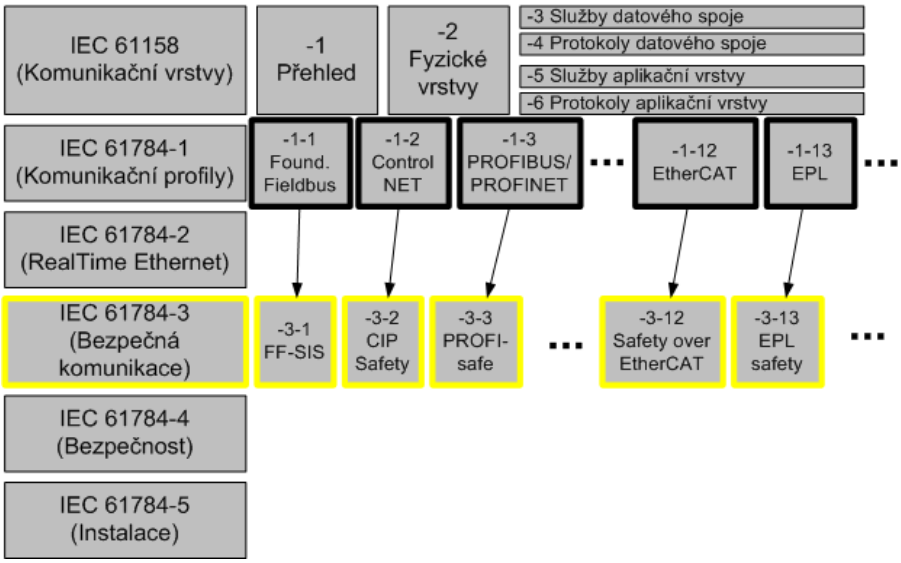
Cíl Po prostudování této kapitoly budete umět

- Popsat normu IEC/ČSN EN 61784.
- Popsat životní cyklus komunikačních sběrnic.
- Popsat možnosti modelování bezpečnostní komunikační sběrnice.

Výklad

12.1. Bezpečnost komunikačních sběrnic podle normy IEC/ČSN EN 61784-3

Jak bylo uvedeno výše, pro sjednocení a standardizaci bezpečnostních sběrnic a jejich profilů byla vytvořena norma **IEC/ČSN EN 61784-3** - *Funkční bezpečnost sběrnic pole*. Jedná se o třetí část normy **IEC/ČSN EN 61784** - *Průmyslové komunikační sítě - Profily*, která vychází z a zásadním způsobem doplňuje výše uvedenou normu **IEC/ČSN EN 61158**. Tato norma definuje základní komunikační sběrnice používané v průmyslu, především jejich fyzické vrstvy, datové spoje, služby a protokoly aplikační vrstvy ISO/OSI modelu. Norma IEC/ČSN EN 61784 se však zaměřuje především na komunikační profily sběrnic. Pro tento text je pak nejvíce podstatná část IEC/ČSN EN 61784-3. Vzájemný vtah obou norem je možné vyčíst z následujícího obrázku.



Obr. 12.1 Znázornění vztahu mezi normou IEC 61158 a IEC 61784 (upraveno z [7]).

Struktura normy IEC/ČSN EN 61784

- IEC/ČSN EN 61784-1: Průmyslové komunikační sítě – Profily – část 1: profily sběrnice pole.
- IEC/ČSN EN 61784-2: Průmyslové komunikační sítě – Profily – část 2: dodatečné profily sběrnic pole pro komunikační sítě v aplikacích reálného času založené na ISO/IEC 8802-3
- IEC/ČSN EN 61784-3: Průmyslové komunikační sítě - Profily - Část 3: Funkční bezpečnost sběrnic pole.
- IEC/ČSN EN 61784-4 : Průmyslové komunikační sítě - Profily - Část 4: Profily pro bezpečnou komunikaci v průmyslových sítích (ve smyslu informativní bezpečnosti).
- IEC/ČSN EN 61784-5: Průmyslové komunikační sítě - Profily - Část 5: instalace sběrnic pole.

Bližší popis obsahu části normy IEC/ČSN EN 61784-3

IEC/ČSN EN 61784-3: obsahuje základní předpisy a definice profilů:

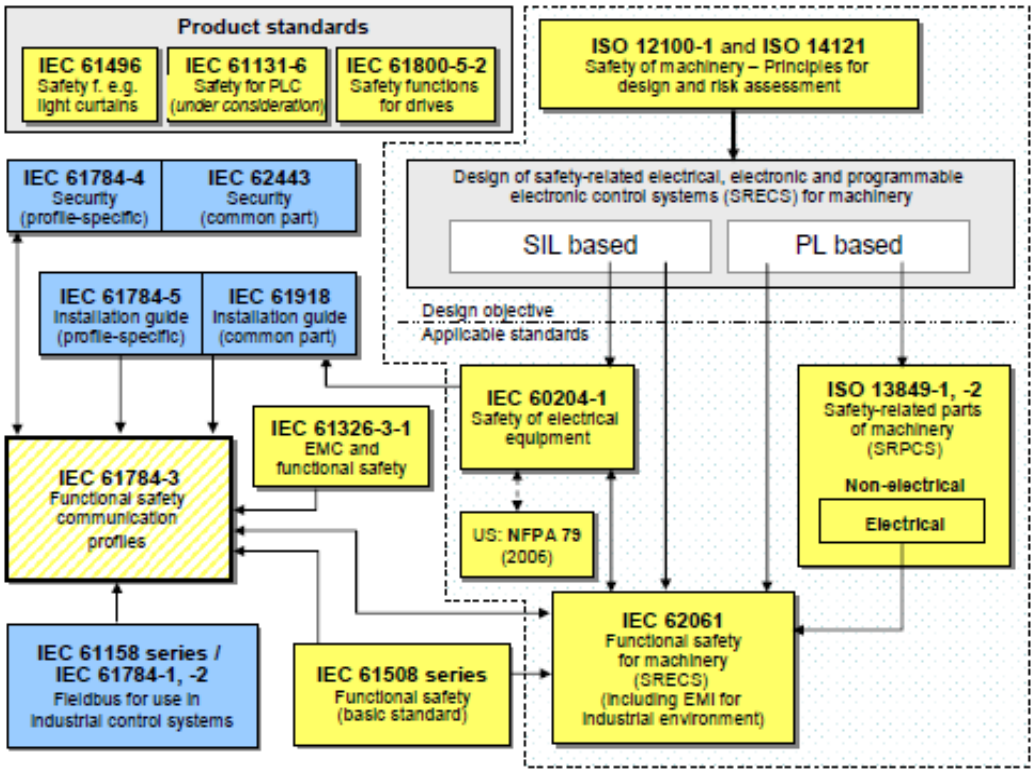
- Společný koncept.
- Přehled technologie – specifikace komunikačních profilů funkční bezpečnosti (Functional Safety Communication Profiles (FSCP's)).
- Společná struktura pro FSCP specifikace v následujících podčástech.

IEC/ČSN EN 61784-3-X: Dodatečné služby specifikace protokolů pro CPF X (CPF – Communication Profile Family). Toto označení odpovídá označením dle specifikace dané normou IEC/ČSN EN 61158. Bezpečnostní profily odpovídajících CPF jsou označovány jako FSCP (Functional Safety Communication Profile)

- Edice 2 (06/2010) obsahuje tyto specifikace:
  - IEC/ČSN EN 61784-3-1: Foundation Fieldbus™ SIS (FSCP 1/1).
  - IEC/ČSN EN 61784-3-2: CIP Safety™ (FSCP 2/1).
  - IEC/ČSN EN 61784-3-3: PROFIsafe™(FSCP 3/1).
  - IEC/ČSN EN 61784-3-6: INTERBUS™ Safety (FSCP 6/7).
  - IEC/ČSN EN 61784-3-8: CC-Link™ Safety (FSCP 8/1).
  - IEC/ČSN EN 61784-3-12: Safety-over-EtherCAT (FSCP 12/1).
  - IEC/ČSN EN 61784-3-13: Ethernet Powerlink Safety (openSAFETY) (FSCP 13/1).
  - IEC/ČSN EN 61784-3-14: EPA Safety (FSCP 14/1).
  - IEC/ČSN EN 61784-3-18: SafetyNET p™ (FSCP 18/1).

V budoucnu se očekává ještě další rozšiřování této normy o specifikace dalších bezpečnostních komunikačních profilů, jako jsou např.: RAPIsafe, P-Net Safety a dalších.

Norem, standardů a doporučení, jakým způsobem realizovat, navrhovat a implementovat ať už bezpečnostní funkce, bezpečné komunikace pro přenos patřičných bezpečnostních dat ve strojním průmyslu nebo v procesní automatizaci, je celé množství. Mnohdy se vzájemně prolínají a doplňují. Jejich vzájemnou souvislost je možné alespoň částečně vyčíst z následujících obrázků obr. 12.2 (**oblast strojních zařízení**) a obr. 12.3 (**oblast procesních zařízení**). [4, 7]



Obr. 12.2 Vztah norem pro funkční bezpečnost a průmyslových sběrnic v oblasti strojních zařízení (upraveno z [4]).

Na Obr. 12. jsou žlutě vyznačeny bezpečnostně orientované standardy, modře pak standardy orientované na sběrnice pole „fieldbus“. Na obrázku jsou uvedeny následující, dříve nezmíněné normy a standardy:

IEC 61496 - Bezpečnostní strojních zařízení - Elektrická snímací ochranná zařízení.

IEC 61131-6 – Programovatelné řídicí jednotky- Funkční bezpečnost (V přípravě, část normy 61131).

IEC 61800-5-2 - Systémy elektrických výkonových pohonů s nastavitelnou rychlostí - Část 5-2: Bezpečnostní požadavky – Funkční.

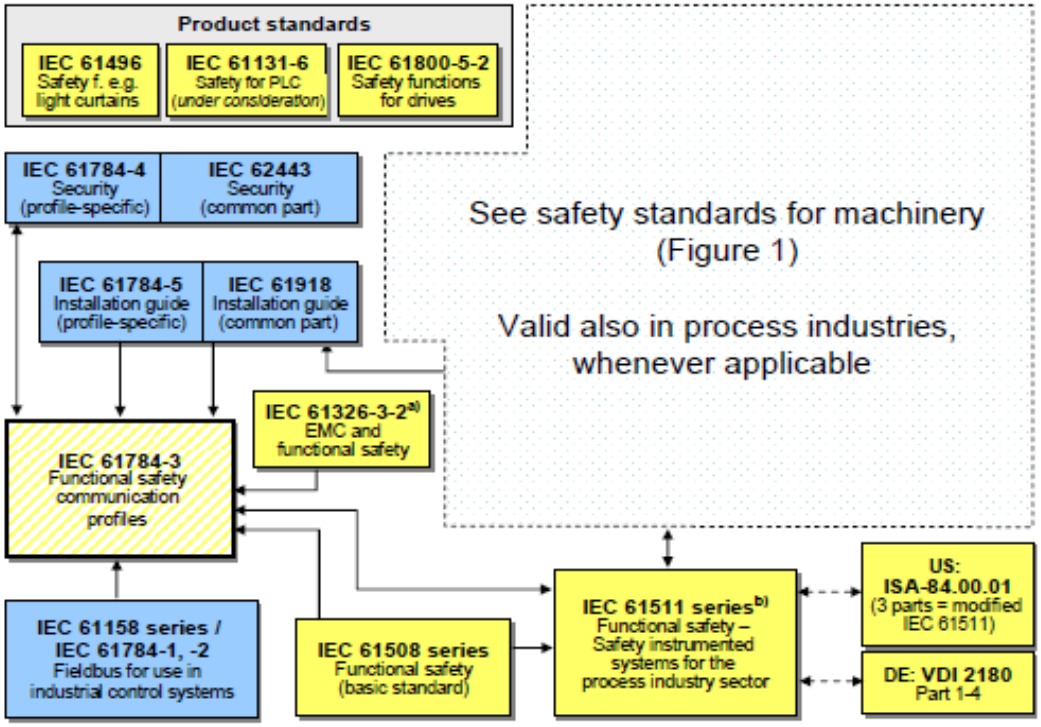
IEC 61326-3-1 - Elektrická měřicí, řídicí a laboratorní zařízení - Požadavky na EMC - Část 3-1: Požadavky na odolnost zařízení zajišťujících nebo určených k zajištění bezpečnosti příbuzných funkcí (funkční bezpečnost) - Všeobecné průmyslové aplikace.

IEC 60204-1 - Bezpečnost strojních zařízení - Elektrická zařízení strojů - Část 1: Všeobecné požadavky.

NFPA 79 – Elektrický standard pro strojní průmysl.

IEC 62443 - Průmyslové komunikační sítě – sítě a systémová bezpečnost

IEC 61918 - Průmyslové komunikační sítě - Instalace komunikačních sítí v průmyslových provozovnách



Obr. 12.3 Vztah norem pro funkční bezpečnost a průmyslových sběrnic v oblasti procesních zařízení (upraveno z [4]).

Na Obr. 12. jsou žlutě opět vyznačeny bezpečnostně orientované standardy, modře pak standardy orientované na sběrnice pole „fieldbus“. Na obrázku jsou uvedeny následující, dříve nezmíněné normy a standardy:

IEC 61326-3-2 - Elektrická měřicí, řídicí a laboratorní zařízení - Požadavky na EMC - Část 3-1: Požadavky na odolnost zařízení zajišťujících nebo určených k zajištění bezpečnosti příbuzných funkcí (funkční bezpečnost) - Průmyslové aplikace se specifikovaným EM prostředím .

ISA-84.00.01 – Americká modifikovaná norma IEC 61511.

VDI 2180 – Německá obdoba normy IEC 61511.

12.2. Životní cyklus bezpečnostní komunikační sběrnice

Životní cyklus bezpečnostní komunikační sběrnice je shodný s obecným životním cyklem obecného HW produktu pro průmyslovou automatizaci a skládá se z následujících kroků:

1. **Koncepce a stanovení požadavků** – stanovení základních požadavků a volba buď standardní průmyslové komunikační sítě, pro kterou bude vytvořen bezpečnostní profil (nadvrstva ISO/OSI), nebo volba úplně nové koncepce výhradně bezpečnostní sběrnice. Vzhledem k tomu, že dnes již existuje řada standardních sběrnic vyhovujících širokému spektru požadavků průmyslové automatizace a celá řada jím odpovídajících bezpečnostních profilů, volí se zpravidla první varianta. Dnes už má však celá řada fieldbus sběrnic specifikovaných normou IEC/ČSN EN 61158 svou vlastní safety vrstvu a na dalších normalizačních specifikacích se pracuje.
2. **Návrh a vývoj** – Spočívá ve volbě správné modelovací metody pro návrh modelu bezpečnostní sběrnice, zahrnující všechny požadavky specifikované normou (SIL, PL, bezpečnostní funkce, …) a také všechny možné chyby a faktory, které mají vliv na spolehlivost a provozuschopnost sběrnice. Výsledkem je pak model celého komunikačního kanálu, založeného na základě již existujících (nová safety vrstva) nebo nových vrstvách

ISO/OSI modelu, tento model, pokud možno co nejpřesněji odpovídající realitě zahrnující všechny externí vlivy a faktory a splňující všechny normativní požadavky.

3. **Výroba a instalace** – je výsledkem předchozího kroku a přenáší se pak do implementace konkrétních SW metod a algoritmů s implementací do konkrétních HW zařízení, tj.: do FW komunikačních karet a rozhraní různých průmyslových zařízení a přístrojů. Součástí je i fyzická instalace kabeláže sběrnice, pokud již nebyla instalována dříve.
4. **Provoz a údržba** – bezpečnostní systém, jehož součástí je bezpečnostní sběrnice, zajišťuje požadované bezpečnostní funkce strojního zařízení, nebo řízeného procesu. Údržba se provádí periodickým vyhodnocováním diagnostických dat provozu na sběrnici, případně vyhodnocením výskytu bezpečnostního zásahu celého systému. Dále pak optickou kontrolou fyzického přenosového média
5. **Likvidace** – nastává v okamžiku změny koncepce, dodavatele, nebo vlivem stárnutí systému apod. [8]

12.3. Modelování bezpečnostní komunikační sběrnice

Modelování přenosových kanálů bezpečnostních komunikačních sběrnic hraje významnou roli při jejich vývoji. Umožňuje odhalit a odstranit většinu nedokonalostí zvolené koncepce již v počátcích vývoje a podat důkaz o úrovni bezpečnosti dané sběrnice. Z pohledu životního cyklu bezpečnostní komunikační sběrnice se zdají být nejdůležitější první dva body, tedy koncepce a specifikace požadavků na tuto sběrnici a následně její návrh a vývoj. Jelikož je celá řada dnes vyvíjených bezpečnostních komunikačních sběrnic založena na již existujících fieldbus standardech (IEC 61158), první bod se zpravidla zjednodušuje jen na výběr již existující sběrnice a specifikaci požadavků a vlastnosti bezpečnostní vrstvy pro tuto sběrnici.

Proto je pak následně důležité spíše vytvoření samostatného modelu bezpečnostní komunikační sběrnice (safety vrstvy) nad již existujícími vrstvami zvolené standardní sběrnice, se zahrnutím všech jejich vlastností. Cílem je vytvořit bezpečnostní komunikační sběrnici s pravděpodobností vzniku chyby/poruchy, rovnající se nule. To je však v praxi zcela nedosažitelné a proto je při vytváření modelu snaha tuto pravděpodobnost vždy alespoň minimalizovat. Velký význam má přitom volba samotné modelovací metody.

Důležité je vybrat metody, které umožňují:

- Modelovat a hodnotit problémy v širokém rozsahu.
- Provádět systematickou kvalitativní nebo kvantitativní analýzu => kvalitativní a kvantitativní přístup.
- Predikovat číselné hodnoty (v případě, pokud jsou dostupná data) => Induktivní a deduktivní přístup.

Z pohledu modelování komunikačního systému je potřebné se zaměřit na následující prvky systému:

- Koncové zařízení s požadovaným SIL uváděného výrobcem (SRE – Safety-Related Equipment).
- Přenosový systém (bezpečnostní vrstva, médium) - (SCL – Safety Communication Layer).

Modelování bezpečnostních vlastností přenosového systému

Modelovaní funkčních vlastností bezpečnostních mechanizmů SCL

Zahrnuje tvorbu úplných, jednoznačných a logických popisů funkčních vlastností bezpečnostních mechanismů. Pro toto je možno velmi úspěšně použit objektově orientované modelování (OOM) – např. UML.

Modelovaní rušících vlivů v komunikačním kanále (EMI)

Zahrnuje modelování vlivů EMI a poruch přenosového kanálu. Výsledkem řešení je výběr kritérií na volbu přenosového a bezpečnostního kódu a výpočet zvýšené chybovosti dekodérů v závislosti na požadavcích na SIL úroveň.

Modelovaní důsledků poruch na bezpečnost přenosového systému

Záměrem je vytvořit model, který umožní identifikovat proces přechodu systému z bezpečného stavu do nebezpečného stavu a umožní vypočítat pravděpodobnost výskytu nebezpečného stavu systému (PFH), jako důsledek působení poruch na činnost systému. [8]

Shrnutí pojmů

Pro sjednocení a standardizaci bezpečnostních komunikačních sběrnic byla vytvořena norma **IEC/ČSN EN 61784-3** nicméně těchto sběrnic je více a ne všechny jsou v této normě definované. Významnou roli při vývoji komunikačních sběrnic má jejich modelování. Umožňuje zohlednit tři základní oblasti: **Modelovaní funkčních vlastností, rušících vlivů a důsledků poruch na bezpečnost přenosového systému.**

Otázky

1. Čemu se věnuje norma IEC/ČSN EN 61784 a její třetí část?
2. Jaký je vztah normy IEC/ČSN EN 61784 k IEC/ČSN EN 61158?
3. Popište základní vztahy norem zabývajících se funkční bezpečností a norem zabývajících se průmyslovými sběrnicemi v oblasti strojních zařízení?
4. Popište životní cyklus bezpečnostní komunikační sběrnice?
5. K čemu slouží modelování bezpečnostních komunikačních sběrnic?

Použitá literatura a další zdroje

1. Láryš, T., Koziorek, J. Význam diagnostiky komunikačních sběrnic v průmyslové automatizaci, *Technická diagnostika z1/2010, ročník XIX*, Ostrava, Asociace technických diagnostiků ČR o.s., 2010, s. 30, ISSN: 1210-311X
2. Láryš, T. Methods and mechanisms for provision safety data transfer at safety fieldbuses, Workshop doktorandů WOEFEX, ročník 2010, Ostrava, VŠB-TU Ostrava - FEI, 2010.
3. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 1998
4. IEC 61784-3 Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial network
5. Franeková, M., Janota A., Rástočný K. Trendy v oblasti komunikačnej bezpečnosti priemyselných sietí. *Advances in Electrical and Electronic Engineering. 2005, vol. 4.* Ostrava 2005. s.253 – 258. ISSN: 1804-3119.

6. Zezulka, F., Úvod do oblasti řídicích počítačů – Část 2, Brno, 2007, VUT Brno – FEEC, [online], [cit. 15-12-2010] http://www.uamt.feec.vutbr.cz/~zezulka/download/LAUP/bezp.pdf
7. Strpf, W., Fieldbus Standard IEC 61158 - Safety Communication Profiles IEC 61784-3, Siemens AG, 2007, Hannover, [online], [cit. 15-12-2010] http://www.dke.de/de/Service/Nachrichten/documents/3stripf.pdf
8. Franeková M., Modelovanie bezpečnostných vlastností priemyselných sietí typu safety fieldbus, Odborný seminář: *„Bezpečnostne relevantné priemyselné a komunikačné systémy*“ sdružení Profibus.sk, Žilina, 2009, [online], [cit. 15-12-2010] http://www.profibus.sk/fileadmin/user_upload/prezentacia_modelovanie_Fieldbus_Fra-1.pdf

Řešená úloha 12.1

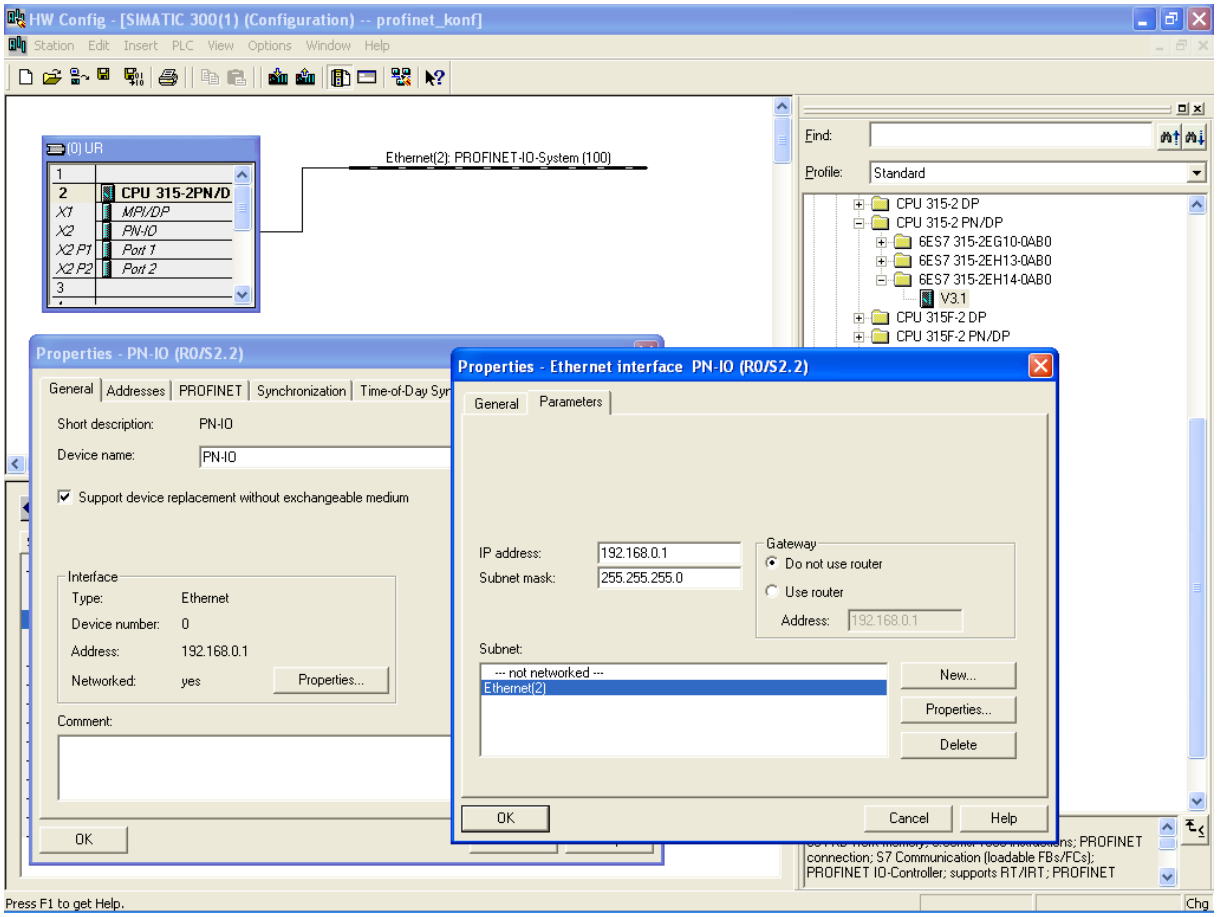
Zadání: Vytvořte konfiguraci a uveďte do provozu 3 zařízení využívající sběrnici Profinet od firmy Siemens. Jako řídicí modu je využito: CPU315-2PN/DP6ES7 315-2EH14-0AB0.

Aplikace vyžaduje po jednotce distribuovaných vstupů a výstupů rychlé odezvy měření analogových hodnot ze snímačů tlaku a rychlé načítání stavů digitálních vstupů. Na druhou jednotku distribuovaných vstupů a výstupů jsou přivedeny informace o stavech stykačů a tlačítek a nevyžadují zvláštní rychlost.

Vyberte vhodný hardware a oživte danou sestavu.

Pro vytvoření a uvedení HW konfigurace do chodu se využije programovacího balíku STEP7 V5.5 Professional 2010 nebo V5.4 + SP5.

Základní konfigurace řídící jednotky vyžaduje vložit tento řídicí modul do RACKu, vytvořit novou ethernetovou síť a přiřadit centrální řídicí jednotce příslušnou IP adresu.

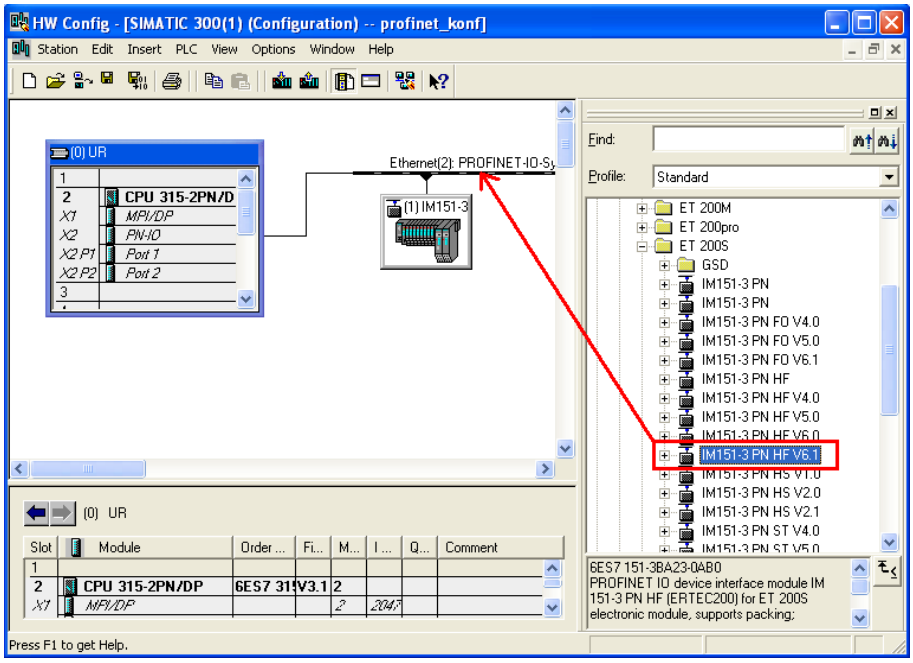


Obr. 12.4 Konfigurace komunikace na sběrnici Profinet.

Pro připojení všech třech zařízení na sběrnici využijte sběrnicovou topologii, protože všechny moduly mají integrovaný dvou portový switch.

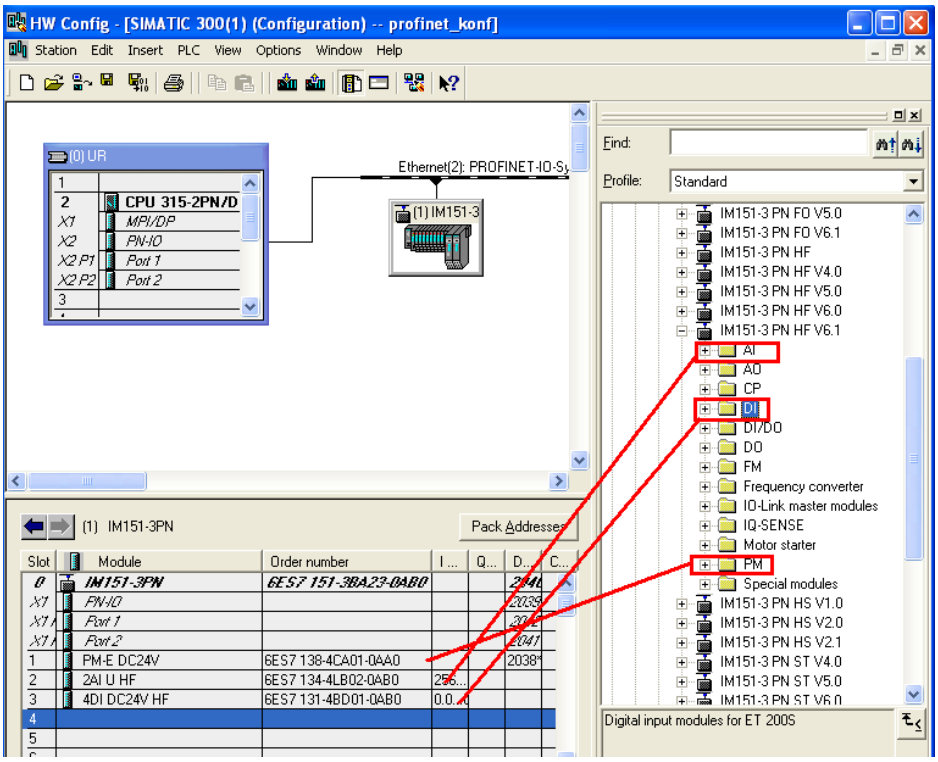
První modul distribuovaných vstupů a výstupů musí být vybrán v provedení HF tj. high feature. Tyto moduly jsou velmi rychlé a proto bude splněna podmínka na rychlé měření analogových signálů . Jednotka distribuovaných systémů není určena avšak musí být vybrána ze složky Profinet IO →I/O→ET200S. Protože využíváme metalický kabel pro komunikaci vyberte typ: IM151-3 PN HF V6.1 obj.č. 6ES7 151-3BA23-0AB0

Kliknutím na daný modul a jejím přetažením se stisknutým levým tlačítkem myši přesuňte tento modul na vytvořenou sběrnici Profinet-IO Systém.



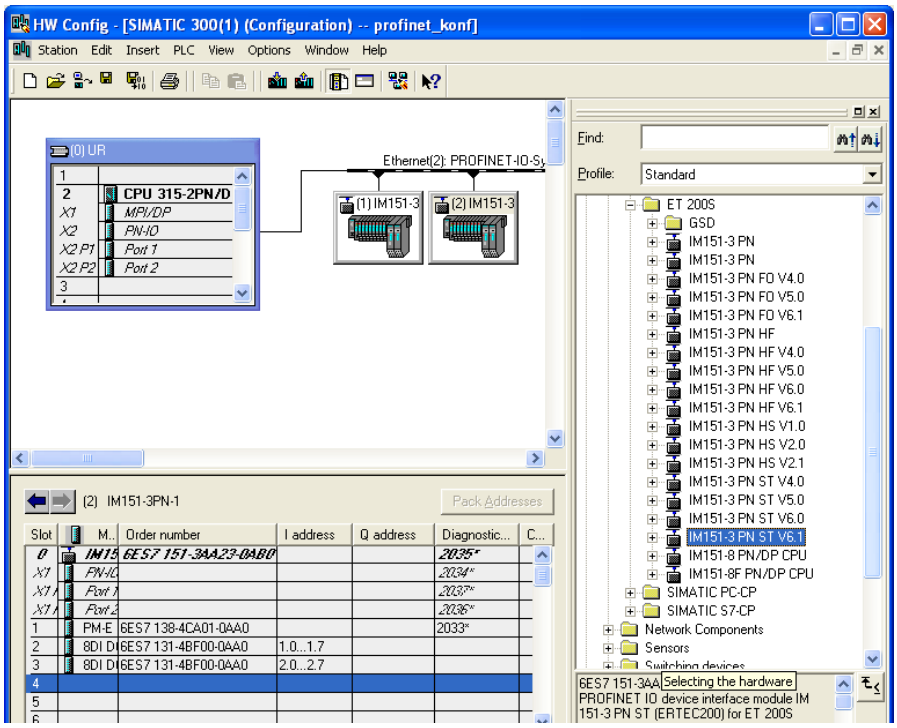
Obr. 12.5 Konfigurace komunikace na sběrnici Profinet.

Aby jednotka distribuovaných vstupů a výstupů pracovala správně, je nutné do prvního slotu umístit napájecí modul za něj příslušný modul analogových vstupů a digitálních vstupů. Jednotlivé moduly se musí vybrat ze složky interface modulu.



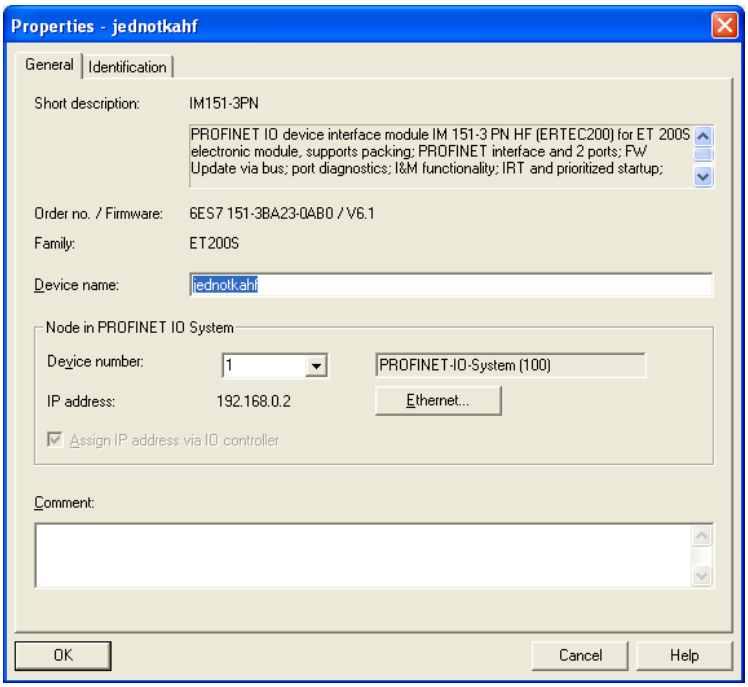
Obr. 12.6 Konfigurace komunikace na sběrnici Profinet.

Stejným způsobem se vloží další decentrální jednotka vstupů a výstupů s tím, že není zde nutné využívat modulů, které jsou velmi rychlé a proto interface modul spolu s dalšími moduly mohou být vybrány s označením ST např. IM151-3 PN ST V6.1.



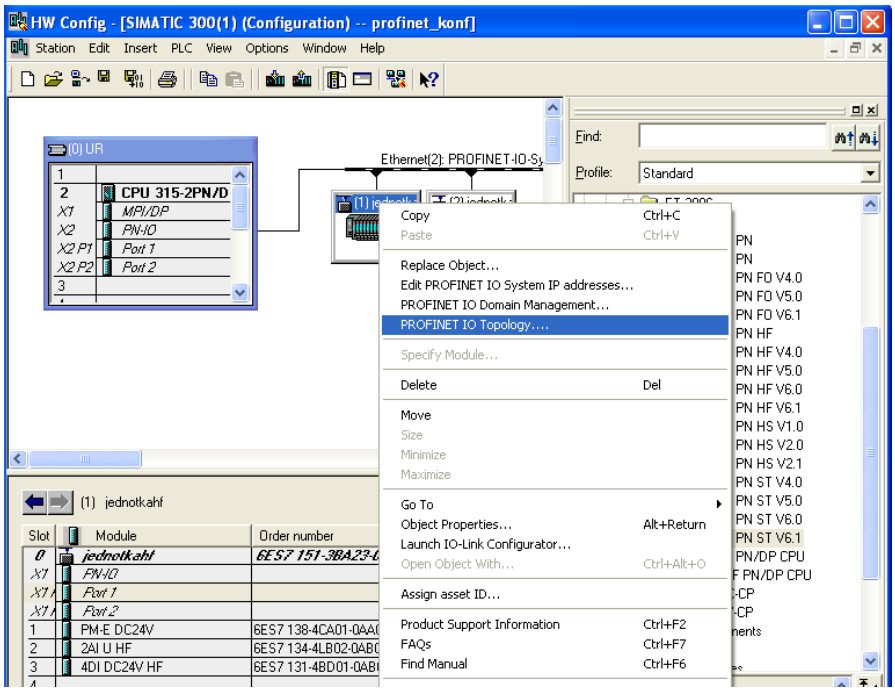
Obr. 12.7 Konfigurace komunikace na sběrnici Profinet.

Každý modul na sběrnici Profinet musí mít jednoznačné jméno. Proto je nutné jej v dalším kroku oběma modulům přidělit kliknutím na modul pravým tlačítkem myši a výběrem Object Properties. Pojmenujte dané periferie např. Jednotkahf a Jednotkast.

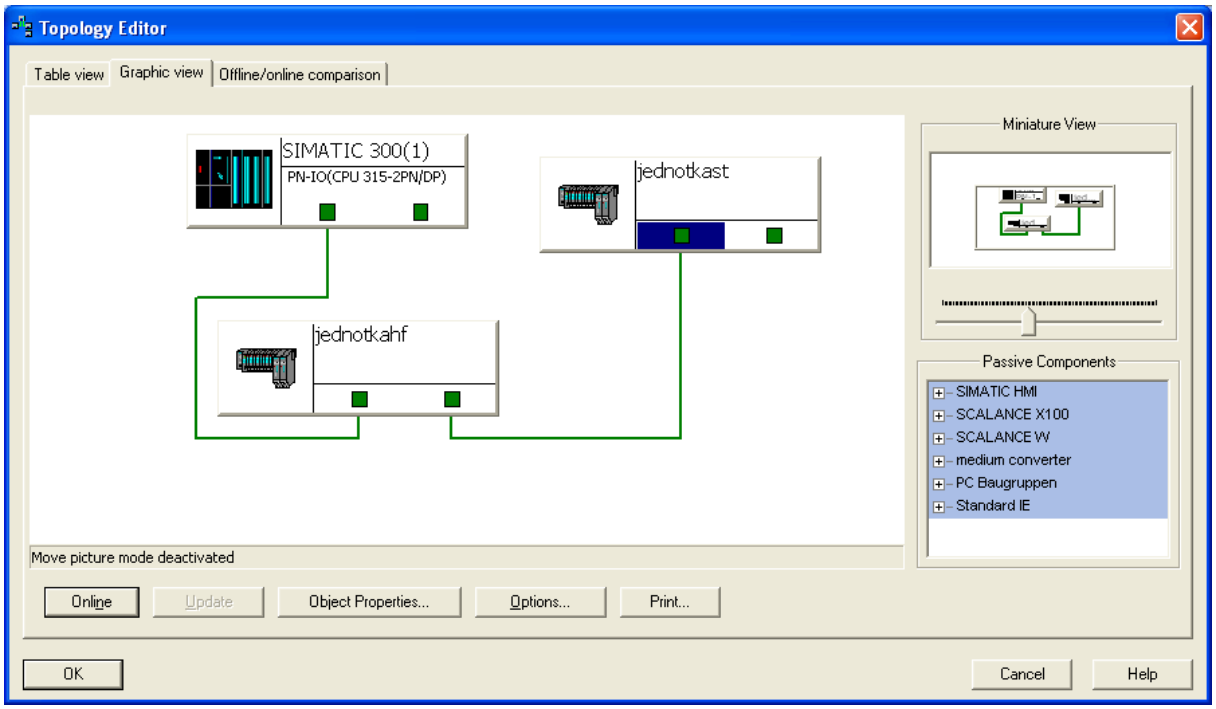


Obr. 12.8 Konfigurace komunikace na sběrnici Profinet.

Pro zajištění konzistence projektu je nutné doplnit také Profinet topologii. Kliknutím pravým tlačítkem myši na sběrnici Profinet a výběrem Profinet IO Topology se otevře editor, zvolte záložku Graphics view. Zde v této záložce technikou Drag &Drop propojte jednotlivé moduly.



Obr. 12.9 Konfigurace komunikace na sběrnici Profinet.

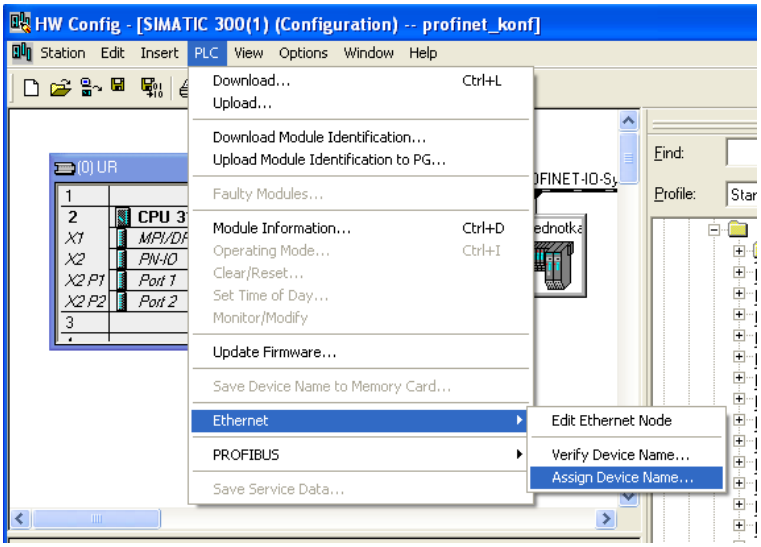


Obr. 12.10 Konfigurace komunikace na sběrnici Profinet.

Tím je dokončena konfigurace IO Topologie. Projekt může být uložen a zkompilován Station → Save and Compile.

Před zápisem HW konfigurace do PLC je nutné ověřit síťové připojení PC v menu Options →Set PG/PC Interface.. Zde nastavte připojení TCP/IP.

Dále je nutné přidělit jména jednotkám ET200S. Klikněte v hardwarové konfiguraci na modul ET200S a v menu vyberte PLC→Ethernet→Assign device name.



Obr. 12.11 Konfigurace komunikace na sběrnici Profinet.

Po kliknutí na tuto volbu bude celá síť zmapována a do tabulky budou vypsány dostupná zařízení. Každé zařízení má svoji MAC adresu, jak centrální řídicí modul, tak jednotlivé interface moduly. Podle dané MAC adresy musíte přiřadit správné jméno. Po úspěšném přiřazení jmen všem modulům je možné zapsat HW konfiguraci kliknutím na PLC→Download.

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI12\

13. BEZPEČNOSTNÍ KOMUNIKAČNÍ SBĚRNICE

Čas ke studiu: 3 hodiny

Cíl Po prostudování této kapitol:y znát základní informace o nejpoužívanějších bezpečnostích komunikačních sběrnicích:

- Ethernet Powerlink Safety (openSafety).
- Profil Profisafe pro Profibus a Profinet.
- AS-iSafe.
- EtherNET/IP Safety.
- Safety over EtherCAT.

Výklad

V předcházející části textu byly popsány základní principy funkce bezpečnostních komunikačních sběrnic, Jak již bylo uvedeno, pro standardizaci bezpečnostních profilů komunikačních sběrnic dnes slouží především norma IEC 61784-3, kde jsou popsány specifikace standardizovaných profilů. Nicméně existuje celá řada dalších bezpečnostních profilů a sběrnic, které v této normě uvedeny nejsou. Avšak i v uvedené normě je dnes standardizováno již devět bezpečnostních profilů. Proto budou v následující části blíže popsány jen některé z nich, a to ty v průmyslové praxi nejvíce rozšířené.

13.1. Ethernet Powerlink Safety (openSafety)

Základní vlastnosti komunikačního protokolu Ethernet Powerlink (EPL) vyvinutého společností B&R byly popsány v kapitole 10.2. Tato sběrnice je charakteristická svou determinističností a tedy vhodností pro použití v aplikacích reálného času. Další práce skupiny EPSG (Ethernet Powerlink Standardization Group) na EPL spočívala ve vývoji bezpečnostního profilu pro tuto sběrnici s názvem EPLsafety. Pod tímto názvem byl profil původně také standardizován v první edici normy IEC 61784-3-13 (FSCP 13). Nicméně vývoj tohoto profilu pokračoval dál a vzhledem k jeho vhodnosti pro použití na prakticky jakékoli sběrnici ethernetového typu bylo jeho použití rozšířeno o možnosti aplikace na sběrnicích SERCOS III, MODBUS TCP/IP, Ehernet/IP a nově i Profinet, což pravděpodobně povede k rychlému rozvoji a rozšíření těchto sběrnic s penSAFETY profilem na průmyslovém trhu. Z důvodu jeho univerzálnosti byl následně změněn jeho název na openSAFETY, pod kterým bude také uveden v příští edici normy IEC 61784-3-13. Bezpečnostní profil openSAFETY splňuje kritéria úrovně integrity bezpečnosti až do SIL 3 podle normy IEC/ČSN EN 61508. Samotná sběrnice EPL vychází z principů sběrnice CANopen a z toho důvodu využívá všech jejích vlastností, především slovníků objektů aplikační vrstvy.

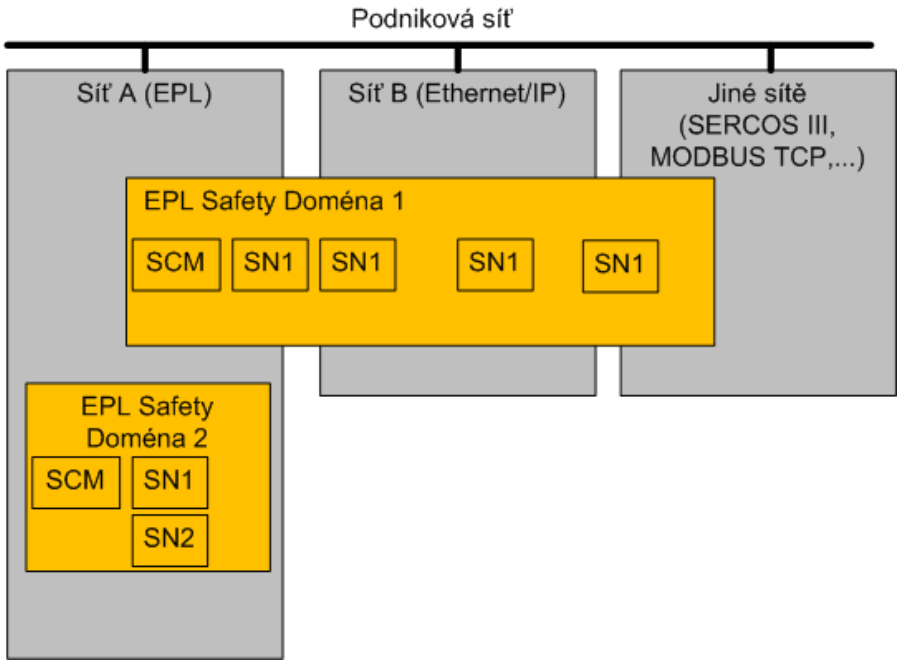
Princip funkce openSafety profilu spočívá, stejně jako u většiny bezpečnostních profilů, v charakteristickém tvaru rámců přenášených po sběrnici. U tohoto profilu se konkrétně jedná o přístup, kdy jsou v jednom rámci zasílány dva identické podrámce stejného obsahu. Každý podrámec je doplněn zabezpečovacím kontrolním součtem. Přijímač pak porovnává oba identické podrámce. Pravděpodobnost, že dojde k poškození dat při přenosu v obou podrámcích je extrémně nízká a dále klesá s rostoucí délkou rámce. Při použití tohoto typu rámce je velmi nepravděpodobné

také riziko poruchy typu „masquerades“ (maškaráda – entita se vydává za jinou) a předchází se také špatnému vyhodnocení standardních maskovaných zpráv.

DATA	*CRC*	*DATA*	*CRC*
Podrámec 1		**Podrámec 1**	
bezpečnostní rámec			

Obr. 13.1: Základní princip openSAFETY rámců.

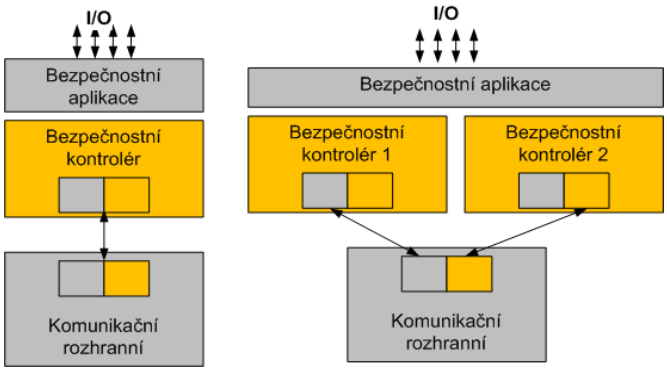
V rámci sběrnice openSafety může existovat až 1023 domén a v každé z nich pak 1023 zařízení. Safey domény mohou být rozšiřovány dalšími sběrnicemi. V každé doméně může existovat Safety Communication Manager (SCM), který monitoruje všechna zařízení v doméně zvané Safety Nodes (SN). SCM je odpovědný za alokaci adres SN, uložení specifických parametrů a permanentní monitorování SN. Komunikace mezi jednotlivými safety doménami pak zajišťuje Safety Gateway. S EPL safety si může uživatel vytvářet sítě s různou hierarchií právě tak jako si pouze vytvořit jednu safety síť.



Obr. 13.2 Safety domény openSafety technologie (upraveno z [1, 2]).

Hardwarový koncept pro Powerlink Safety

Úroveň integrity bezpečnosti (SIL), která může být dosažena se softwarem openSAFETY převážně závisí na použité HW architektuře. Software openSAFETY byl vytvořen pro použití v zařízeních se SIL-3. K dosažení požadavků SIL-1 je dostačující použít např. jeden jednoduchý Safety Controller (SC), který zajistí bezpečnost aplikace. K dosažení SIL-3, musí být Safety Controller navržen jako redundantní.



Obr. 13.3 a) SIL-1/SIL-2 hardwarová architektura b) SIL-3 hardwarová architektura (upraveno z [1, 2]).

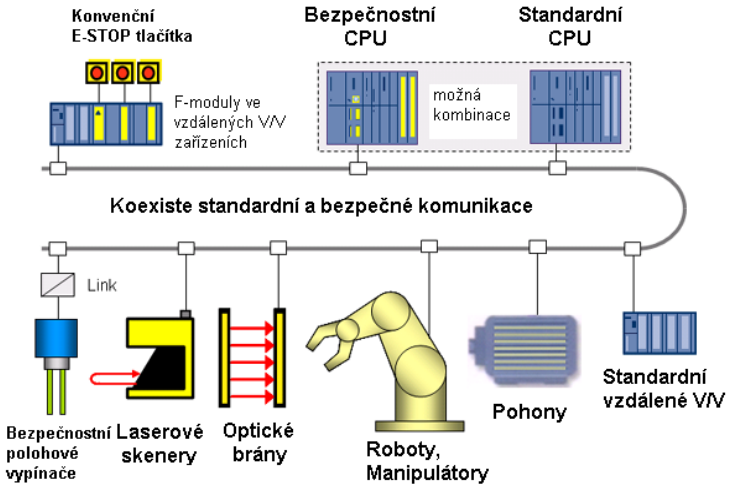
Bezpečnostní sběrnice EPL openSAFETY se od ostatních bezpečnostních sběrnic liší, a to diametrálně. Byla totiž vyvinuta za účelem integrace bezpečnostních funkcí do řešení využívajících různé sběrnicové systémy. Hlavní výhodou je především základ na bázi ethernetového HW bez nutnosti vývoje dalších specifických HW komponent. Už samotný protokol EPL je voně šiřitelný jako openSource stejně jako specifikace profilu openSafety pod BSD licencí. Ve spojení bezpečnostních kritérií profilu openSAFETY s hlavními výhodami EPL jako je rychlost, determinističnost, má tato sběrnice potenciál stát se mezinárodně uznávaným a široce používaným standardem pro průmyslovou komunikaci. Spojení EPL a openSafety je sice velice preferováno, ale v podstatě nic nebrání tomu použít tuto technologii i s jinými ne bezpečnými sběrnicemi (především založenými na bázi Ethernetu, ale ne jen jeho). Díky openSource protokolu openSAFETY je pak prakticky komukoli umožněno vyvinout si bezpečností profil pro vlastní (ne jen) ethernetovou sběrnici. Lze také dále předpokládat, že EPSG bude pokračovat ve vývoji dalších openSafety řešení pro sběrnice na bázi průmyslového Ethernetu. [1, 2]

13.2. PROFIsafe

Jedná se o bezpečnostní komunikační profil vyvinutý společností Siemens pro použití s komunikačními sběrnicemi Profibus a Profinet. V mezinárodní normě IEC 61784-3-3 je standardizován pod označením FSCP 3. Jednalo se vůbec o první bezpečnostní profil uvedený v této normě. Stejně jako většina bezpečnostních sběrnic, jsou i sběrnice Profibus a Profinet s tímto profilem certifikovány pro použití v systémech s úrovní integrity bezpečnosti až SIL 3. Profil PROFIsafe existuje ve dvou verzích. Verze V1 pro použití se sběrnicí Profibus-DP (CPF 3/1) a verze V2 pro použití se sběrnicemi Profinet IO (CPF 3/2), Profinet CBA (CPF 3/3) a/nebo Profibus-DP. Verze V2 je už tedy univerzální profil pro obě platformy. Pro verzi Profibus-PA, pro použití v procesní automatizaci (IEC61511) publikovala standardizační organizace NAMUR normu NE97 pro specifikaci bezpečné komunikace zařízení v této sběrnici.

Prakticky od počátku je tento otevřený a uživatelsky nezávislý standard podporován sdružením Profibus International (PI) sdružující velké množství výrobců a uživatelů. Nevýhoda oproti předchozímu profilu openSAFETY spočívá v omezeném použití pouze pro sběrnice Profibus a Profinet. V bezpečnostních aplikacích systémů TIA (Totally Integrated Automation) firmy Siemens slouží sběrnice s tímto profilem pro zajištění funkční bezpečnosti celé řady komunikujících komponent od bezpečnostních logických automatů, přes decentralizované moduly vstupů/výstupů, jednotky pro řízení pohonů až po brány do jiných standardních nebo bezpečnostních sítí jako je ASIsafe (sběrnice AS-i s bezpečnostním profilem). Stejně jako většina sběrnic s bezpečnostními profily i tato umožňuje současný přenos safety a non-safety dat, stejně jako propojování standardních a bezpečnostních segmentů sítě Profibus nebo Profinet. Důležitým faktorem, díky

kterému získává v současné době profil PROFIsafe náskok před svými konkurenty je implementace tohoto profilu do bezdrátových sítí jako je WLAN a Bluetooth.



Obr. 13.4 Příklad využití protokolu PROFIsafe (upraveno z [3]).

Zařízení připojené do sítě PROFIsafe, musí mít na síti jednoznačnou hardwarově nastavovanou adresu (F-adresu). V případě komunikace s využitím bezpečnostních funkcí má přenášená zpráva vyšší prioritu než zprávy ostatní. Vysílač a přijímač na síti jednoduše identifikují, že zpráva je na síti jedinečná, čímž se ověřuje její platnost. Pro bezpečnostní prvky ve sběrnicích s profilem PROFIsafe jsou definovány a dodržovány standardy známé z Profibus a Profinet jako např. GSD soubory. Zde jsou uloženy parametry všech komunikujících komponent, jako jsou například, frekvenční měniče, moduly vzdálených vstupů/výstupů (I/O), laserové skenery apod. zvaná *F-Devices*. GSD soubory pro takováto zařízení jsou obdobné těm standardním, nicméně specificky doplněny/pozměněny v závislosti na svých bezpečnostních funkcích a obecnému určení pro bezpečnostní komunikaci. Tyto specifické parametry jsou nazývány *F-parameters*. Bezpečnostní parametry typické pro konkrétní zařízení (např. laser skener) se nazývají *„iParameters“*. Uložení a přenos všech těchto parametrů do komunikujících zařízení musí být taktéž zabezpečen. Tyto *F-parametry* jsou přenášeny do komunikujícího zařízení během konfigurace a jsou to například použitá SIL úroveň, kódové označení, konfigurace vstupů/výstupů, nastavení watchdog apod. Bezpečnostní řídicí automaty, ve kterých je realizována bezpečnostní aplikace (možno i standardní), jsou nazývány *F-Host*. Komunikující zařízení si pak s bezpečnostním řídicím automatem (*F-Host*) v závislosti na bezpečnostní aplikaci mezi sebou zasílají aplikační data, zvaná *F-I/O data*.

Profil PROFIsafe umožňuje detekovat chyby jako např. narušení adresy, zpoždění nebo ztráta dat pomocí následujících mechanismů:

- Sekvenční číslování PROFIsafe zpráv.
- Monitorování času (watchdog).
- Identifikace odesilatele a příjemce pomocí F-adres.
- CRC kód.

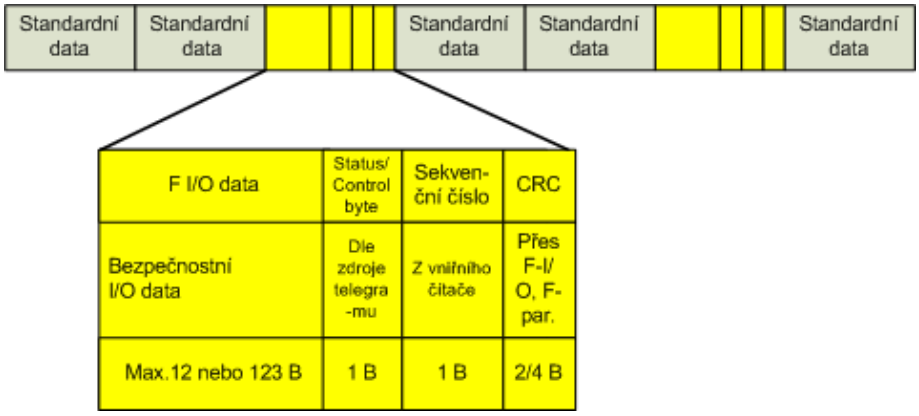
Přehled vztahů mezi bezpečnostními opatřeními a komunikačními poruchami, které je možno eliminovat jsou uvedeny v následující tabulce.

Tab. 13.1 - Přehled možných chyb a poruch na sběrnici a metody jejich detekce a eliminace

Opatření / Chyba	Sekvenční číslování	WatchDog	Status/Control Byte	CRC
opakování	●			
ztráta dat	●	●		
vsunutí	●	●	●	
nesprávné pořadí	●			
poškození dat				●
zpoždění		●		
spřažení safety a standardních dat (Maskarade)		●	●	●
FIFO chyba registru (chyba dodržení pořadí First-IN – First-Out)		●		
chyba paměti síťového prvku (Switch)	●			

PROFIsafe formát zprávy

PROFIsafe zprávy, které se přenášejí mezi bezpečnostními řídícími jednotkami a jeho bezpečnostními moduly, jsou přenášeny spolu se standardními zprávami na sítích Profibus nebo Profinet. Formát PROFIsafe telegramu se skládá z následujících částí: blok *F-I/O* dat, Status/Control Byte, blok pro přenos hodnoty čítače sekvenčního číslování zpráv (pouze u verze V1) a blok pro přenos CRC kódu. *V F-I/O* data bloku se přenáší bezpečnostní informace mezi *F-Host* a *F-Device*. V závislosti na aplikacích, kde jsou různé požadavky na délku (počet) přenášených dat, existují dva typy bezpečnostních telegramů – krátký (do délky 12 Byte) a dlouhý (do délky až 123 Byte). *F-I/*O data jsou následována jedním „*Control bytem*“, pokud se jedná o přenos z *F-Host* do *F-Device*, nebo jedním „*Status bytem*“ pokud se jedná o přenos opačného směru. Tento „*Control/Status byte*“ slouží pro synchronizaci odesilatele a příjemce PROFIsafe zprávy. Následuje blok tří bytů pro přenos hodnoty čítače sekvenčního čísla. Ten slouží k rozpoznání, jestli přijímač přijal všechny telegramy a to i ve správném pořadí. Každý zaslaný rámec očekává potvrzení v podobě rámce se stejným pořadovým číslem. Hodnota „0“ je vyhrazena pro první spuštění nebo indikaci poruchy. Pro tento účel je použit 8-bitový čítač (1 Byte) ve verzi V1 a 24-bitový čítač (3 Byty) ve verzi V2. Od verze V2 se už také nepoužívá přenos celé hodnoty čítače (celé 3 byty), ale pouze virtuální hodnota čítače (*VCN - Virtual Consecutive Number),* reprezentována tzv. „Toggle“ bitem přenášeným v rámci „*Status/Control byte*“. Sekvenční čítač je umístěn v *F-Device* a neguje hodnotu tohoto bitu každou inkrementací vnitřního čítače. Tato modifikace umožňuje eliminovat případnou chybu paměti některých síťových komponent (switch). Poslední částí telegramu je CRC kontrolní součet. Jeho délka se liší podle módu délky přenášených dat a verze profilu. Pro verzi V1 jsou to 2 byty pro max. délku dat 12 byte a 4 byty pro max. délku dat 123 byte. U verze V2 (označováno také někdy jako CRC2) je to 3 byty pro max. délku dat 12 byte a 4 byty pro max. délku dat 123 byte. Kontrolní součet se vypočítává přes F-I/O data a F-parameters (u V2 ještě také přes VCN). Na následujících obrázcích jsou zobrazeny struktury telegramů obou verzí profilu PROFIsafe a jejich vnoření do standardního toku dat. [3, 4]



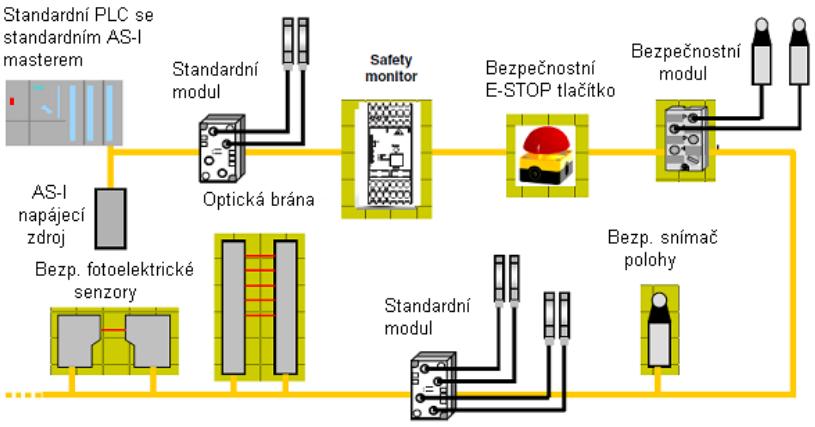
Obr. 13.5 Bezpečnostní telegram vložený ve standardním datovém toku na příkladu ProfiSafe V1 (upraveno z [3, 4]).

F I/O Data	Status/Control Byte		CRC2
		Toggle Bit	Přes F I/O data a F-parameters
Max. 12 nebo 123 Byte	1 Byte		3 nebo 4 Byte

Obr. 13.6 Struktura bezpečnostního telegramu ProfiSafe V2.

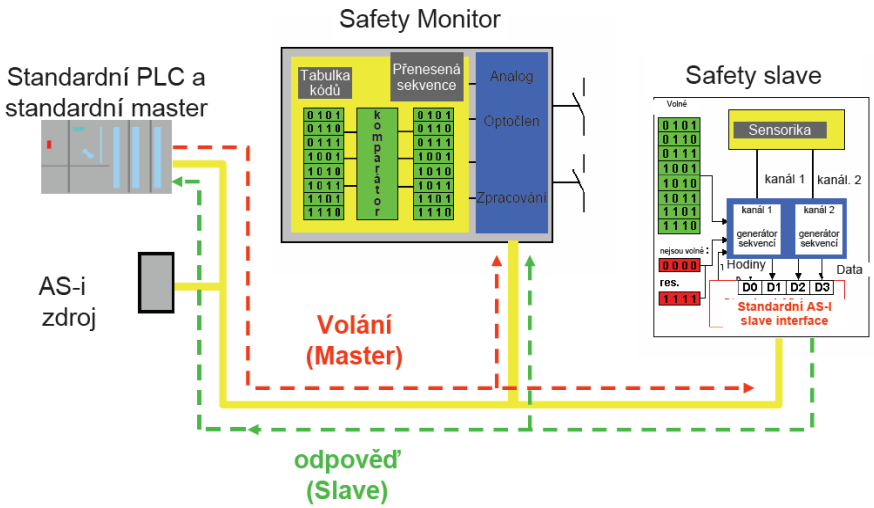
13.3. Safety At Work (ASIsafe)

Pro bezpečnou komunikaci na sběrnici AS-Interface slouží bezpečnostní profil AS-i Safety At Work, někdy také zjednodušeně označován jako ASIsafe. Jedná se o koncepci poněkud odlišnou od dvou předchozích, jelikož je založena i na speciálním HW zařízení, o kterém bude řeč dále. Tento profil není také specifikován v normě IEC 61784-3, nicméně je certifikován pro použití v systémech pro zajištění funkční bezpečnosti až do úrovně SIL3 podle nory IEC 61508. Splněn je také obecný předpoklad u těchto sběrnic na současnou standardní a safety komunikaci a tedy použití standardních i bezpečných slave zařízení na sběrnici AS-i. V zásadě existují v současnosti dvě možnosti koncepce použití této bezpečné komunikace v safety-orientovaných aplikacích.



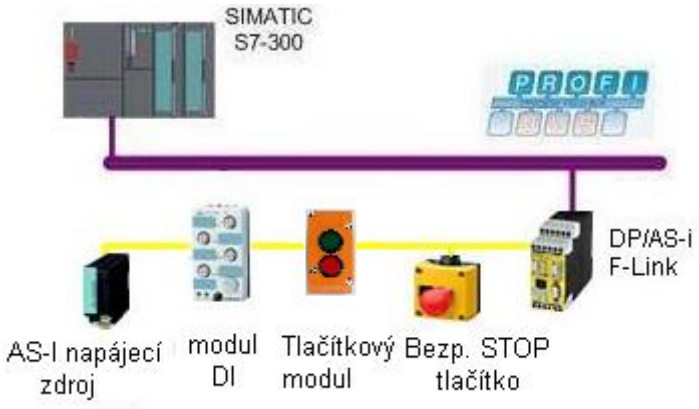
Obr. 13.7 Celková koncepce propojení standardní a safety oblasti na sběrnici AS-i (upraveno z [9]).

První je založena na použití tzv. Safety Monitoru spolu s bezpečným slave (Safety Slave), nebo i několika najednou. Bezpečný slave je z hlediska sběrnice AS-i, slave jako každý jiný. Má přidělenou slave adresu, komunikuje stejným principem na úrovni linkové vrstvy. Nicméně obsahuje pouze bezpečné vstupy, tzn., že neexistuje slave z bezpečnými výstupy pro bezpečné řízení akčních členů. Nicméně existuji AS-i slave moduly kombinující v jednom HW celku bezpečné vstupy spolu se standardními výstupy. Bezpečné vstupní slave moduly mohou existovat i v podobě optických bran či laserových skenerů apod. Každý bezpečný slave má v sobě výrobcem naprogramovanou bitovou tabulku (8 x 4 bitů) nesoucí informaci o stavu jeho vstupů. Tuto tabulku vysílá bezpečnostní slave na dotaz mastera na sběrnici v kódové sekvenci po čtyřech bitech. Pro tuto sekvenci platí řada pravidel. Masterem na sběrnici může být v tomto případě standardní AS-i master (PLC). Safety Monitor, který je současně i akčním členem sběrnice ASIsafe, neustále monitoruje komunikaci mezi masterem a slave zařízeními a porovnává data vysílaná bezpečnostními slave s uloženými tabulkami, tedy porovnává přijatou kódovou sekvenci s referenční hodnotou, kterou má uloženou v paměti. Tuto referenční hodnotu všech bezpečnostních slave modulů si Safety Monitor uloží do paměti při prvním spuštění. V případě že dojde k detekci rozdílu mezi zasílanou a referenční hodnotou stavu slave vstupního zařízení, vygeneruje Safety Monitor povel na uvedení celého systému do bezpečného stavu, prostřednictvím svých digitálních výstupů připojených např. na stykače akčních prvků. Safety Monitor obsahuje dva mikroprocesory, které nezávisle na sobě provádějí porovnávání přijímaných sekvencí a navzájem také kontrolují svojí činnost. Safety Monitor je možné konfigurovat SW nástrojem ASIMon. Zde je možné definovat logická pravidla funkčních podmínek (logické kombinace stavů několika slave vstupů) pro sepnutí nebo rozepnutí kontaktů relé bezpečnostního monitoru. Touto aplikací se nastavuje i slave adresa Safety Monitoru a je možné vyčíst celou strukturu bezpečnostní sítě. Kontakty relé Safety Monitoru je pak možno připojit na stykače akčního členu (např. motoru) pro uvedení stroje do bezpečného stavu (většinou stop/klid stav).



Obr. 13.8 Princip zajištění funkční bezpečnosti díky přenosu kódové sekvence (upraveno z [9]).

Druhou možností je použití bezpečnostních slave modulů na sběrnici AS-i spolu s převodníkem DP/AS-i F-Link. Ten slouží jako komunikační rozhraní mezi průmyslovými sítěmi AS-i (profil ASIsafe) a Profibus-DP (profil PROFIsafe). Shromažďuje signály binárních bezpečnostních senzorů na nejnižší úrovni řízení, které komunikují v bezpečnostním profilu ASIsafe a předává je nadřazené úrovni komunikující v profilu PROFIsafe, která je reprezentovaná bezpečnostním PLC. Kromě toho je plnohodnotnou jednotkou master splňující požadavky specifikace AS-i s obousměrným přenosem standardních binárních i analogových hodnot. Toto zařízení v sobě zahrnuje AS-i Master a Safety Monitor pro převod bezpečnostních signálu ze vstupu AS-i do protokolu PROFIsafe.

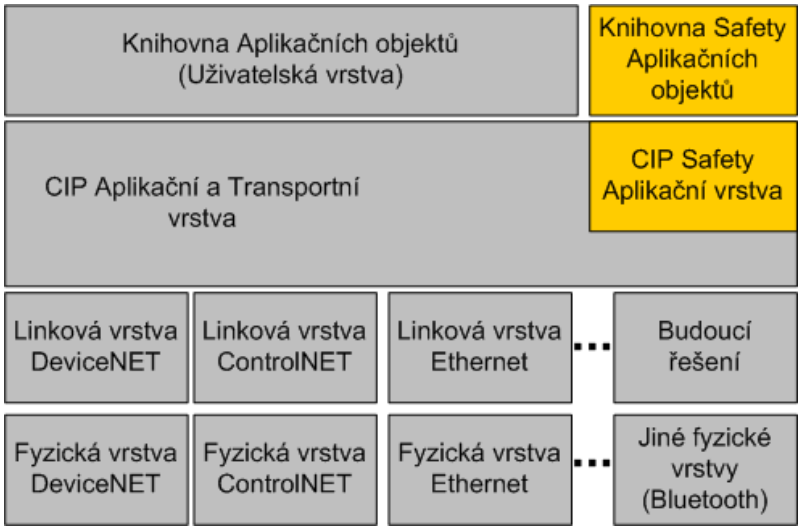


Obr. 13.9 Aplikace s využitím ASIsafe a DP/AS-i F-Link (instalace v Laboratoři programovatelných automatů na VŠB-TU Ostrava).

Řešení funkční bezpečnosti na bázi této sběrnice nachází řadu zastánců a aplikačního užití díky své jednoduchosti, která vyplývá již ze standardní koncepce AS-i. Rozšíření o bezpečnou komunikaci spočívá pouze v doplnění stávající koncepce o bezpečnostní monitor a slave vstupní zařízení. Safety Monitor je navíc oproti bezpečnostním PLC poměrně jednoduché zařízení což má vliv i na ekonomickou stránku věci. Tato sběrnice pro bezpečnou komunikaci tak nachází uplatnění tam, kde je třeba současnou instalaci sítě AS-i komponent doplnit nebo upravit pro bezpečně orientovaný provoz s patřičnou úrovní SIL. To může nastat například v souvislosti s novými legislativními požadavky na bezpečnost provozu již dříve realizovaných aplikací. Z ekonomického hlediska je tak výhodnější současnou sběrnici AS-i doplnit Safety Monitorem a doplnit/nahradit bezpečnostní vstupy, takže není třeba měnit stávající PLC za nesporně dražší bezpečnostní PLC. Další výhodou je i garantovaná doba odezvy od vyhodnocení chyby až po zásah Safety Monitoru, která je max. 40ms. Nespornou výhodou je i možnost propojení této sběrnice se sběrnicí Profibus-DP a jeho aplikací s profilem PROFIsafe. [5, 6, 7, 8]

13.4. EtherNET/IP Safety

Tak jak bylo uvedeno v kapitole 10.3 (sběrnice EtherNET/IP), je tato sběrnice založena na protokolu CIP (Common Industrial Protocol), stejně jako např. DeviceNET a ControlNET. Kromě stávajících specifikací CIP Motion pro řízení pohonů a CIP Sync pro synchronizaci, byla pracovní skupinou CIP Safety Special Interest Group asociace ODVA (Open DeviceNET Vendor Association) v roce 2005 představena specifikace CIP Safety. Ta rozšiřuje použití uvedených tří sběrnic pro použití v aplikacích s ohledem na funkční bezpečnost. Následně byl profil CIP Safety certifikován podle normy IEC 61508 pro použití v aplikacích s úrovní bezpečnosti až SIL 3. CIP Safety je možné kombinovat v jeden okamžik s ostatními specifikacemi CIP Motion a CIP Sync. V závislosti na zvolené sběrnici (EtherNET/IP, DeviceNET, ControlNET), je tedy možné vytvořit komunikační sběrnici nezávislou na fyzické vrstvě a integrovat v ní funkce pro standardní řízení, řízení pohybu, synchronizaci a bezpečnostní komunikaci. Při použití s EtherNET/IP je pak i velice snadné další propojení do podnikových a informačních sítí. Díky CIP protokolu je taky možné vzájemně propojovat všechny tři sběrnice a samozřejmě je také možný současný přenos standardních a bezpečnostních dat po těchto sběrnicích.
Specifikace CIP Safety spočívá v modifikaci protokolu CIP na úrovni aplikační vrstvy a to konkrétně v použití tzv. „Safety Validator“ objektu. Tento objekt je zodpovědný za správu CIP Safety spojení a slouží jako rozhranní mezi objekty bezpečnostní aplikace a linkovou vrstvou. Objekt „Safety Validator“ zajišťuje integritu přenosu bezpečnostních dat.



Obr. 13.10 Komunikační model s CIP Safety profilem (upraveno z [10]).

Protokol CIP Safety neslouží k úplnému potlačení komunikačních chyb, ale zajišťuje integritu přenosu bezpečnostních dat tím, že použitím speciálních mechanismů dokáže detekovat poruchy a umožňuje zařízením na sběrnici provádět patřičná opatření pro uvedení systému do bezpečného stavu. Za detekci komunikačních poruch je zodpovědný objekt „Safety Validator“. V následující tabulce jsou zobrazeny možné příčiny komunikačních chyb a metod objektu „Safety Validator“.

Tab. 13.2 Potencionální chyby v komunikaci s CIP Safety a metody jejich detekce.

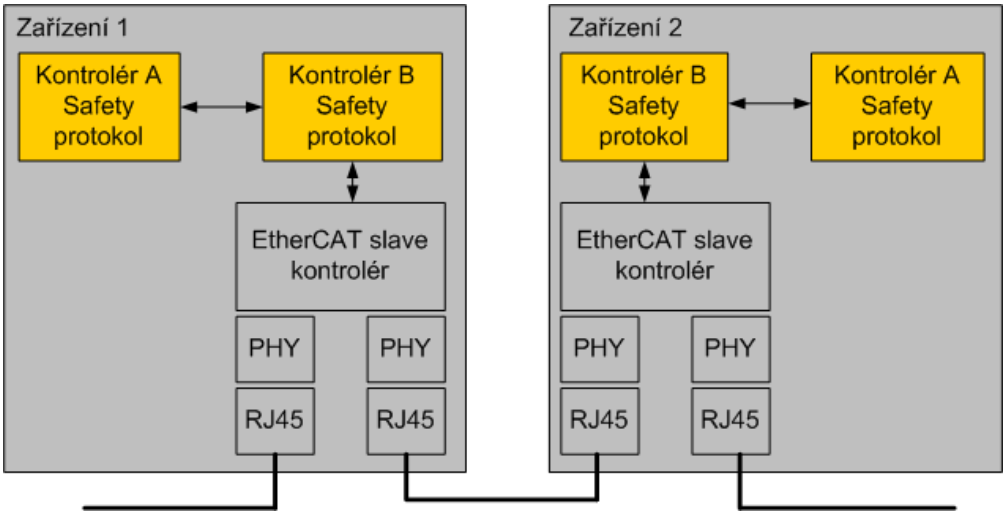
Opatření / Chyba	**Časová značka**	**Identifikace odesilatele a příjemce**	**Bezpečnostní CRC**	**Redundance s kontrolou překřížení**	**Rozdílná opatření pro standardní a safety data**
opakování	●		●		
ztráta dat	●		●		
vsunutí	●	●	●		
nesprávné pořadí	●		●		
poškození dat			●	●	
zpoždění	●				
spřažení mezi safety daty (Maskarade)		●			
spřažení standardních a safety dat (Maskarade)	●	●	●	●	●
chyba paměti síťového prvku (Switch)	●				

a) **Časová značka** – Producent a konzument koordinují svou komunikaci pomocí tzv. „Ping request“ a „Ping Responce“. Po navázání spojení mezi producentem vystaví producent „Ping Request“ a konzument odpoví hodnotou svého vnitřního časovače. Konzument si od získané hodnoty odečte hodnotu vlastního čítače (která uběhla od vystavení požadavku až do přijetí odpovědi) a vypočte tzv. offset. Ta je pak přidávána jako časová značka ke každé zasílané zprávě. Konzument si po každé přijaté zprávě odečte od časové značky hodnotu svého vlastního čítače, a je-li výsledek větší než povolené minimum, vystaví se porucha zpoždění a systém se patřičnými mechanizmy uvede do bezpečného stavu. Tento princip se používá u více komunikačních modelů.

b) **Identifikace odesilatele a příjemce** – Přenášená data obsahují jako doplňující informace jedinečné identifikátory zdroje a cíle dat, které se pak navzájem porovnávají. Je tedy vyloučena nepovolená komunikace mezi účastníky na síti, stejně jako „útok“ na síť z neoprávněného zdroje.
c) **Bezpečnostní CRC** – Modifikované CRC pro bezpečnostní účely charakteristické specifickým polynomem nebo délkou, či daty, přes která se vypočítává.
d) **Redundance s kontrolou překřížení** – Používá se jak redundance dat, tak i CRC s překřížením. Zvyšuje se tak tzv. Hammingova vzdálenost, což je minimální počet binárních pozic, na kterých došlo ke změně (chyb), při kterém už nemusí být možné poruchu detekovat či opravit. Při přenosu redundantních dat je tak možné opravit více chyb, ale zvyšuje se tak zároveň datový tok. Redundance dat se používá zvláště v případě přenosu relativně velkých bloků dat (cca 250 byte), naopak pro menší objemy dat se používá redundantní křížený CRC pro zvýšení integrity přenášených dat.
e) **Rozdílná opatření pro Standardní a Safety data** – CIP Safety protokol a jeho bezpečnostní mechanismy se používají výhradně pro safety-related data. To umožňuje zamezit chybě typu „Maskarade“ mezi datovými rámci standardních a safety zařízení na síti. [10]

13.5. Safety over EtherCAT

Sběrnice EtherCAT popsaná v kap. 10.4 našla díky svým nesporným výhodám (RealTime) uplatnění v řadě aplikací a stává se stále oblíbenější o rozšířenější. Proto se dalo očekávat, že i pro tuto sběrnici bude snaha vytvořit komunikační profil pro použití v safety-orientovaných aplikacích. Brzy po rozšíření sběrnice EtherCAT tak byla sdružením ETG (EtherCAT Technology Group) představena specifikace „Safety over EtherCAT“ (FSoE) a v roce 2010 byla standardizována mezinárodní normou IEC 61784-3-12 (FSCP 12). FSoE byl certifikován podle normy IEC 61508 pro použití v aplikacích s úrovní integrity bezpečnosti až SIL 3. Jedná se opět o bezpečnostní profil sběrnice založený na „Black Channel“ principu, takže je opět možné současný přenos bezpečnostních a standardních dat. Navíc díky tomuto obecnému přístupu je možné tento profil teoreticky použít i na jiných sběrnicích ethernetového typu a to i pro bezdrátovou komunikaci. Organizace ETG nedávno také rozšířila FSoE o speciální funkce pro bezpečné řízení pohonů na sběrnici EtherCAT pod označením „Safety Drive Profile“. Kombinace těchto tří základních kamenů moderní automatizace – Standardní RT komunikace, funkční bezpečnost a řízení pohonů - z této sběrnice tvoří ideálního kandidáta na vedoucí pozici v žebříčku sběrnic pro náročné průmyslové aplikace.
Tento profil nijak neomezuje délku přenášených rámců, přičemž je možné přenášet i velmi krátké rámce. Mechanismy pro detekci poruch na sběrnici jsou v podstatě obdobné jako u výše popsaných sběrnic (CRC kontrolní součet, sekvenční číslování, unikátní slave adresy apod.). Nicméně existují některá specifika odpovídající EtheCATové sběrnici. Například pro detekci zpoždění, vkládání, ztrátu dat apod. založenému na použití watchdog časovače, není použita hierarchie „Producent - Konzument“ ale “Master - Slave“, kde je možné přímo identifikovat a lokalizovat místo poruchy. Co se týče HW architektury, každé slave zařízení obsahuje dva nezávislé procesory, vyhodnocující bezpečnostní komunikaci nezávisle na sobě kontrolující svojí činnost. [11]



Obr. 13.11 Princip komunikace s profilem Safety Over EtherCAT (upraveno z [12]).

13.6. Další bezpečnostní komunikační sběrnice

Bezpečnostní komunikační sběrnice (profily) uvedené v předchozích kapitolách jsou pouze výběrem těch nejrozšířenějších a nejpoužívanějších. Jelikož se funkční bezpečnost stává stále důležitějším a sledovanějším aspektem průmyslové automatizace, bylo vyvinuto velké množství dalších komunikačních sběrnic nebo komunikačních profilů. Stěžejní část tvoří ty, které jsou dnes specifikovány mezinárodní normou IEC 61784-3, nicméně není to pravidlem. Výjimkou je zcela určitě profil ASIsafe pro sběrnici AS-i. Mezi komunikační sběrnice s možností použití v aplikacích pro zajištění funkční bezpečnosti, definované normou IEC 61784-3 a zde dosud nezmíněné patří např.:

- IEC/ČSN EN 61784-3-1: Foundation Fieldbus™ SIS (FSCP 1/1).
- IEC/ČSN EN 61784-3-6: INTERBUS™ Safety (FSCP 6/7).
- IEC/ČSN EN 61784-3-8: CC-Link™ Safety (FSCP 8/1).
- IEC/ČSN EN 61784-3-14: EPA Safety (FSCP 14/1).
- IEC/ČSN EN 61784-3-18: SafetyNET p™ (FSCP 18/1).

Nicméně existují další bezpečnostní profily pro sběrnice, které jsou standardizovány normou IEC 61158 - Průmyslové komunikační sítě – Specifikace sběrnice pole, ze které vychází struktura normy IEC 61784. U bezpečnostních profilů těchto sběrnic se dá očekávat, že se objeví v některé z dalších edic uvedené normy. Jedná se především o Modbus TCP/IP Safety a SERCOS III Safety.
Možností jak implementovat do Modbus TCP/IP sběrnice safety vrstvu je použití již zmíněné technologie openSafety vyvinutou společností B&R. V současné době je také známa i technologie pro zajištění funkční bezpečnosti na bázi sběrnice Modbus od společnosti HIMA. Tato společnost se problematikou funkční bezpečnosti v průmyslové automatizaci (procesní, strojní) zabývá již poměrně dlouho a detailně.
Pro ethernetovou realtime sběrnici SERCOS III (SErial Realtime COmmunications System) původně vyvinutou převážně pro řízení pohonů je už také dnes vyvinut bezpečnostní profil na bázi řešení openSAFETY od společnosti B&R nebo na bázi protokolu CIP safety. U těchto dvou sběrnic lze tedy očekávat, že se brzy standardizují a začnou postupně rozšiřovat, jelikož už teď jejich standardní varianty zabírají neopomenutelný podíl ve spektru průmyslové komunikace.

Další sběrnice, které nejsou standardizované normou IEC 61158 a mají svůj bezpečnostní profil je už výše zmíněná ASIsafe a dále pak také velice rozšířená sběrnice CANopen profilem CANopen Safety.

CANopen Safety profil byl vyvinutý organizací CiA (CAN in Automation) jako specifikace s označením CiA 304. Tato společnost publikovala dokument pod označením DSP 304 V1.0 (CANopen Framework for Safety-related Communication). Tento dokument nedefinuje nějaký specifický profil pro safety orientovaná zařízení, nicméně umožňuje implementaci bezpečnostních vlastností společně s libovolným profilem CANopen zařízení. Hlavním účelem dokumentu DSP 304 je, aby zavedl dodatečné komunikační objekty SRDO (Safety-Related data object), společně s klasickými CANopen komunikačními objekty PDO (Process Data Object) a SDO (Service Data Object). Dalšími bezpečnostními sběrnicemi jsou například „Safeethernet a „EsaLAN“. Safeethernet byla vyvinuta už před více než deseti lety společností HIMA a to nezávisle, prioritně pro jejich vlastní aplikace a není tedy možné si ji plést s bezpečnostní sběrnicí Ethernet/IP safety, založeném na CIP safety. Řešení safeethernet je nicméně také založeno na standardu ethernetové technologie (IEEE 802.3).
EsaLAN (Elan Safety Local Area Network) je otevřené sběrnicové řešení na bázi sběrnice CAN, které bylo na rozdíl od většiny ostatních vyvinuto výhradně pro úlohy v oblasti zajištění funkční bezpečnosti. Systém je sestaven z centrální řídicí jednotky nebo přímým propojením decentralizovaných ukončovacích jednotek a propojovací stanice mezi nimi. Komerční senzory a akční členy mohou být ke sběrnici připojeny prostřednictvím krátké „připínací“ linky. EsaLAN je sběrnice typu multi-master.
Naprostým specifikem jsou pak sběrnice pro speciální použití, jako jsou dopravní a drážní systémy, nebo systémy s požadavkem na bezdrátový přenos, o kterých bude řeč v následující kapitole.

Shrnutí pojmů

S rozvojem aplikací s ohledem na funkční bezpečnost se také dále vyvíjejí bezpečnostní komunikační sběrnice. V současné době existují bezpečnostní komunikační profily pro většinu nejrozšířenějších standardních komunikačních sběrnic. Profil, který zažívá v současnosti velký úspěch je **openSafety** vyvinutý organizací **EPSG** původně pro **Ethernet Powerlink**. Nyní je však možné jej použít i pro **EthernetIP, Modbus TCP, SERCOS III a Profinet**. To je dáno univerzálním **„Black Channel“** princip pro ethernetově založené sběrnice. Dalším rozšířeným profilem je **PROFIsafe** pro sběrnice **Profinet a Profibus** od společnosti Siemens. Obdobně univerzální jako **openSafety** je i profil **CIPsafety** pro sběrnice **Ethernet/IP, ControlNET a DeviceNET**. Bezpečnostní komunikační profil pod označením **„Safety over EtherCAT“** byl také vyvinut i pro realtime sběrnici **EtherCAT**. Všechny uvedené profily jsou standardizovány normou **IEC 61784-3** a specifikovány porůzné sběrnice. V této normě však nejsou uvedeny všechna používaná bezpečnostní komunikační řešení, jako je velice rozšířený profil **ASIsafe** nebo **CANopen Safety**.

Otázky

1. Co je principem řešení bezpečné komunikace pro sběrnice EPL, Ethernet/IP, SERCOS III a Profinet?

2. Jakou funkci má Safety Monitor ve sběrnici ASIsafe?
3. Jaký bezpečnostní profil je možné použít pro sběrnice Ethernet/IP, DeviceNET a ControlNET?
4. Jaké jsou další, méně rozšířené, bezpečné profily pro komunikační sběrnice?

Použitá literatura a další zdroje

1. openSAFETY – how it works, [online], [cit. 15-12-2010] http://www.open-safety.com/index.php?id=19
2. Introduction openSAFETY, [online], [cit. 15-12-2010] http://www.ixxat.com/ethernet_powerlink_safety_intro_en.html
3. Ethernet Powerlink – sériový přeborník v desetiboji, AUTOMA, 2008, číslo 02. ISSN 1210-9592.
4. PI International, PROFIsafe – System Description, 2007, Germany, [online], [cit. 15-12-2010] http://www.sci-eng.mmu.ac.uk/ascent/literature/documents/C01_PROFIsafe_System_Description_4342_Jul07.pdf
5. Žižka, I., Bezpečnost s Distributed Safety, 2009, [online], [cit. 15-12-2010] http://www.siemens.cz/siemjetstorage/files/59605_TIABezpecnost$s$Distributed$Safety.pdf
6. Štohl,R., Fiedler, P., Dubjel, R., Bezpečnostní systém AS-Interface Safety at Work (část 1), Automa, č.07, 2007, str FCC Public, Praha, [online], [cit. 15-12-2010] http://www.odbornecasopisy.cz/index.php?id_document=34334
7. Štohl,R., Fiedler, P., Dubjel, R., Bezpečnostní systém AS-Interface Safety at Work (část 2), Automa, č.10, 2007, str FCC Public, Praha, [online], [cit. 15-12-2010] http://www.odbornecasopisy.cz/index.php?id_document=34208
8. AS-interface Česká republika, AS-interface Safety At Work – Představení technologie Safety At Work, Seminář Safety At Work, Brno, 2005, [online], [cit. 15-12-2010] http://www.as-interface.cz/Seminar/ASI_Safety_at_Work.pdf
9. Siemens AG, AS-Interface Safety Monitor – Operating Instructions, ed. 2008, Germany, [online], [cit. 15-12-2010] http://www.sea.siemens.com/us/internet-dms/ia/ControlProducts/IEC-OEMControlComponents/docs_Brochures/ASiSafetyMon_HardwareManual_09.pdf
10. David A. Vasko, Suresh R. Nair, CIP Safety: Safety Networking for the Future,2003, [online], [cit. 15-12-2010] http://www.ab.com/networks/ethernet/get/CIPSafetyWhitePaper.pdf
11. Safety over EtherCAT, [online], [cit. 15-12-2010] http://www.ethercat.org/pdf/english/pcc0107_safety_over_ethercat_e.pdf

Řešená úloha 13.1

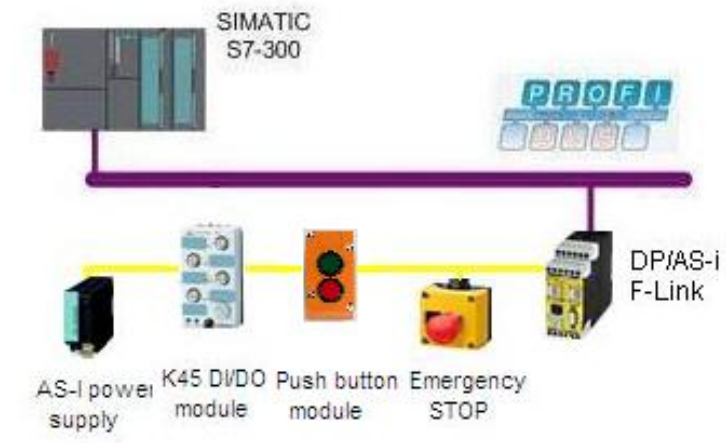
Řešená úloha popisuje tvorbu demonstrační aplikace distribuovaného bezpečnostního ŘS založeného na bezpečnostních prvcích firmy Siemens.

Úloha řeší propojení bezpečnostního PLC prostřednictvím sběrnice Profibus-DP s komunikační bránou DP/AS-i F-link, a tedy se sběrnicí AS-i. Na této sběrnici jsou připojeny další bezpečnostní prvky pro průmyslovou automatizaci komunikující s ŘS pomoci protokolu AS-i Safe. Převodník

DP/AS-i F-Link slouží jako komunikační rozhraní mezi průmyslovými sítěmi AS-interface (profil ASIsafe) a Profibus-DP (profil Profisafe). Použitý procesor PLC umožňuje také komunikaci po síti Ethernet.

Schéma struktury řídicího systému

Tak jak bylo popsáno výše, základní struktura celého ŘS se skládá ze vzájemně propojených komunikačních sběrnic Profibus -DP a AS-i. Ty jsou připojeny k centrálnímu PLC zajišťující celou komunikaci a procesní řízení. Na sběrnici AS-i jsou pak umístěny bezpečnostní prvky (ne výhradně) nejnižší procesní úrovně. Na sběrnici Profibus -DP pak mohou být připojeny další prvky, jako jsou necentrální periferie apod.



Obr. 13.12 - Schéma struktury ŘS.

Prvky řídicího systému

- SIMATIC CPU 315F-2PN/DP
- DP/AS-i F-Link - Převodník DP/AS-i F-Link slouží jako komunikační rozhraní mezi průmyslovými sítěmi AS-interface (profil ASIsafe) a Profibus (profil Profisafe). Shromažďuje signály binárních bezpečnostních senzorů na nejnižší úrovni pyramidy řízení, které komunikují v bezpečnostním profilu ASIsafe a předává je nadřazené úrovni komunikující v profilu Profisafe. Kromě toho je plnohodnotnou jednotkou master splňující požadavky specifikace AS-interface verze 3.0 s obousměrným přenosem standardních binárních i analogových hodnot. Díky integraci do systému SIMATIC Step 7 může uživatel projektovat v profilu bezpečnostní komunikace ASIsafe. Toto zařízení v sobě sdružuje AS-i Master (spec. 3.0) a bezpečnostní monitor pro převod bezpečnostních signálu ze vstupu AS-i do protokolu PROFIsafe. V této konfiguraci byl použit DP/AS-i F-Link s objednacím číslem (3RK3141-1CD1) a na síti Profibus-DP mu byla přidělena adresa 1.
- Bezpečnostní tlačítko Emergency STOP - bezpečnostní tlačítko sloužící k nouzovému zastavení jakéhokoli systému (podle jeho programem dané funkce). Umožňuje jednoduché připojení a odpojení od sběrnice AS-i. Poskytuje krytí IP20, ale existují i s krytím IP 65/IP 67. V této konfiguraci bylo použito tlačítko s označením 3SB3 s objednacím číslem (3SF5 811 0AX08) a na síti AS-i mu byla přidělena adresa 3.
- Bezpečnostní v/v modul K45F - kompaktní modul K45F ASIsafe má dvakrát více bezpečnostních vstupů než jeho předchozí provedení, které jsou umístěny ve stejném krytu. Díky tomu mohou být připojeny dva bezpečnostní senzory v kategorii 4/SIL 3, jako např. dva vypínače nouzového zastavení nebo dva polohové spínače. Tím se snižují náklady a šetří místo v zařízení. Tyto moduly nabízí krytí IP 20 nebo až IP 65/IP 67. Bezpečnosti v/v modul který podle konfigurace umožňuje následující zapojení - 2 bezpečnostní vstupy v

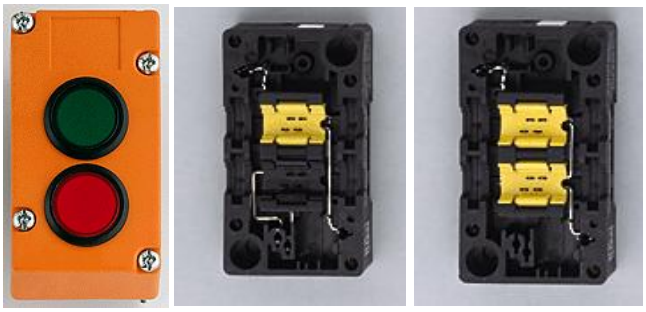
kategorii 4 dle EN 954-1 nebo SIL3 podle IEC 61508, 4 bezpečnostní vstupy v kategorii 2 dle EN 954-1 nebo SIL1 podle IEC 61508, 2 bezpečnostní vstupy a 2 standardní výstupy (napájení přes AS-i nebo externím zdrojem 24 VDC). V této konfiguraci byl použit modul s objednacím číslem (3RK1 405-1BQ20-0AA3) a na síti AS-i mu byla přidělena adresa 1.

- Tlačítkový spínač AC2018 - jedná se o aktivní prvek dvou podsvětlených tlačítek od společnosti IFM Electronic, který je přímo připojen na sběrnici AS-i . Skládá se ze dvou částí: spodní modulový díl (AC5000 nebo AC 5003) a horní díl AC2018. Montáž modulových dílu se provádí na montážní lištu a zadní stěnu modulu. Modulové díly mohou být buď pro jeden kabel AS-i s externím napájením (AC5003) nebo dva AS-i kabely (AC5000). Horní funkční moduly pak určují konkrétní funkci celku. Tlačítka nabízí ochranu proti neúmyslnému doteku. V této konfiguraci byl použit modul AC2018 a na síti AS-i mu byla přidělena adresa 2.
- AS-i Napájecí zdroj - napájecí zdroj sběrnice AS-i slouží k napájení sběrnice. Generuje vysoce stabilní stejnosměrné napětí o hodnotě 30 VDC bez zbytkového zvlnění. Proudové zatížení od 3 do 8 A, krytí IP20, detekce zkratu apod.

Obr. 13.13 - DP/AS-i F-Link.

Obr. 13.14 - bezpečnostní tlačítko Emergency STOP.

Obr. 13.15 - Bezpečností modul vstupů a výstupů K45F.



Obr. 13.16 - a) tlačítkový spínač AC2018, b) modulový díl AC5000 a c) AC 5003.

Obr. 13.17 - Napájecí zdroj AS-i.

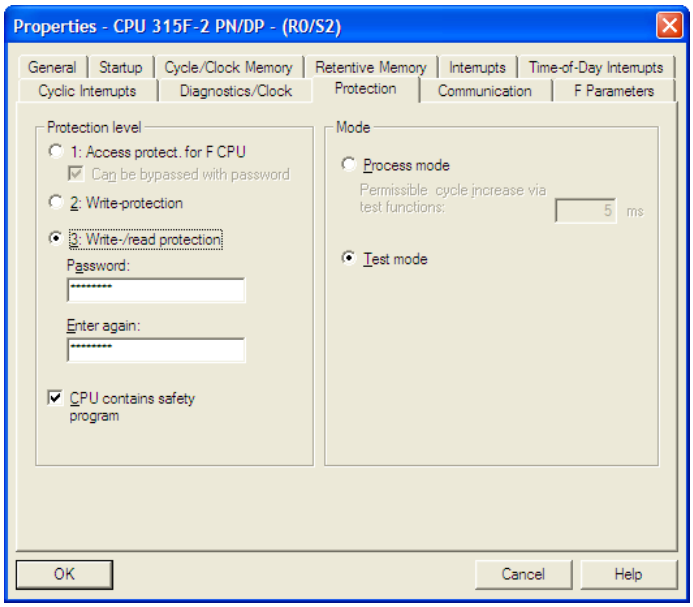
HW konfigurace PLC

Celá aplikace ŘS je vytvořena ve vývojovém prostředí STEP7. Nejprve je nutno vytvořit HW konfiguraci, která je pak nahrána do PLC. V okně aplikace HW konfigurace se na pracovní plochu vloží rack a do první pozice se pak umístí napájecí zdroj PS 307/5A a příslušný typ CPU (315F-2PN/DP). Při jeho vložení je uživatel vyzván ke konfiguraci průmyslové sběrnice Profibus-DP a Ethernet (zadání IP adresy apod.)

Obr. 13.18 – Výsledná fyzická konfigurace PLC s bezpečnostními prvky..

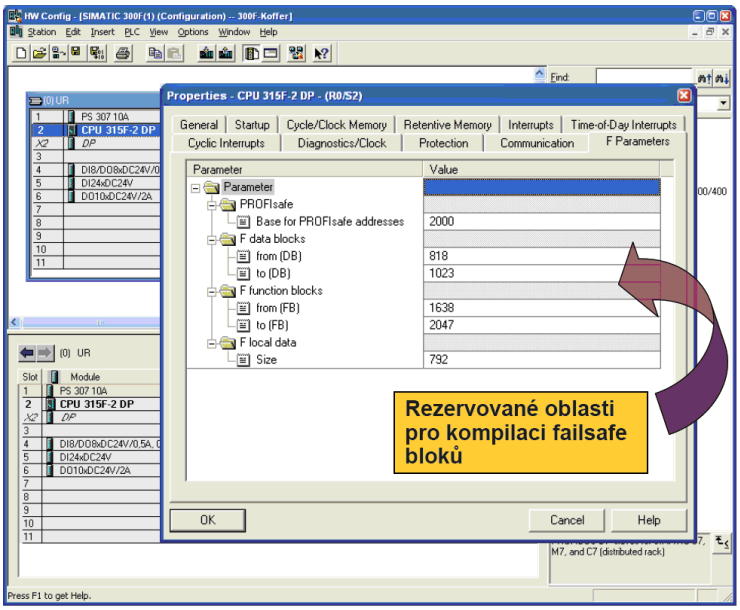
Základní kroky pro vytvoření hardwarové konfigurace jsou stejné, jako pro vytvoření hardwarové konfigurace pro standardní moduly. Je nezbytně nutné mít nainstalován doplňující SW balík S7 Distributed Safety (je dostupný zdarma ke stažení na stránkách výrobce), protože jinak v hardwarovém katalogu nejsou k dispozici bezpečnostní moduly. Kliknutím pravým tlačítkem myši na daný typ bezpečnostního CPU a výběrem „Object Properties“ se zobrazí následující okno (Obr. 9), kde je v záložce Protection nutné nastavit heslo, které chrání program v CPU před možností změny programu bez vědomí programátora. Pro jednoduchost bylo v tomto případě zvoleno heslo: „0000“. Toto je také důležitá vlastnost, patřící k programu zajišťující funkční

bezpečnost. Je také bezpodmínečně nutné zaškrtnout check-box CPU contains safety program, jestliže PLC bude obsahovat safety program. Jinak nebudou naprogramované bezpečnostní funkce vyhodnocovány. V hardwarové konfiguraci se musí také nastavit interval cyklického přerušování, který musí být shodný s nastavením v obr. 13.19. Tento čas je odhadnut a plně stačí na simulaci otevření dveří. Pro přesné nastavení slouží tabulka, ve které je zaznamenán potřebný čas na vykonání příslušných safety funkcí a funkčních bloků s přihlédnutím na typ hardwaru.



Obr. 13.19 - Dialogové okno vlastností F-CPU.

Další poměrně důležitou vlastností je záložka F-Parametres, kde se nastavuje Profisafe adresa a oblasti pro kompilaci failsafe bloku, jak je zobrazeno na Obr. 13.20.



Obr. 13.20 - Rezervované oblasti pro kompilaci failsafe bloků.

SM334 analog input/output module

Sestavu bezpečnostního PLC nemusí vždy nutně obsahovat pouze moduly bezpečnostní. Proto je v hardwarové sestavě také vložena standardní karta analogových vstupů a výstupů. Karta analogových vstupů/výstupů je umístěna do 4 slotu racku 0. Tato karta nese výrobní označení: 6ES7334-0CE01-0AA0 a má následující vlastnosti:

- 4 vstupy v jedné skupině a 2 výstupy v jedné skupině.
- Rozlišení 8 bitů.
- Programovatelný vstupní rozsah pro každý kanál zvlášť (napěťový/proudový).

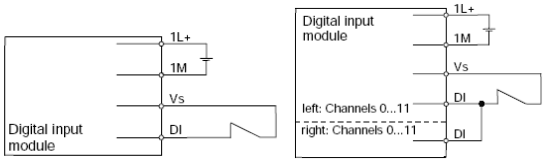
Safety Protector

Za standardními moduly se musí pro přechod na bezpečnostní moduly umístit Safety Protector 6ES7 195-7KF00-0XA0. Safety protector chrání bezpečnostní moduly před přepětím, které by mohlo způsobit chybu. Neobsahuje adresu, nepožaduje diagnostické zprávy, a proto se nemusí vkládat do žádného slotu v racku ve STEP7.

SM326F digital input module – Safety Integrated

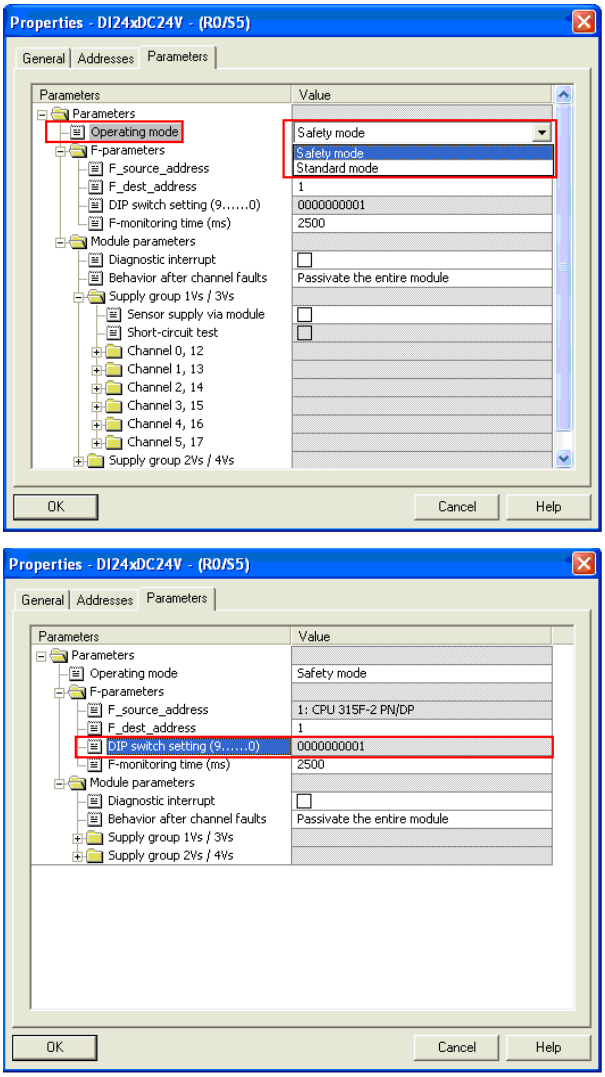
Jak bylo uvedeno výše, tento modul digitálních vstupů i každý další modul na síti tvořenou z bezpečnostních prvků musí mít jednoznačnou PROFIsafe adresu. PROFIsafe adresa se nastavuje na DIP přepínačích, které jsou umístěny na spodní straně modulu digitálních vstupů. Je nutné také správně zohlednit zapojení snímačů na tento modul digitálních vstupů s přihlédnutím k požadované bezpečnostní kategorii. Tento modul digitálních vstupů může být používán ve standardním režimu nebo v bezpečnostním režimu. Na Obr. 13.21a) je zobrazeno připojení v bezpečnostním módu, kde jeden snímač je připojen na jeden kanál tj. 1oo1. Tímto zapojením je možné využívat až 24DI. Na Obr. 13.21 b) je zobrazen příklad zapojení snímače, který je připojen na jeden kanál na dva protilehlé vstupy. Tato konfigurace odpovídá zapojení 1oo2. Při tomto zapojení můžete využívat až 12 kanálů. Napájecí napětí pro snímače je možné odebírat přímo z modulu digitálních vstupů a výstupů. Modul digitálních vstupů SM326F je vložen do slotu 5 racku 0 a má následující vlastnosti:

- 24 vstupů, izolovaných ve skupinách po 12.
- 24VDC napájecí vstupní napětí.
- Možné externí napájení snímačů.
- Group error display (SF).
- Safe mode display (SAFE).
- Status indikátor pro každý kanál (zelená LED).
- Konfigurace v Run (CiR) – možné ve standardním módu.
- Diagnostika alarmu s přiřazením parametrů.
- Nastavitelný mód – standardní, bezpečnostní.
- Konfigurovatelná možnost 1oo1 nebo 1oo2 pro každý kanál.
- Jednoduché PROFIsafe přiřazení adres.

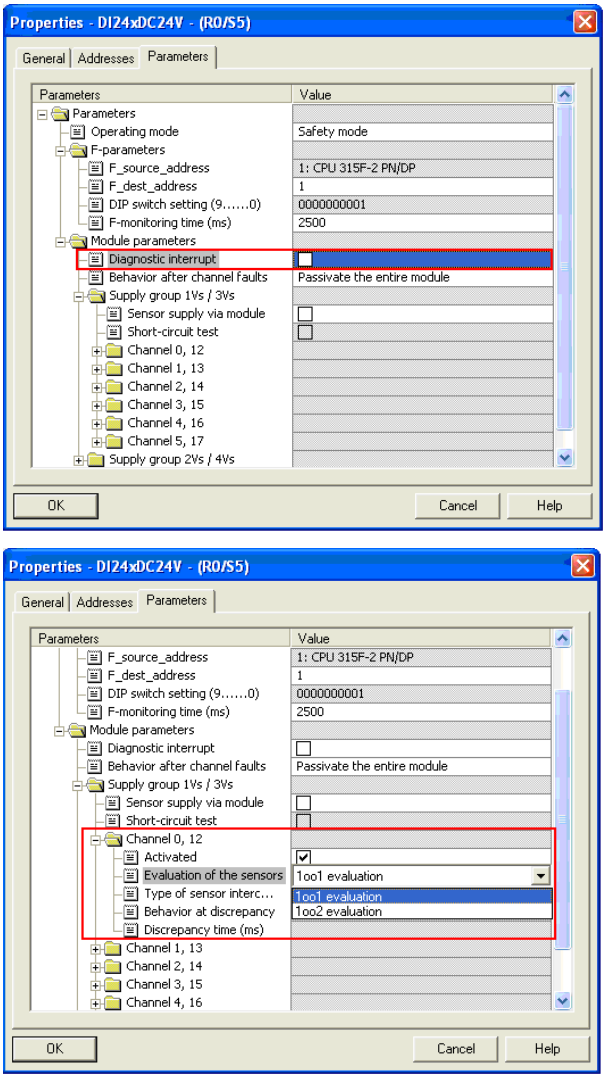


Obr. 13.21 – a) Připojení snímače 1oo1, b) a) Připojení snímače 1oo2.

Digitální modul SM326F je nutné nakonfigurovat ve STEP7. Kliknutím pravým tlačítkem myši na digitální modul SM326F a výběru Object Properties se zobrazí následující Obr. 13.22a). V prvním kroku se zvolí, jestli je modul používám jako standardní nebo bezpečnostní v záložce F-Parameters. Druhým krokem je nastavení adresy modulu digitálních vstupů Obr. 13.22b). Dalším krokem aktivace nebo deaktivace diagnostického přerušení Obr. 13.23a). Posledním krokem je nastavení typu připojení jednotlivých kanálů Obr. 13.23b).



Obr. 13.22 a) Nastavení stand. nebo bezp. módu, b) Nastavení adresy modulu.



Obr. 13.23 a) Nastavení diagnostického přerušení b) Nastavení jednotlivých kanálů.

SM326F digital output module – Safety Integrated

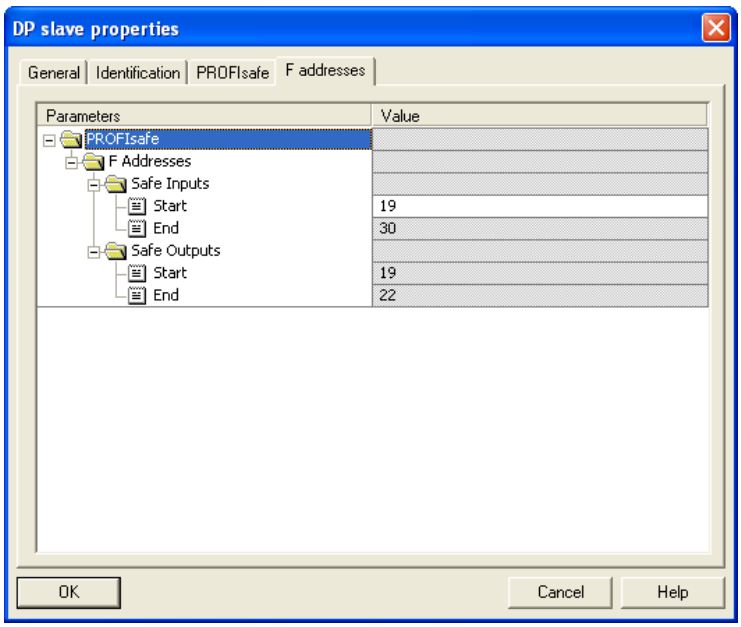
I tento modul digitálních výstupů i každý další modul na síti tvořenou z bezpečnostních prvků musí mít jednoznačnou PROFIsafe adresu. PROFIsafe adresa se nastavuje na DIP přepínačích. DIP přepínače najdete na spodní straně modulu digitálních výstupů. Připojení akčního členu podléhá jednak také příslušné bezpečnostní kategorii a také jestli je např. možné jedním digitálním výstupem spínat dvě relé. Modul digitálních výstupů SM326F s výrobním označením (6ES7 326-2BF40-0AB0) je vložen do slotu 6 racku 0 a má následující vlastnosti:

- 8 výstupů, izolovaných jako dvě skupiny po 4.
- P-M přepínač (polarita source/sink).
- Výstupní proud 2A.
- 24VDC napájecí vstupní napětí.
- Vhodný pro solenoidové ventily, světelné indikátory.
- Group error display (SF).
- Safe mode display (SAFE).
- Status indikátor pro každý kanál (zelená LED).

- Diagnostika alarmu s přiřazením parametrů.
- Může být použit v bezpečnostním režimu.

Převodník DP/AS-i F-Link

Pro konfiguraci tohoto převodníku mezi sběrnicemi Profibus-DP a AS-i musí být ve vlastnostech CPU nejprve nakonfigurována sběrnice Profibus -DP. To provedeme dvojím poklikáním na položku MPI/DP ve slotu X1 v racku 0. Zde se vybere typ sběrnice (Profibus) a definuje se adresa CPU na této sběrnici a také další vlastnosti jako je přenosová rychlost apod. Po tomto kroku je možné na sběrnici vložit přetažením z knihovny DP/AS-i F-Link. Je však nutné mít předem nainstalovaný balíček Object Manager OM F-Link for STEP 7. Jedná se o balíček určený pro snadnější práci s DP/AS-i F-Linkem v prostředí HW konfigurace STEP 7. Po instalaci tohoto balíčku je možné tento převodník najít v knihovně: Profibus DP/DP/AS-i/ DP/AS-i F-Link/ RK3141-1CD10, kde se vybere správný typ a verze zařízení. Zde je použit RK3141-1CD10 v1.0. Dvojím poklikáním na tento blok se otevře okno parametrizace, které je zobrazeno na Obr. 13.24. Zde se v záložce „General“ nastaví Profibus adresa a v záložce F-addresses počáteční adresy bezpečnostních vstupů a výstupů modulů připojených na sběrnici AS-i.

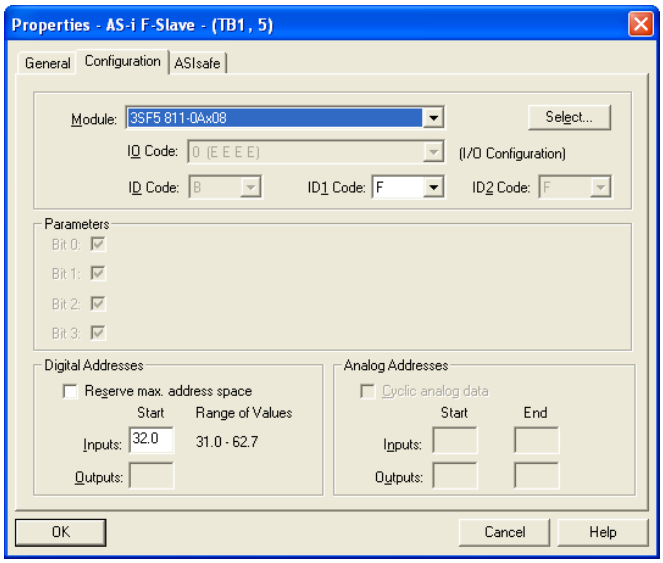


Obr. 13.24 - DP/AS-i F-Link.

Po označení tohoto převodníku lze již do něj (do spodního okna – viz Obr. 13.26) vkládat jednotlivá zařízení (slave, F-slave), která jsou fyzicky přítomna na sběrnici AS-i z knihovny: Profibus DP/DP/AS-i/ DP/AS-i F-Link/ RK3141-1CD10/V1.0. Pozor, bezpečnostní zařízení na sběrnici AS-i zabírají plnou adresu sítě, tedy A i B a lze jich na síť proto vložit jen 31, standardních slave potom při rozšířené adresací více. Nesmíme zapomenout, že slave zařízení musí být vkládána do takových pozic/adres, které odpovídají jednotlivým specifickým adresám, které má v sobě každé zařízení uloženo. Pro tento případ je to adresa1 pro modul K45F, adresa 2 pro standardní tlačítkový modul a adresa 3 pro tlačítko Emergency STOP.

Po jejich vložení stačí již na každý z nich poklikat a otevře se okno jeho parametrizace (Obr. 13.25), kde se v oblasti Module vybere přesný typ slave zařízení na sběrnici podle jeho výrobního označení.Tímto se již přednastaví všechny jeho parametry určující jeho význam a funkci na sběrnici AS-i jako je I/O kód (určuje počet a kombinaci v/v na zařízení), ID kód (základní+rozšířený, jednoznačně definuje funkci zařízení), digitální a analogové adresy apod. Pokud není podle výrobního označení, zařízení v seznamu přítomno, lze vybrat „univerzální typ“ a parametrizovat jej

ručně. To se týká především zařízení jiných výrobců než Siemens. Což je případ zde použitého tlačítkového modulu od společnosti Ifm. Použití tohoto modulu zde také dokazuje, že je možné na jednu sběrnici AS-i připojovat jednak standardní, tak i bezpečnostní zařízení. Na Obr. 13.26 je zobrazena výsledná HW konfigurace celého distribuovaného bezpečnostního ŘS.



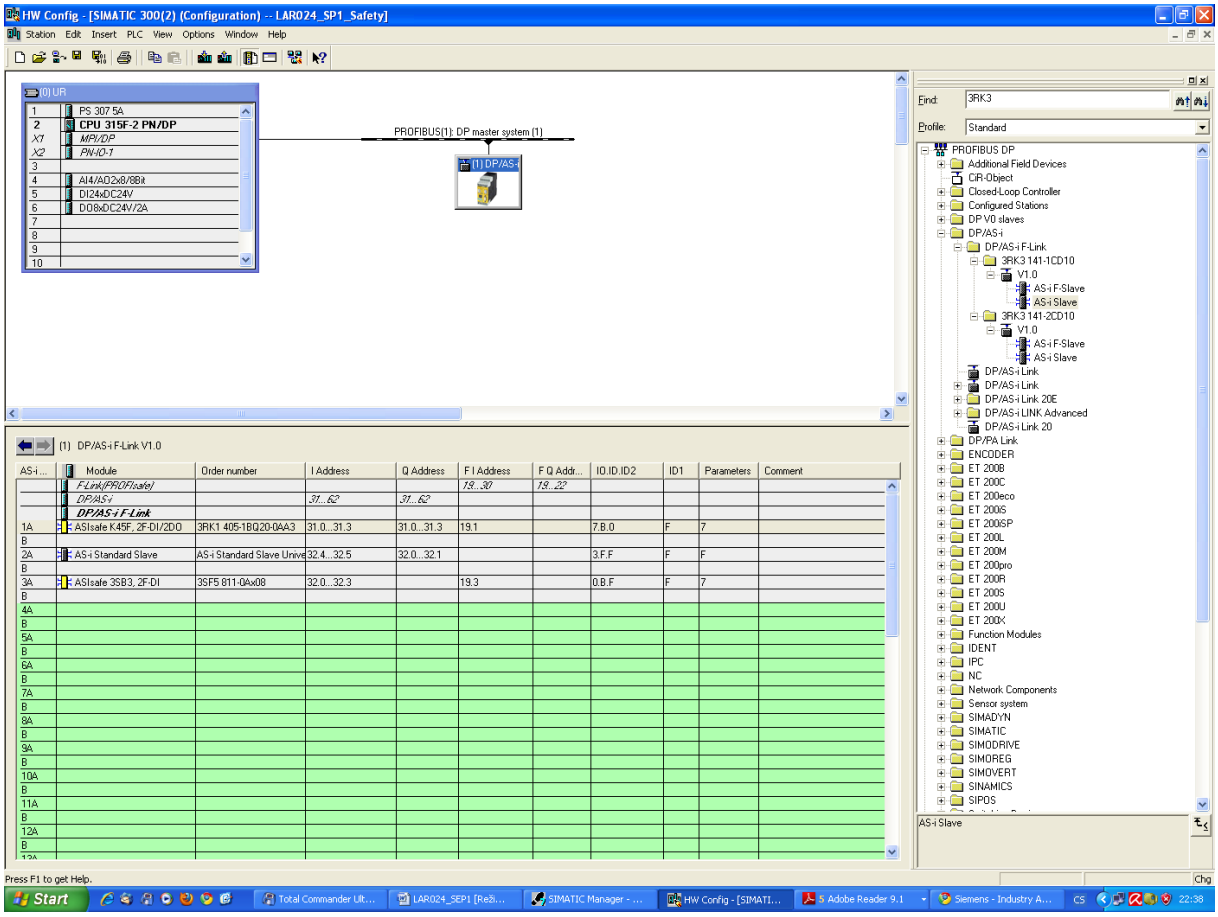
Obr. 13.25 - Parametrizační okno slave zařízení na sběrnici AS-i.

Popis bezpečnostní řídicí aplikace PLC

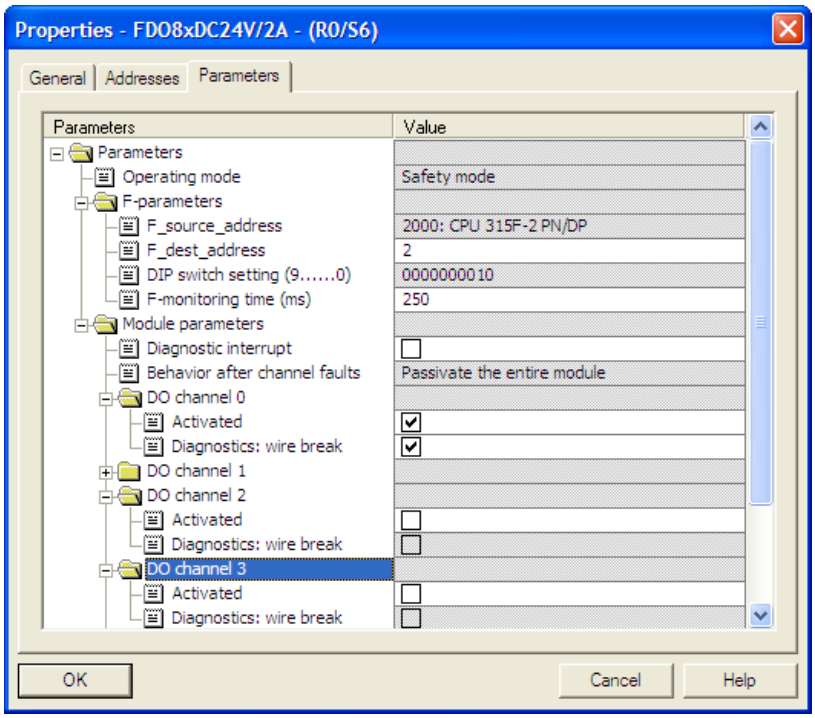
Pro názornou demonstraci možnosti využití výše popsané konfigurace ŘS pro zajištění funkční bezpečnosti byl zvolen fiktivní proces řízení trojfázového asynchronního motoru/ventilátoru umístěného v kleci pro zajištění bezpečnosti před úrazem obsluhy nebo vstupem pevných těles. Otevření této klece je vyhodnocováno snímačem, který je připojen na 2 bezpečnostní vstupy AS-i modulu. Toto zapojení zajišťuje dílčí funkční bezpečnost kategorie 4 podle normy EN 954-1 / SIL3 podle normy IEC 62061 nebo PLe podle nové normy EN ISO 13849-1.

Modul F-DI umístěný na PLC nebude v této konkrétní aplikaci využit v bezpečnostním módu, ale jen ve standardním módu využívající jeden kanál pro zajištění určité zpětné vazby o sepnutí stykačů. Na jeden vstup tohoto modulu pracujícím ve standardním módu bude tedy připojen pomocný signalizační kontakt stykačů, který díky svému mech. spřažení indikuje jejich sepnutí.

Na modulu F-DO umístěném na PLC bude v této konkrétní aplikaci využit pouze jeden kanál, který bude spínat 2 kontakty stykačů motoru. Proto je vhodné ostatní kanály deaktivovat a nastavit parametry tohoto modulu podle následujícího Obr. 13.27. Musí být aktivován bezpečnostní mód, nastavená správná Profisafe adresa, parametr F-monitoring time musí být nastaven na vyšší hodnotu než je volací perioda OB35, která je v tomto případě 200ms. Je aktivován pouze jeden kanál a je zapnuta diagnostika přerušení kabelu.



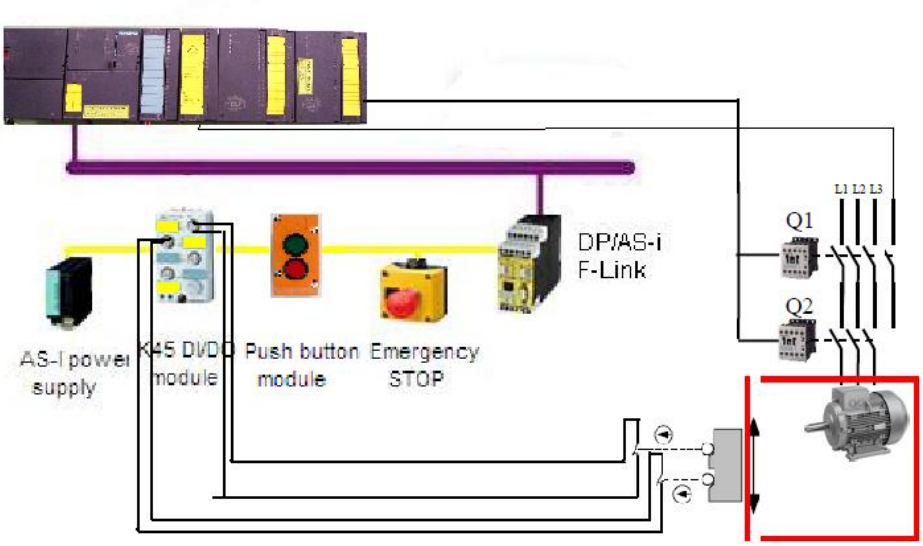
Obr. 13.26 - HW konfigurace celého distribuovaného bezpečnostního ŘS.



Obr. 13.27 - Dialogové okno parametrizace F-DO modulu.

Výsledná funkce systému je následující. Motor v kleci se startuje zeleným tlačítkem standardího AS-i modulu. Chod motoru je signalizován zeleným světlem. Stroj běží nepřetržitě, dokud nedojde

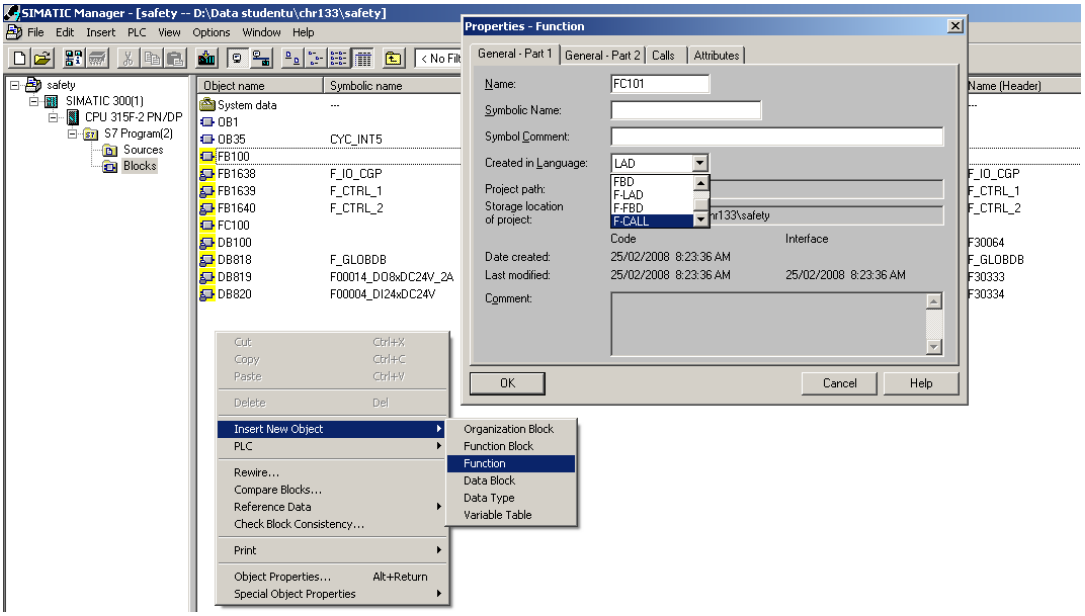
k jeho vypnutí tlačítkem Emergency Stop, nebo pokud nejsou otevřeny dveře klece. Pak dojde k zastavení motoru a jeho opětovné spuštění je možné až po rozepnutí „Emergency Stop“, zavření bezpečnostní klece a kvitaci poruchy červeným tlačítkem na standardním AS-i slave modulu. „Násilné“ zastavení systému je signalizováno také červeným světlem na standardním AS-i modulu. Výsledné zapojení je zobrazeno na následujícím Obr. 13.28.



Obr. 13.28 - Výsledné zapojení celého systému

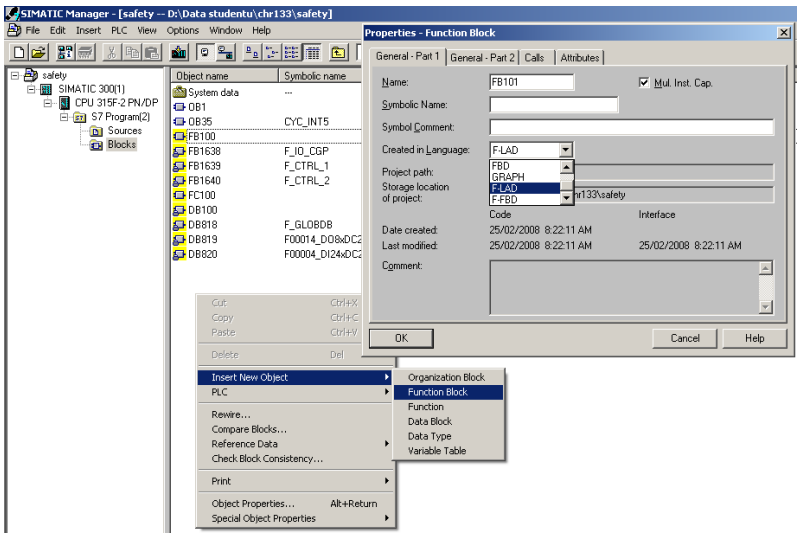
Vytvoření základní struktury safety programu

Celý postup vytvoření bezpečnostní aplikace spočívá ve vytvoření funkce F-CALL. Tak se vytvoří F-runtime skupina. Kliknutím pravým tlačítkem myši a výběrem v menu Insert New Object → Function se vloží funkce. Dále je nutné tuto novou funkci specifikovat, že se jedná o funkci tvořící F-runtime skupinu, jak ukazuje Obr. 13.29.

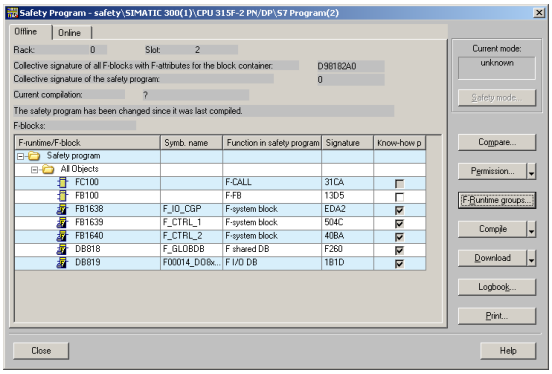


Obr. 13.29 - Definice nové funkce jako F-CALL.

F-runtime skupina obsahuje failsafe funkční bloky (safe funkce a v ní vnořené F-FB) plnící safety funkce. Dalším krokem je vložení F-FB do F-CALL. Opět kliknutím pravým tlačítkem myši a výběrem Insert New Object → Function Block se vloží funkční blok. Vyvolá se okno podle Obr. 13.30, kde se musí specifikovat, v jakém jazyce bude uživatel programovat. Musí být vybrán buď jazyk LAD– F-LAD nebo FBD F-FBD. Funkční blok F-FB 1 musí být volán z funkce F-FC1 a funkce F-FC1 musí být cyklicky volána z organizačního bloku OB35. Spuštění editace safety programu se vyvolá příkazem v menu Options→Edit safety program (Obr. 13.31).

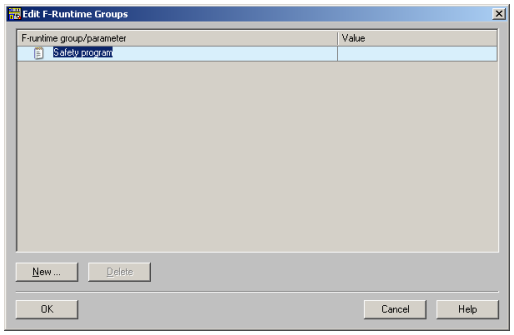


Obr. 13.30 - Vytvoření funkčního bloku, volba jazyka.

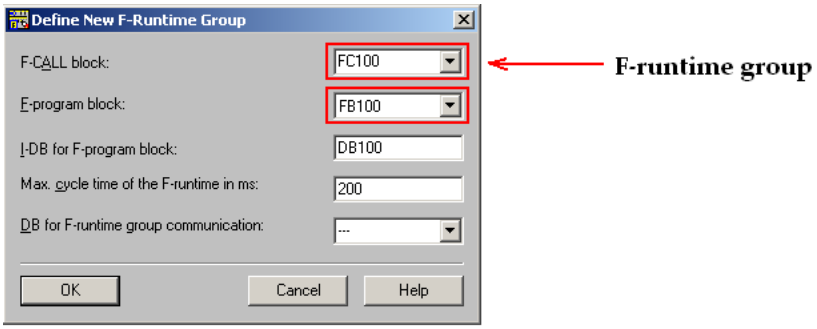


Obr. 13.31 - Safety program.

Kliknutím na tlačítko F-Runtime groups se vytvoří hierarchie volání jednotlivých F-runtime bloků a jejich F-FB. Nejprve budete vyzváni k vložení nového hesla a jejího potvrzení např. heslo „0000“. Nová F-runtime skupina se vytvoří klinutím na tlačítko New… (Obr. 13.32). Zobrazí se dialogové okno, ve kterém se musí specifikovat F-CALL block: tj. v našem případě F-FC1. Dále se musí do F-CALL umístit funkční blok F-FB1 a pro funkční blok se vytvoří instanční datový blok DB1. Kliknutím na tlačítko OK bude přijat požadavek na vytvoření struktury volání Obr. 13.33.

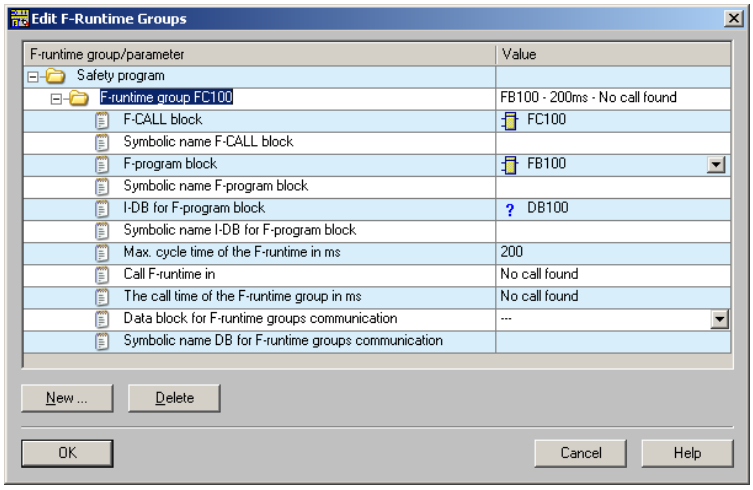


Obr. 13.32 - Editace F-runtime skupin.



Obr. 13.33 - Definice nové F-Runtime skupiny.

Kliknutím na tlačítko OK podle Obr. 13.34 se provede generování funkčních bloků. Program vyzve uživatele pro potvrzení, že je nutné vytvořit chybějící bloky - instanční datový blok pro F-FB1.



Obr. 13.34 - Výsledek vytvoření F-Runtime skupiny.

Safety program

Do funkčního bloku F-FB1 se musí vkládat jen certifikované F-FB a tím vytvářet safety program. Safety funkční bloky se vkládají technikou Drag&Drop do programu z knihovny Libraries → Distributed Safety → F-Application Blocks.

Tímto stylem je možné např. vložit funkční blok FB219, který slouží pro odkvitování všech poruch najednou, které se mohou např. vyskytnout na kanálu safety modulu apod. Bližší informace a popis funkčních bloků je uveden v nápovědě po stisku tlačítka F1. K funkčnímu bloku je samozřejmě nutné vytvořit jeho vlastní instanční datový blok např. DB219.

Popis požadované bezpečnostní funkce pro řízení motoru uzavřeného v bezpečnostní kleci byl již popsán výše. Zde budou již pouze popsány jednotlivé bezpečnostní funkce reprezentované F-FB a

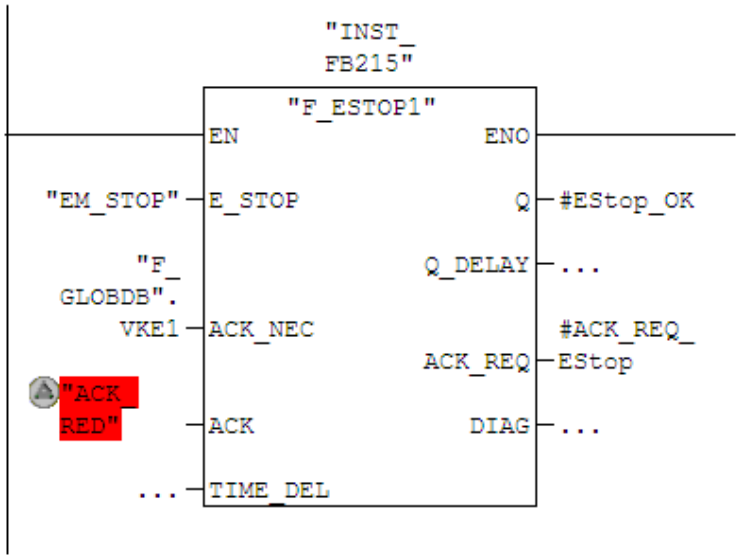
celkové chování bezpečného systému. Monitorování polohy dveří je nejčastější realizací na různých strojích, aby v případě otevření dveří obsluhou nemohla být obsluha zraněna od např. rotujících částí stroje apod. Stejně tak bezpečnostní tlačítko „Emergency STOP“ je nedílnou součástí téměř většiny průmyslových procesů, využívajících pohyblivé komponenty strojů, a které jsou řešeny s ohledem na zajištění patřičné úrovně funkční bezpečnosti. Níže popisovaný program je celý obsažen v F-FB1.

Network 1:

Tento FB215 s knihovny „Distribuated safety“ slouží pro vyhodnocování tlačítka „Emergency STOP“ a potvrzování po jeho stisknutí a uvolnění. Logickým signálem „1“ na vstupu ACK_NEC je signalizováno, že je vyžadováno manuální potvrzení k nastavení výstupu Q do log. 1. Bit "F_GLODB".VKE1 na vstupu ACK_NEC tohoto FB je statická proměnná s přednastavenou hodnotou log. 1. Je tedy vyžadováno potvrzení také po restartu systému. Samotná kvitace (potvrzení) je přivedeno na vstup ACK

Výstup Q (#EStop_OK) je nastaven do log. 1, teprve když E_STOP je v log 1 (rozepnuto) a bylo stisknuto potvrzovací tlačítko jako odezva na jeho stisknutí. Pomocí výstupu ACK_REQ (#ACK_REQ_EStop), je signalizováno, že je požadováno uživatelské potvrzení na vstupu ACK (po stisknutí tl. EMERGENCY STOP).

```
Network 1: Title:
Vyhodnocení tlačítka Emergency Stop, kvitace se provadi cervenym tlacitkem na
stand. slave
```



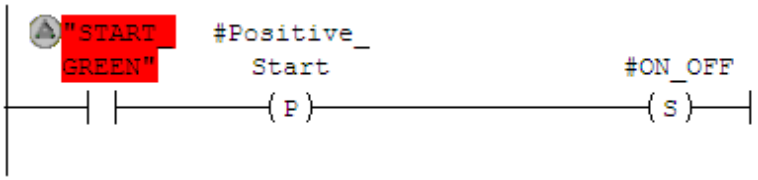
Network 2:

Tento network testuje náběžnou hranu zeleného tlačítka na stand AS-i modulu a pak nastavuje do log. 1 lokální proměnou pro spuštění motoru.

POZOR: Pro předávání informací v safety programu smí být použity pouze lokální proměnné, protože není dovoleno ze safety programu zapisovat a číst informace v uživatelské datové paměti.

Network 2: Title:

```
Náběžnou hranou zeleneho tlačítka START na stand. slave se setuje příznak,
ktery
startuje motor, za patřičnych podminek
```

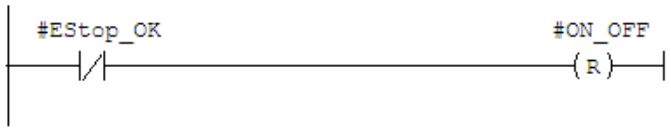


Network 3:

Tento network resetuje proměnnou pro start motoru, pokud je sepnuto tlačítko EM. STOP, nebo není kvitováno jeho předchozí stisknutí

Network 3: F_: F_Global_Data Block

```
Pokud je stisknuto tlacitko Em. Stop nebo neni po rozepnuti kvitovano, resetuje
se priznak pro spusteni motoru
```



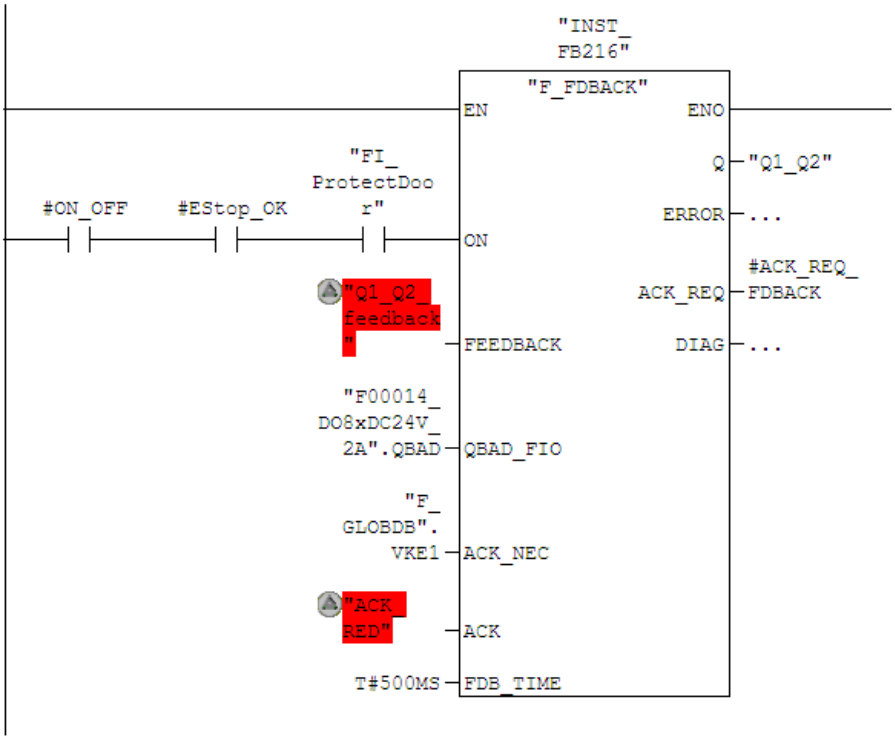
Network 4:

Tento network slouží k monitorování zpětné vazby v safety programu pomocí F-FB 216. Tento F-FB sleduje stav výstupu a na vstupu informaci o tomto výstupu (sepnutí stykačů). Chyba je signalizována na výstupu ERROR, pokud dojde prodlení mezi vstupem a výstupem delším než je nastavený parametr FDB_TIME. Vstupy ACK_NEC a ACK mají obdobnou funkci jako u bezp. tlačítka. Parametr QBAD_FIO pak sleduje případnou chybu samotného modulu. Výstup Q ("Q1_Q2") bloku FB216 pakliže je vstup ON v log. 1. To je splněno, pokud ve stejný okamžik platí:

- FEEDBACK="1" (DI snimajici stav stykače)
- Žádný read-back error
- #EStop_OK =1
- ON/OFF =1 (normal switching duty)
- Protective Door" =1 (bezp. vstup z AS-i modulu, ochranné dveře klece zavřeny)

Network 4: Title:

```
Fb pro sepnuti stykace motoru za podminek: 1. je pozadavek na start, 2. neni
Total stop a je kvitace, 3. jsou zavreny dvere od klece, 4. neni chyba modulu
pro vyhodnoceni zavreni klece
```



Network 5:

Tento network pouze sleduje a signalizuje chod motoru (sepnutí stykače), rozsvícení zelené signálky na stand. AS-i slave modulu.

Network 5: signalka na START tlacitku stand. (sviti=motor jede)

```
Pokud je sepnut stykac(motor bezi), sviti zelene tlacitko
```

Network 6:

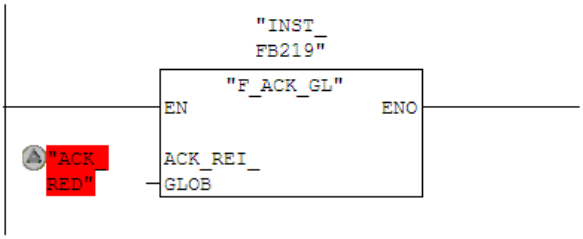
Tento network pouze sleduje a signalizuje požadavek na kvitaci od Em. STOP, nebo od ZV. Pak rozsvítí červenou signálku na stand. AS-i modulu.

```
Network 6: signalka na kvit tlacitku stand slave (sviti=nekvitovano a nelze
pokud je pozadavek na kvitaci od tlacitka nebo ZV sviti cervene kvitovaci
tlacitko (sviti=nekvitovano a nelze spustit)
```

Network 7:

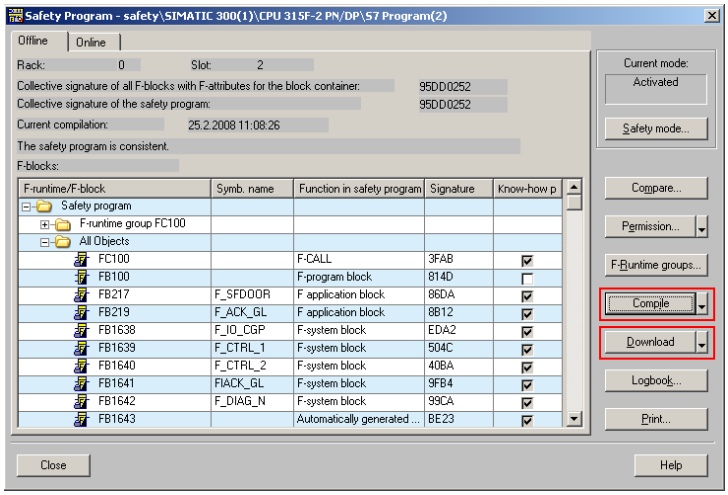
Bezpečnostní FB219 v tomto network slouží pro celkovou reintegraci. To znamená, že generuje potvrzení pro simultánní reintegraci všech bezpečných I/O kanálu bezpečných I/O F-runtime skupiny po komunikačních chybách nebo po chybách bezpečných I/O nebo I/O kanálů

```
Network 7 : Title:
Po kvitaci cervenym tlacitkem na stand modulu (toto pak zhasne), se vola FB pro
reintegraci vsech failsafe IO
```



Kompilace programu, zápis do bezpečnostního PLC

Před kompilací programu je nutné zavřít veškerá otevřená okna. Kompilace se provádí v editoru safety programu kliknutím na tlačítko Compile (Obr. 13.35). Po úspěšném výsledku kompilace, která se zobrazí na konci kompilace, se může přistoupit k zápisu programu do PLC.



Obr. 13.35 - Kompilace a zápis programu do PLC.

Běh programu v programovatelném automatu se musí ukončit přepnutím přepínače režimu automatu do režimu STOP nejlépe přímo na PLC. Následně se musí nastavit komunikace s PLC (MPI nebo přes Ethernet). Kliknutím na tlačítko Download (Obr. 13.35) bude program zapsán do PLC. Uživatel může být vyzván pro zápis hesla při downloadu programu do PLC. Monitorování výše uvedeného programu je možné např. pomocí VAT tabulky, kde se vloží příslušné proměnné

DVD-ROM

Řešený příklad naleznete na DVD:\CVICENI13\

14. BEZDRÁTOVÉ KOMUNIKAČNÍ SBĚRNICE A JEJICH VZTAH K FUNKČNÍ BEZPEČNOSTI

Čas ke studiu: 3 hodiny

Cíl Po prostudování tohoto odstavce budete umět

- Vyjmenovat základní výhody a nevýhody bezdrátové komunikace.
- Popsat problematiku bezdrátové komunikace.
- Popsat základní principy některých bezdrátových technologií v průmyslu.

Výklad

Vzájemná komunikace mezi stroji, jejich komponenty, řídicími systémy a periferiemi (senzory a akční členy) je dnes většinou realizována díky komunikačním sběrnicím s metalickou nebo optickou fyzickou vrstvou. Jejich vývoj a rozšíření znamenal obrovský skok od stavu, kdy byla veškerá komunikace řešena přístupem: centralizované drátové spojení bod-bod. Avšak i zavedení komunikačních sběrnic neumožňuje vyřešit všechny aplikační problémy. Jedná se například o mechanické pohyblivé systémy, nebo rozlohou velké systémy, na nichž je umístěna mnohdy rozsáhlá senzorika, popřípadě akční členy. Obecně u stroje, technologie a zařízení kde je klasické kabelové spojení nemožné, značně složité, nespolehlivé nebo nákladné. Jako příklad můžeme uvést portálové manipulátory, robotické paže, různé rotující součásti jako jsou soustruhy, mlýny, míchačky apod. U takovýchto technologií se přenos dat realizuje většinou různými sběrnými kartáči, kroužky, kluznými kontakty, pohyblivými kabelovými konzolami apod. Je proto velice obtížné spolehlivě přenášet data, jelikož takovéto komunikační spojení mezi pohyblivými částmi strojů a soustrojí jsou častokrát velice nespolehlivé, opotřebovávají se a jsou zdrojem rušení a výpadků. Další problémy se mohou vyskytovat u zařízení, kde se sice nevyskytují žádné pohyblivé části, nicméně specifické konstrukční řešení stroje nedovoluje použití standardní drátové sběrnice. Nejen technické problémy však byly důvodem vývoje a aplikace bezdrátových sběrnic. Svůj podíl na tom mají i ekonomické aspekty, jelikož zaváděním bezdrátových sběrnic se snižují náklady na kabeláž, kabelové trasy a úpravy technického řešení celé technologie za účelem vyřešení problémů konektivity.

Zde nastupuje možnost aplikace bezdrátových komunikačních sběrnic (sítí). Jejich principy vycházejí převážně z již komerčně používaných bezdrátových technologií (informační a multimediální technika), a to buď částečně nebo úplně (Wi-Fi, Bluetooth,…). Jejich aplikace v komerčním sektoru však nevyžadují takové nároky na spolehlivost, dostupnost a odolnost jako jejich průmyslové ekvivalenty. Nicméně jsou známé i průmyslové bezdrátové sběrnice, které zcela vycházejí ze svých výhradně průmyslových drátových variant. V průmyslových aplikacích je v souvislosti s použitím bezdrátových sběrnic často diskutován problém elektromagnetické kompatibility. Zdrojem EMI v průmyslových aplikacích mohou být především frekvenční měniče nebo vysoké spínané výkony. Ve skutečnosti se u tohoto druhu EMI jedná o frekvence rušení v řádech kHz, kdežto bezdrátová komunikace probíhá v řádech GHz (Wi-Fi). Dosud byla řeč o poměrně rychlé bezdrátové komunikaci pro kontinuální sběr a přenos dat. Nicméně v průmyslových aplikacích se používají i odlišná bezdrátová řešení jako je ZigBee, IrDa, RFID, nebo mobilní a rádiové sítě. Aplikace využívající tyto bezdrátové spojení buď nevyžadují kontinuální spojení (GSM, GPRS, RFID, …) nebo nepotřebují přenášet objemné data. V prvém případě se jedná

dálkovou správu procesů a technologií, čili jednoduchou diagnostiku, či povelování (GSM,GPRS, EDGE, UMTS, HSPA, rádiové sítě). Ve druhém případě se pak jedná o identifikační systémy a jednoduché přístroje, ze kterých se vyčítají různé identifikační údaje, nebo se jednoduše parametrizují pomocí bezdrátových technologií jako je IrDa, RFID a ZigBee.
Jelikož je těchto bezdrátových technologií a jejich aplikací značné množství, budou v následujícím textu stručně popsány základní charakteristiky a aplikační použití některých z nich a následně bude uvedena možnost jejich použití v aplikacích s požadavkem na zajištění patřičné úrovně funkční bezpečnosti (safety-orientované aplikace).

14.1. Přehled běžných bezdrátových komunikačních technologií používaných v průmyslu

Wireless LAN

Pod zkratkou Wi-Fi (wireless-fidelity = bezdrátová věrnost) se skrývá bezdrátový komunikační standard několika verzí pod souhrnným označením IEEE 802.11. Původním určením bylo bezdrátové spojení přenosných zařízení do lokálních sítí WLAN (Wireless LAN), později se uplatnilo i pro bezdrátové připojení do rozsáhlejších sítí a sítě Internet. To je zaručeno především díky vzájemné kompatibilitě obou standardů IEEE 802.3 a IEEE 802.11. Wi-Fi rozhranní jsou dnes prakticky ve všech přenosných počítačích a stále častěji se objevují v mobilních telefonech (SmartPhone). Jako přenosové médium se využívá bezlicenčního pásma a to na frekvencích především 2,4 GHz a 5 GHz. Podle verze IEEE 802.11 (a,b,g,n) jsou definovány různé typy použitých modulací. Výhoda takto vysokých nosných frekvencí pro použití v průmyslu již byla zmíněna, nicméně nevýhodou je, díky bezlicenčnímu užití, dnes již značně zarušené přenosové frekvenční pásmo a nebezpečí neoprávněného přístupu k síti. Jako u všech bezdrátových sítí se jedná o otevřený komunikační protokol, takže je nutné patřičně zajistit bezpečnost (security) sítě. To platí tím spíše u průmyslových aplikací. K zabezpečení se používají různé šifrovací mechanismy (WEP, WPA, WPA2), kontrola MAC adres, blokování vysílání SSID (identifikační označení) apod. Použití této technologie v průmyslu (převážně specifikace IEEE 802.11a – 5 GHz) je především v provozech a aplikacích, kde je již klasická komunikace založena na ethernetových technologiích, jako je např. Profinet od společnosti Siemens. Ta má tuto technologii vyvinutou a aplikovanou v mnoha provozech již poměrně dlouhou dobu. [1]

Bluetooth

Mezi další velice oblíbenou bezdrátovou komerční komunikační technologii, která si postupem času nachází uplatnění i v průmyslu je i technologie Bluetooth. Ta byla původně vyvinuta za účelem komunikace mobilních zařízení, jakými jsou telefony, PDA, notebooky apod. Je definována standardem IEEE 802.15.1. Stejně jako Wi-Fi, využívá frekvence 2,4 GHz v bezlicenčním pásmu. Používá však metodu rozprostřeného spektra FHSS (Frequency Hopping Spread Spectrum), kdy je během jedné sekundy provedeno 1600 změn frekvence mezi 79 frekvencemi s rozestupem 1 MHz. Tato metoda tak zajišťuje odolnost proti EMI a umožňuje tak použití této technologie v průmyslových aplikacích. Pro standard Bluetooth je definováno několik výkonových úrovní: 2,5 mW, 10 mW, 100 mW. Těmto úrovním samozřejmě odpovídá i maximální komunikační dosah: 1 m, 10 m a 100m. To platí pro otevřený prostor, v uzavřených prostorách tento dosah často klesá. V průmyslových aplikacích je však potřeba zajištění dostatečného dosahu (i jako rezerva), což je zajišťováno dalším zvyšováním výkonu. Tím se však zvyšuje riziko rádiové interference, především s Wi-Fi, která pracuje na stejné frekvenci. Je proto nutné vhodně optimalizovat nejen výkon, ale i vyzařovací antény a celou rádiovou síť.

V průmyslu se Bluetooth používá pro bezdrátovou komunikaci s přístroji na větším počtu jednotlivých pracovišť, kde je třeba vytvořit mnoho nezávislých lokálních bezdrátových spojení. Této bezdrátové komunikaci se hodně věnuje společnost Phoenix Contact. Nedávno se však objevila i bezdrátová verze komunikačního protokolu Profibus-DP od společnosti Helmholtz využívající místo fyzické vrstvy bezdrátovou technologii Bluetooth. [2]

ZigBee

Obdobnou komunikační technologií jako je Bluetooth, je novější ZigBee. Je standardizována ve stejné skupině IEEE 802.15, konkrétně IEEE 802.15.4 a stejně tak slouží k propojování nízkovýkonových zařízení do sítě PAN (Personal Area Network) s dosahem do 75m. Byla vyvinuta na základě mnoha odůvodnění, proč nelze v průmyslových aplikacích použít technologii Bluetooth. Byla tedy vyvinuta výhradně se záměrem použití v průmyslových aplikacích. Pracuje opět v bezlicenčním pásmu, tentokrát však ve frekvenčním rozsahu přibližně 868 MHz, 902–928 MHz a 2,4 GHz při přenosové rychlosti 20, 40, 250 kbit/s. Jedná se o jednoduchou, flexibilní, odolnou technologii s nízkou spotřebou, vhodnou pro použití v aplikacích pro řízení budov (kontrola vytápění, ovládání žaluzií, zabezpečovací systémy apod.), ve zdravotnictví, spotřební elektronice, nebo jako komunikační rozhranní počítačových technologií. [3]

WiMAX

Jako doplněk pro bezdrátovou technologii Wi-Fi, která byla prvotně určena pro vnitřní použití byla vyvinuta další bezdrátová komunikační technologie pro použití výhradně venkovní - WiMAX (Worldwide Interoperability for Microwave Access). Takovéto vyhrazení dnes již ale příliš neplatí. Na trh byla uvedena v roce 2003 pod označením IEEE 802.16. Určitou dobu po uvedení technologie WiMAX se čekalo, že tato brzy nahradí Wi-Fi, či bude alespoň rovnoměrným konkurentem. Nestalo se tak především díky složité licenční politice. WiMAX se tak nestal následovníkem Wi-Fi ale jeho doplňkem. Jak již bylo řečeno, je určen pro venkovní použití s o mnoho vyšším dosahem než Wi-Fi. Řádově se jedná o desítky kilometrů čtverečních a více, s přenosovou rychlostí do 70 MB/s. Tato technologie se tak hodí pro metropolitní sítě (na celé město jen několik vysílačů), nebo naopak málo obydlené oblasti. Podle definice IEEE 802.16 je tato síť určena pro použití v licenčních i bezlicenčních frekvencích od 2 do 11 GHz. V České republice se však používá pouze licenční frekvence 3,5 GHz. To také možná brání jejímu širšímu použití. Do průmyslové automatizace tato technologie zatím moc nepronikla, a to i díky poměrně slabému rozšíření v komerčním sektoru. [4]

WISA

WISA (Wireless Interface for Sensors and Actuators) je bezdrátová komunikační technologie vyvinutá společností ABB a určená výhradně pro použití s jejími automatizačními komponentami. Pracuje v bezlicenčním pásmu 2,4 GHz s dosahem 5-10 m. Architektura bezdrátové komunikace je postavena na komunikačním modulu v konfiguraci PLC ABB a bezdrátových modulech V/V nebo přímo senzorů pro bezdrátovou komunikaci. Zvláštností je že umožňuje volitelné doplnění o moduly generující elektromagnetické pole pro bezdrátové napájení těchto senzorů s dosahem až 3x3 metry. [5]

WirelessHART

WirelessHart je další bezdrátová komunikační technologie určená výhradně pro průmyslové použití. Vychází ze svého předchůdce drátové sběrnice HART (Highway Addressabel Remote Transducer). Standardní drátová sběrnice je založena na klasické proudové smyčce, na které jsou ještě navíc namodulována digitální data. Komunikace je typu Master – Multi slave. V průmyslu se používá pro komunikaci nadřazeného řídicího systému (PLC) s různými inteligentními přístroji a senzory (field devices). Po jedné sběrnici se tak ve stejný okamžik přenášejí jak analogová data (teplota, tlak), tak i data digitální (různé meze vyhodnocené přístrojem, pulsně modulovaná analogová hodnota apod.) O další rozvoj sběrnice HART se stará HCF (HART Communication Foundation), která v roce 2008 představila veřejně dostupnou specifikaci HART 7.1 (WirelessHART) pod standardem IEC 62591. Žádná z předchozích bezdrátových technologií nedosáhla takového uznání na mezinárodní úrovni.

Komunikace opět probíhá v bezlicenčním ISM pásmu 2,4 GHz. Je zpětně kompatibilní se současnými HART instalacemi. Hierarchie komunikační sítě WirelessHART se skládá z jedné komunikační brány (Wireless Gateway) a několika zařízení (smart senzors apod.) pro komunikaci

po této síti. V současné době jsou k dispozici i WirelessHART Gateway do jiných průmyslových sběrnic jako je Profibus nebo MODBUS. [6]

IrDa

IrDa je poněkud specifická bezdrátová technologie založená na principu komunikace pomocí infračerveného světla. Byla vyvinuta konsorciem IrDa (Infrared Data Association) pro komunikaci přenosných zařízení na krátkou vzdálenost. Vysílačem jsou infračervené diody, které vysílají modulované záření (pulsní modulace) o vlnové délce 875 nm. Přijímačem jsou naopak fotodiody. Tato technologie, která bývá součástí mobilních telefonů, notebooků a jiných zařízení začíná být velice rychle vytlačována jinými technologiemi (Bluetooth), které nejsou degradovány základní nevýhodou IrDa, což je nutnost přímé viditelnosti vysílače a přijímače. Maximální dosah činí od 20cm do max. 1m, podle výkonu vysílače a okolních podmínkách (sekundární světelné emise). Komunikace je možná s max. přenosovou rychlostí 115 kb/s. Pro tuto bezdrátovou technologii bylo také vytvořeno hned několik komunikačních protokolů podle zamýšleného aplikačního užití. V průmyslové praxi se používá převážně pro komunikaci s různými mobilními terminály, pokladny, zdravotnická zařízení apod. [7]

RFID

Radio Frequency Identification (RFID), bezdrátová technologie původně vyvinutá k identifikaci zboží. Iniciátorem vývoje se stala americká obchodní společnost. Princip komunikace spočívá v periodickém vysílání impulsů do okolí čtečkou RFID čipů. Pokud se v její blízkosti objeví nějaký RFID čip, tak prostřednictvím své vlastní antény (fóliové) nabije svůj vnitřní kondenzátor pro získání energie a následně odešle zpět své identifikační údaje RFID snímači. Ten je pak přijme a předá dál k dalšímu zpracování. Tento princip se nazývá pasivní. Existují však i aktivní RFID čipy s vlastním napájením, které se používají k aktivní lokalizaci. Jsou však již dražší. Čipy využívají převážně nosnou frekvenci 125 kHz, 134 kHz a 13,56 MHz. V některých státech se dají používat i další frekvence jako 868 MHz (v Evropě) a 915 MHz (v Americe). Identifikační údaje jsou uloženy prostřednictvím 96-bitového čísla. To umožňuje přidělit 268 milionům výrobců produkujícím každý 16 milionů druhů výrobků (tříd) a v každé třídě je prostor pro 68 miliard sériových čísel. RFID technologie se dnes používá k identifikaci zboží, ale i jako přístupové systémy, nebo k identifikaci výrobků a jejich lokalizace v jednotlivých fázích výroby. [8]

GSM/GPRS

GSM (Globální Systém pro Mobilní komunikaci původně však francouzsky „Groupe Spécial Mobile“) je nejrozšířenější standard pro mobilní komunikaci na světě. Je provozován od roku 1991. GSM je vystavěna na tzv. buňkové síti, kdy se mobilní telefon připojuje do komunikační sítě prostřednictvím nejbližší buňky. Každá buňka pokrývá oblast podle svého výkonu, maximálně však okruh v dosahu 35 km. GSM síť pracuje na několika frekvencích (900,1800,1900 MHz, v některých zemích jiné). GSM síť, používající digitální komunikaci, bývá označována za síť druhé generace - 2G. První generací je označována technologie ještě s analogovým přenosem. GSM technologie využívá ke komunikaci tzv. kombinovaný multiplex FDMA/TDMA (Frequency Division Multiple Access / Time Division Multiple Access). Přenosová rychlost v GSM síti je max. 14,4 kbit/s (obousměrně). Funkce GSM sítí je rozdělena do tzv. služeb jako jsou hlasové hovory nebo SMS (Short Message Service).

V roce 1997 byla do GSM standardu doplněna modifikace pro paketový přenos dat. Jde o mobilní datovou službu v sítích GSM označovanou jako GPRS (General Packet Radio Service). Tato technologie je už označována jako 2,5 generace a umožňuje přenosovou rychlost dat až 57,6 kbit/s. Využívá paketově přepínaný provoz, což znamená, že více uživatelů může sdílet stejný přenosový kanál. Celá přenosová kapacita je v okamžik odesílání dat vyhrazena těm uživatelům, kteří zrovna posílají data. GPRS se využívá například pro čtení e-mailů, prohlížení webových stránek – tedy občasný či periodický přenos dat.

V průmyslových aplikacích se GSM/GPRS mobilní komunikace používá k monitoringu a řízení technologických zařízení na velké vzdálenost popř. na dálkovou správu, kdy je po předání technologie zákazníkovi dodavatelem poskytován ještě dodatečný servis v záruční či pozáruční

době. Tento servis či dálkový monitoring a řízení je pak při použití technologie GPRS možné provádět na velké vzdálenosti bez nutnosti přítomnosti technika v místě instalace technologie. Technologií GPRS je možné dosáhnout kontinuálního toku dat při nízké rychlosti s použitím tzv. GPRS datových modemů. SMS zprávy se využívají k jednoduché parametrizaci/řízení technologie, či jako krátký informační zdroj o stavu technologie a to na vyžádání nebo při výskytu určité události. Nevýhodou se může zdát fakt, že veškerá komunikace v sítích GSM je zpoplatněna operátorem sítě. Tento druh komunikace se z výše uvedených důvodu (spolehlivost, nízká přenosová rychlost, zpoplatnění) ale i z jiných důvodů nepoužívá pro přenos funkčně bezpečných dat v aplikacích pro zajištění funkční bezpečnosti. [9]

EDGE/EGPRS

EDGE (Enhanced Data rates for Global Evolution), nebo také Enhanced Data rates for GSM Evolution je dalším vývojovým stupněm v technologii GSM po zavedení datových přenosů pomocí GPRS. Tato technologie je už označována jako 2.75G (generace). Její vývoj byl založen na již dostupné GSM síti a díky svým vylepšením poskytuje především vyšší přenosovou rychlost. Toho je dosaženo použitím modulace s vyšším počtem stavů. Celková přenosová rychlost se tak teoreticky může blížit až 384 kbit/s. V praxi se však používá rychlost okolo 200kbit/s. Na rozdíl od konvenční technologie GSM, EDGE vyžaduje instalaci dodatečných technických prostředků v komunikační síti. EDGE síť tak není automaticky dostupná všude tam, kde je signál sítě GSM, nicméně její dostupnost se pořád rozšiřuje a v mobilních zařízeních je její dostupnost automaticky signalizována.
Stejně jako GSM síť nabízí datovou službu v podobě GPRS, EDGE síť obsahuje obdobnou implementaci s označením EGPRS (Enhanced GPRS). Ta je zpětně kompatibilní s GPRS. [9]

UMTS

Dalším vývojovým stupněm v mobilních komunikačních sítích je technologie UMTS (Universal Mobile Telecommunication System) označována již jako síť třetí generace (3G). Tato síť je koncipována jako nástupce technologie GSM a je standardizována organizací 3GPP jako evropský standard. Původní technické označení bylo odvozeno od použité přístupové metody W-CDMA (Wideband Code Division Multiple Access). Označení UMTS bylo zvoleno spíše z obchodních důvodů. Širokopásmová přístupová metoda W-CDMA (metoda kódové dělení), nepoužívá žádné časové dělení, ale všichni uživatelé používají přidělené frekvenční pásmo po celou dobu. Přístupová metoda W-CDMA může být dále také kombinována s TDMA a FDMA pro duplexní přenos pod označením UMTS FDD nebo UMTS TDD (UMTS Time/Frequency Division Duplex). Přenosové pásmo se skládá z jednoho párového pásma (1920 až 1980 MHz + 2110 až 2170 MHz) a jednoho nepárového pásma (1910 až 1920 MHz + 2010 až 2025 MHz). Nicméně zavedením technologií W-CDMA došlo k lepšímu využití frekvenčního pásma a tím pádem ke zvýšení přenosové rychlosti až na 2 Mbit/s. Technologie UMTS si opět vyžaduje určité úpravy technického vybavení komunikační GSM sítě. V současné době tak probíhá postupné zavádění UMTS sítě do stávající GSM sítě a zatím se nepočítá s variantou, že by v dohledné době úplně nahradila GSM síť.
UMTS definuje i protokoly pro Downlink a Uplink komunikaci pod označením HSPA (High-Speed Packet Access). HSPA se dále dělí na HSDPA a HSUPA (High-Speed Downlink/Uplink Packet Access). HSDPA bývá také označována jako síť 3.5G (generace) a HSUPA jako síť 3.75G (generace). Poslední specifikace komunikační sítě UMTS zvyšuje oproti původní verzi komunikační rychlost pro downlink až na 28.8 Mbit/s (HSDPA) a pro uplink až na 11.5 Mbit/s (HSUPA). [9]

GPS

Zkratka GPS (Global Positioning System) znamená globální polohový systém používaný k přesnému určení polohy a času kdekoli na Zemi (nebo i nad ní). Jedná se o satelitní navigační systém a tedy logicky opět o bezdrátový přenos informací. Je provozován Ministerstvem obrany Spojených států amerických. Princip funkce spočívá v přijímání signálů z několika družic umístěných na oběžné dráze Země. Na základě těchto přijímaných signálů je možné pomocí několika metod určit polohu přijímače s přesností na desítky až jednotky metrů. U speciálních

vojenských aplikací dokonce s přesností až na centimetry. Metody a přístupy pro určování polohy jsou poměrně složité a jejich podrobný popis by byl velice obsáhlý. Americký NAVSTAR GPS je v současnosti jediný plně funkční globální navigační satelitní systém (GNSS – Global Navigation Satellite System), nicméně vyvíjejí se i další jako např. evropský Galileo, ruský GLONASS, nebo čínský COMPASS. GPS se používá v řadě vojenských i komerčních aplikacích jako je automobilový průmysl, navigační systémy v mobilních telefonech apod. Každá družice mimo jiné také obsahuje atomové hodiny a vysílá tak přesný čas. Pro aplikace v průmyslu se používá převážně za účelem přesné synchronizace času, tedy ne k určování polohy ani ke komunikačním účelům (GPS přijímače jsou pasivní zařízení – pouze přijímají signál). Synchronizace času v průmyslových řídicích systémech (PLC) je velice důležitá k přesnému datování vzniklých událostí nebo nežádoucích stavů pro pozdější diagnostiku, nebo pro účely regulace a řízení závislé na přesném lokálním času.

DCF77

Pro synchronizaci času v průmyslových aplikacích se na území střední Evropy používá také velice oblíbený dlouhovlnný rádiový časový signál vysílány z vysílače v Mainflingenu (Německo – nedaleko Frankfurtu nad Mohanem). Tento vysílač pracuje na frekvenci 77,5 kHz a je proto nazýván DCF77. Vysílač má výkon 50 kW a dosah přibližně v okruhu 1500 – 2000 km. Jeho použití je tedy omezeno na tuto oblast střední Evropy. V komerčním sektoru se používá k synchronizaci času některých digitálních hodin, budíků, meteostanic apod. Nicméně existuje i řada automatizačních komponent různých výrobců využívající tuto metodu k synchronizaci času v různých průmyslových aplikacích.

14.2. Spolehlivost průmyslových bezdrátových technologií

V bezdrátových komunikačních sběrnicích oproti standardním nabývají velice na významu pojmy spolehlivost (reliability) a dostupnost (availibility). To je logicky dáno charakterem bezdrátového přenosu informací. Vzduch jako přenosové médium totiž automaticky vždy nezajišťuje komunikační spojení. Mezi komunikujícími účastníky se může vyskytnout překážka bránící šíření signálu, mohou se zhoršit povětrnostní podmínky ovlivňující šíření signálu prostředím, může nastat interference mezi několika bezdrátovými sítěmi, nebo se v důsledku mobility komunikujících komponent, tyto mohou dostat z dosahu některého účastníka. Proto je nutné i u standardních průmyslových komunikačních protokolů pro bezdrátové systémy vyvinout mechanismy a postupy pro zajištění co nejlepší spolehlivosti, a dostupnosti. A v případě ztráty komunikačního spojení podniknout takové kroky, aby byla technologie uvedena do bezpečného stavu. Ty mohou být obdobné jako u drátových sběrnic, kde může také dojít ke ztrátě komunikace vlivem porušení kabelu.

Dalším neopomenutelným faktem je bezpečnost bezdrátových sběrnic ve smyslu „Security“, jelikož bezdrátové sítě jsou otevřené komunikační systémy s rizikem neoprávněného přístupu k síti neautorizovaným účastníkem. Mezi tyto zásahy patří buď jen pasivní naslouchání, nebo mnohem nebezpečnější aktivní útok v podobě smazání důležitých dat, nebo naopak vložení nežádoucích dat či jiné útoky. Zajištění této bezpečnosti je realizováno prostřednictvím speciálních šifrovacích mechanismů, použitím přístupových certifikátů apod.

Spolehlivost v komunikaci je vyjádřena jako záruka že žádná data nebudou během přenosu poškozena (pozměněna), nebo ztracena a že všichni účastnící obdrží svá data v požadovaný okamžik (dobu). V průmyslové praxi je možné najít mnoho příkladů aplikací, v nichž je bezdrátová komunikace spolehlivější než komunikace prostřednictvím kabelových sítí. Nicméně pořád je řeč o spolehlivosti (reliability) bezdrátových komunikačních sítí a ne o jejich bezpečnosti (safety) nebo snad zabezpečení (security). Obě zmíněné problematiky jsou rozsáhlého charakteru. V další části textu budou proto zmíněny jen základní přístupy a příklady bezdrátové komunikace použité v systémech s ohledem na funkční bezpečnost (Functional Safety). [10]

14.3. Bezdrátové sběrnice v aplikacích pro zajištění funkční bezpečnosti

Bezdrátové technologie se rozšiřují také do aplikací orientovaných na funkční bezpečnost. Mnoho bezdrátových technologií používaných v průmyslu se použitým přístupem sériového přenosu dat určitým způsobem podobá klasickým sběrnicím s metalickým či optickým vedením. Ukázkovým příkladem je bezdrátový Ethernet WLAN, který je kompatibilní s jeho metalickou/optickou variantou. Proto z obecného hlediska je pravděpodobné, že rozšiřující bezpečnostní profily, které jsou používány v klasických ethernetových sběrnicích pro zajištění funkční bezpečnosti, lze aplikovat i na bezdrátovou sběrnici LAN. Jelikož i samotný ethernet v aplikační vrstvě nerozlišuje, zda se jedná o bezdrátovou nebo drátovou sběrnici, lze říci, že profily používané pro funkční bezpečnost, které jsou implementovány ještě nad touto vrstvou, je teoreticky možné aplikovat i na tuto sběrnici.
Mnoho pravděpodobných poruch (prakticky všechny) na klasických sběrnicích, pro které jsou definovány a aplikovány bezpečnostní mechanizmy v safety vrstvě, je relevantních i u sběrnic bezdrátových. Nicméně bezdrátové sběrnice ale přinášejí také jiná úskalí vzniku chyb v těchto sběrnicích, která u klasických sběrnic reflektovány logicky být nemusejí (slabý signál, ztráta spojení apod.). I tyto zdroje komunikačních poruch však mohou být detekovány a eliminovány pomocí safety mechanismů používaných u kabelových sběrnic (viz. ztráta spojení u drátových a bezdrátových sběrnic). Pokud budou všechna potencionální rizika brána v úvahu, budou určena patřičná bezpečnostní opatření a definovány a implementovány odpovídající metody pro jejich minimalizaci, pak může být prakticky obecně jakákoli bezdrátová sběrnice použita v aplikacích pro zajištění funkční bezpečnosti. [11]

Jak již bylo řečeno, bezdrátové sběrnice díky své podobnosti komunikačního modelu ve vyšších vrstvách nepřinášejí téměř žádné nové typy komunikačních poruch než sběrnice klasické. Jediným podstatným rozdílem je rozdílnost v pravděpodobnosti výskytu některých těchto poruch. Například pravděpodobnost vzniku poruchy „poškození dat“ (corruption error) je v bezdrátových sítích větší a to z důvodu většího bitového poměru chyb (bit error ratios), nebo krátkodobých výpadků dat, díky špatnému spojení bezdrátových komponent (špatný signál). Může být také očekáváno, že chyba maskování je více závažná, protože bezdrátové sítě jsou více náchylné k úmyslnému či neúmyslnému narušení neoprávněným zásahem (připojením) do sítě. Proto jsou u bezdrátových sítí (nejen v průmyslu) kladeny větší nároky na autentifikační a šifrovací techniky. To je však problém bezpečnosti ve smyslu „Security“, což je problematika velmi rozsáhlá. Nicméně pokud u těchto sítí není možné dosáhnout patřičné úrovně bezpečnosti v tomto smyslu, není možné tyto sběrnice používat v aplikacích pro zajištění funkční bezpečnosti. I když se na první pohled jedná o dvě nesouvisející problematiky, v oblasti funkční bezpečnosti s bezdrátovými komunikačními komponentami je třeba zohlednit a zajistit obojí. [12]

Profisafe pro bezdrátové sítě pro WLAN a Bluetooth

Bezpečnostní komunikační profil PROFIsafe (V2.4) pro ethernetovou sběrnici Profinet byl prvním počinem v bezdrátové funkční bezpečnosti a v současné době je snad jediným používaným řešením funkční bezpečnosti pro bezdrátové sítě. Nicméně se tato oblast v současné době hodně rozvíjí a lze očekávat, že přinejmenším se velmi brzy objeví specifikace a následně i certifikace bezpečnostních bezdrátových sběrnic založených především na Ethernetu. To vyplývá ze samotného konceptu komunikace v Ethernetových sítích.
Vzhledem k tomu, že společně s WLAN byl profil PROFIsafe specifikován a certifikován i pro sítě Bluetooth a tyto sítě jsou v průmyslu také čím dál rozšířenější, dá se očekávat, že se vývoj bezpečnostních profilů bude ubírat i tímto směrem. [13]

RFID komunikace ve Funkční bezpečnosti.

Německá firma EUCHNER, která se již dlouhou dobu zabývá vývojem bezpečnostních prvků pro automatizaci, uvedla na trh nové produkty využívající technologii RFID. Konkrétně se jedná o elektronické bezkontaktní bezpečnostní spínače. Tyto bezkontaktní spínače pracují na principu

RFID čipu a čtecího a vyhodnocovacího zařízení. Nahrazují tedy mechanické kódování klasických elektromechanických spínačů elektronickým kódováním (unikátní kód). Každý aktuátor obsahuje RFID čip s unikátním kódem. Snímací zařízení (spínač) několikrát za sekundu zjišťuje přítomnost čipu s tímto unikátním kódem a porovnává jej s kódem uloženým ve své paměti. Po vyhodnocení shody pak vestavěná elektronika provede požadovaný zásah (sepne svůj bezpečnostní výstup). Neexistuje tady možnost chybného hlášení stavu v případě zalomení spínací vidličky u elektromechanických spínačů. Jakékoli poškození čipu nebo čtecí hlavy znemožní správné porovnání kódů a okamžitě automaticky vypne své bezpečnostní výstupy. Tyto výstupy mohou spínat přímo výkonové akční členy. Vestavěná elektronika má i vysokou úroveň vlastní diagnostiky. Použití této technologie vylučuje možné mechanické poruchy elektromechanických systémů, nevyžaduje přesné seřízení vzájemné polohy RFID čipu a čtecí hlavy a je také odolné proti znečištění či jiným vlivům okolí. Tuto technologii je možné použít například k vyhodnocení vstupu do nebezpečných prostor, ale existuje i celá řada modifikací pro použití v jiných aplikacích. [14]

Další bezdrátové sběrnice pro použití v bezpečnostních aplikacích

Nedávno se již objevila i specifikace CIP safety protokolu pro použití v bezdrátových sítích, takže lze brzy očekávat, že budou certifikovány a na trhu se tak objeví bezdrátové safety komponenty pro sběrnice DeviceNET safety a Ethernet/IP safety. Společnost HIMA, zabývající se také funkční bezpečností, ve svých materiálech uvádí, že také jejich ethernetová sběrnice Safeethernet umožňuje bezdrátovou komunikaci. Sběrnice EsaLAN má již ve svém portfoliu komunikačních komponent také prvky pro bezdrátovou komunikaci v této bezpečnostní sběrnici.

Shrnutí pojmů

V bezdrátových průmyslových komunikačních systémech se dnes používají převážně technologie vycházející z komerčního sektoru, jako s ethernetovými sběrnicemi kompatibilní **Wi-Fi,** nebo **Bluetooth**. Tyto bezdrátové technologie byly upraveny pro použití v průmyslu. Jejich nespornou výhodou je jejich použití v případech kdy technické řešení, nebo okolní podmínky vylučují použití tradičních kabelových tras, nebo je to ekonomicky výhodnější. Použité bezdrátové technologie se také liší podle svého určení. Zde rozlišujeme např.: rychlý kontinuální sběr dat/řízení (**Wi-Fi, Bluetooth, WirelessHART**), identifikační, přístupové a logistické systémy (**RFID, ZigBee**), dálkovou správu, diagnostiku, jednoduché povelování (**GSM, GPRS**,…). Novým trendem je pak použití bezdrátové komunikace v safety-orientovaných aplikacích. Zde se stává sběrnicí s vedoucím postavením **WLAN** s profilem **PROFIsafe a Bluetooth**, nebo některé další ne tolik univerzální řešení. Objevují se i aplikace s použitím technologie **RFID.**

Otázky

1. Co znamená pojem „Spolehlivost“.
2. Jaké jsou základní výhody a nevýhody bezdrátových komunikačních sběrnic.
3. Jaké bezdrátové komunikační technologie se používají v průmyslových aplikacích.

Použitá literatura a další zdroje

1. Řehák J., Co je to WiFi – úvod do technologie, [online], [cit. 15-12-2010] http://hw.cz/ethernet/wifi/wifi_co_to_je.html.
2. Řehák J., Osobní sítě - Bluetooth a IEEE 802.15, [online], [cit. 15-12-2010] http://hw.cz/Produkty/Ethernet/ART917-Osobni-site---Bluetooth-a-IEEE-802.15.html.
3. Vojáček A., ZigBee - novinka na poli bezdrátové komunikace, [online], [cit. 15-12-2010] http://hw.cz/Rozhrani/ART1299-ZigBee---novinka-na-poli-bezdratove-komunikace.html.
4. Pužmanová R., WiMAX a budoucnost mobilních služeb, [online], [cit. 15-12-2010] http://www.lupa.cz/clanky/wimax-a-budoucnost-mobilnich-sluzeb/.
5. VAE Prosys, Bezdrátový sběr dat WISA, [online], [cit. 15-12-2010] http://www.vaeprosys.cz/chapter.asp?k=38&mk=9&ms=38.
6. Standard WirelessHART z pohledu předních dodavatelů řídicí techniky, AUTOMA 10/2010, [online], [cit. 15-12-2010] http://www.odbornecasopisy.cz/index.php?id_document=42082.
7. Myslík V., Řehák J., IrDa – Kompletní popis, [online], [cit. 15-12-2010] http://hw.cz/Teorie-a-praxe/Dokumentace/ART784-IrDa---Kompletni-popis.html.
8. Vojáček A., RFID senzory – současná situace, [online], [cit. 15-12-2010] http://automatizace.hw.cz/rfid-senzory-soucasna-situace.
9. Standardy mobilních telefonů. Wikipedia. [online], [cit. 15-12-2010] http://tomas.richtr.cz/mobil/bunk-gsm.htm
10. Spolehlivá bezdrátová komunikace už není oxymóron, AUTOMA 08/2009.
11. Validation of safety-related Wireless machine control systems, Timo Malm, Jacques Hérard, Jørgen Bøegh & Maarit Kivipuro TR 605 Approved 2007-03 Nordic Innovation systems.
12. Safety of Digital Communications in Machines Jarmo Alanen, Marita Hietikko & Timo Malm VTT Industrial Systems.
13. Profil Profisafe i pro bezdrátové sítě, AUTOMA 06/2007.
14. Bezkontaktní bezpečnostní spínače s využitím RFID, AUTOMA 08-09/2010.

Řešená úloha 14.1

Zadání: Prezentace hlavních programů.

Předmětem cvičení je prezentace hlavních programů, na kterých studentu v rámci předmětu pracovali.

Rejstřík