VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY
DEPARTMENT OF CONTROL AND INSTRUMENTATION

CIP SAFETY
CIP SAFETY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Michal Šmoldas

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Radek Štohl, Ph.D.

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Kybernetika, automatizace a měření**
Ústav automatizace a měřicí techniky

Student: Bc. Michal Šmoldas ***ID:*** 164853
Ročník: 2 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

CIP Safety

POKYNY PRO VYPRACOVÁNÍ:

1. Proveďte literární rešerši o technologii CIP a zaměřte se na jeho jednotlivá rozšíření.
2. Detailně popište rozšíření CIP Safety v bezpečnosti strojů.
3. Navrhněte a vytvořte laboratorní úlohu s bezpečnostní instrumentací laboratoři založené na technologii CIP Safety.
4. Ověřte své řešení.

DOPORUČENÁ LITERATURA:

CIP Common Specification. ODVA.

CIP Safety Specification. ODVA.

Vasko, D. A. et al. CIP Safety: Safety Networking for the Future. 38th annual IEEE International Conference on Communications. USA 2003.

Dle vlastního literárního průzkumu a doporučení vedoucího práce.

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 14.5.2018

Vedoucí práce: Ing. Radek Štohl, Ph.D.
Konzultant:

doc. Ing. Václav Jirsík, CSc.
předseda oborové rady

Abstrakt

Tato diplomová práce se zabývá rozborem technologie CIP a vytvořením laboratorní úlohy z komponentů založených na této technologii. Cílem práce je vytvoření literární rešerše o technologii CIP a jeho jednotlivých rozšíření se zaměřením na CIP Safety. Dále je sestaven funkční laboratorní panel z dostupných komponentů v laboratoři FEKT VUT Brno, podporujících tuto technologií, se specifikací zadání laboratorní úlohy. Funkčnost panelu byla ověřena SW řešením laboratorní úlohy s vizualizací a řízením virtuální výrobní linky. Výsledkem práce je literární rešerše o technologii CIP, funkční laboratorní panel, specifikace zadání laboratorní úlohy a SW řešení úlohy s vizualizací a řízením virtuální výrobní linky.

Klíčová slova

Průmyslové komunikační sítě, CIP, CIP Safety, komponenty, bezpečnostní laboratoř, laboratorní úloha, HW a SW řešení.

Abstract

This master´s thesis deals with the analysis of CIP technology and the creation of laboratory tasks from components based on this technology. The aim of the thesis is to create a literary research on CIP technology and its individual extensions focusing on CIP Safety. Further, a functional laboratory panel is assembled from the available components in the FEKT VUT Brno laboratory supporting this technology CIP Safety, specifying the assignment of the laboratory task. Functionality of the panel has been verified by the SW solution of the laboratory task with visualization and control of the virtual production line. The result of the work is literary research on CIP technology, functional laboratory panel, specification of assignment of laboratory task and SW solution of task with visualization and control of virtual production line.

Keywords

Industrial communications networks, CIP, CIP Safety, components, safety laboratory, laboratory task, HW and SW Solutions.

Bibliografická citace:

ŠMOLDAS, M. *CIP Safety*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 81 s. Vedoucí diplomové práce Ing. Radek Štohl, Ph.D.

Prohlášení

„Prohlašuji, že svou diplomovou práci na téma CIP Safety jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.
Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.”

V Brně dne: 10. května 2018 .....

podpis autora

Poděkování

Děkuji vedoucímu diplomové práce Ing. RADKU ŠTOHLOVI Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé diplomové práce.

V Brně dne: 10. května 2018 .....

podpis autora

Obsah

Seznam symbolů a zkratek

Zkratky:

CIP	common industry protocol *(průmyslový komunikační protokol)*
EtherNet/IP	EtherNet/industrial protocol *(ethernetový průmyslový protokol)*
ISO	international standards organization *(mezinárodní organizace pro normalizaci)*
OSI	open system interconnection *(model pro propojení otevřených systémů)*
IEEE	instituts of electrical and electronics engineers *(institut pro elektrotechnické a elektronické inženýrstvý)*
IP	internet protocol *(internet protokol)*
TCP	transmission control protocol *(protokol pro obousměrný přenos dat)*
HTTP	hypertext tranfer protocol *(internetový protokol pro výměnu HTML souborů)*
SNMP	simple network management protocol *(internetový protokol pro zprávu sítě)*
DHCP	dynamic host configuration protocol *(protokol používaný k automat konfiguraci zařízení v síti)*
ID	identity dokument *(identifikační číslo)*
MAC	medium acces control *(jedineční identifikátor zařízení v síti)*
CSMA/CD	carrier sense multiple / collision detection *(protokol k určení přístupu médiím přenosu)*
TCP	transmission control protocol *(internetový komunikační protokol se zárukou doručení)*
UDP	user datagram protocol *(internetový komunikační protokol bez záruky doručení)*
I/O	input / output *(vstupy/výstupy)*

ODVA	open devicenet vendors association *(organizace vyvíjející komunikační protokol CIP)*
CAN	controller area network *(sběrnice pro komunikaci senzorů a funkčních jednotek)*
RS485	standard dvouvodičové sériové komunikace.
TDMA	time devison multiple access *(časová metoda sdílení přístupu k síti)*
UCMM	unconnected message manager *(správce nepřiřazených zpráv)*
IP xx	stupeň ochrany proti vniknutí cizího předmětu a kapaliny
TNC	označení konektoru
CTDMA	concurrent time domain multiple access *(kódovaná časová metoda sdílení přístupu k síti)*
NUT	network update time *(čas obnovení sítě)*
EDS	electronic data sheet *(elektronický list)*
ASCII	american standard code for information interchange *(americký standardní kód pro výměnu informací)*
SIGs	special interest groups. *(speciálně zaměřená skupina)*
SIL	safety integrity level *(úroveň integrity bezpečnosti)*
PL	performance level *(úroveň vlastností)*
CRC	cyclic cedundancy check *(kontrolní součet)*
PID	production identification *(produkční identifikátor)*
SW	software

HW	hardware
PLC	programmable logic controller (programovatelný *automat)*
OPC DA	open platform communications data access *(skupina standardů určená k real-time komunikaci)*
ČSN EN ISO	soustava Českých technických norem převzatá (harmonizovaná) z Evropských norem
BOOTP/DHCP	bootstrap protocol / dynamic host configuration protocol *(program pro vyhledání zařízení podle MAC adresy)*
DIP Switch	dual in-line package switch *(vícenásobný přepínač)*
ADD-ON Profile	doplňkový profil
DI	dual input *(relé se zdvojeným vstupem)*
DIS	dual input solid-state *(relé se zdvojeným polovodičovým vstupem)*
EM	expansion module *(relé s pomocnými kontakty)*
EMD	expansion module delayed. *(relé s pomocnými kontakty se zpožděním)*
GLP	guardlocking proximity module. *(relé s modulem pro ovládání zámků)*
GLT	guardlocking with time-delay. *(relé s modulem pro ovládání zámků s časovou prodlevou)*
RFID	radio frequency identification *(rádiový frekvenční identifikátor)*
LC	light curtain *(světelná clona)*
ESTOP	emerigency stop *(nouzové zastavení)*
RIN	redundant input *(zdvojený vstup)*

Seznam obrázků

Seznam tabulek

1 ÚVOD

V současné době prochází automatizace manipulačních procesů a technologií kolosálním vývojem. Neustálá modernizace a navyšování nároků zákazníků, ať už ze stran technologie, financí, ale i bezpečnosti strojů nebo obsluhy, má za následek vývoj nových komunikačních sběrnic a protokolů. Tyto nově vyvinuté nástroje slouží k usnadnění návrhu automatizovaného pracoviště, či realizace projektů v rámci výrobního průmyslu.

Prvním bodem zadání mojí diplomové práce s názvem CIP Safety je vytvoření literární rešerše o technologii CIP a jejich rozšířeních. Celá literární rešerše je rozdělena do několika kapitol. V první části je popsána technologie CIP, jejímž cílem je spojení průmyslových sítí EtherNet/IP™, DeviceNet™, CompoNet™ a ControlNet™ jediným univerzálním komunikačním protokolem. Z tohoto důvodu jsou v prvních kapitolách práce popsány základní principy, rozdíly a vzájemné podobnosti čtyř výše uvedených průmyslových sítí. Po seznámení čtenářů se základními principy, následuje část o samotném CIP průmyslovém komunikačním protokolu a jeho jednotlivých rozšířeních CIP Energy, CIP Sync, CIP Motion, CIP Security a CIP Specification libraly.

Druhým bodem zadání je podrobné popsání rozšíření CIP Safety. Tento bod už je částečně splněn při popisu technologie CIP, avšak pokračuje rozšířením o podrobnější popis CIP Safety a jeho vnitřních principech.

Třetím bodem zadání je vytvoření laboratorní úlohy s prvky podporující CIP Safety protokol. Před samotnou specifikací zadání seznamuji čtenáře s dostupným softwarem ve školní laboratoři fakulty FEKT VUT Brno. Dále provádím rozbor a popis dostupných komponentů. Po seznámení se s komponenty a zjištění jejich možností je nutné navrhnout zapojení s celkovou topologií sítě. Následuje fyzická montáž, zapojením komponentů a vytvoření funkční HW konfigurace. Zajímavým řešením je vytvoření vizualizace a řízení virtuální linky.

Dalším krokem je formulace zadání, dle možností mnou vytvořeného laboratorního panelu a následná tvorba vlastního řešení s vizualizací. V rozboru vlastního řešení se zaměřuji na popis řízení, použití předdefinovaných funkcí, rozdělení logiky a popis tvorby vizualizace výrobní linky.

2 PRŮMYSLOVÉ KOMUNIKAČNÍ SÍTĚ

V následující kapitole jsou popsány vybrané průmyslové komunikační sítě, které se stávají nezbytnou součástí při automatizaci procesů. Používají se pro přenos, analýzu, sběr dat a informací nezbytných pro řízení v průmyslu.

Postupnou modernizací průmyslu a vývojem techniky vznikl nespočet komunikačních sítí a průmyslových sběrnic na bázi odlišných standardů, dle rozdílných norem, pro různé části světa. Vniklé modifikace se přizpůsobují potřebám v průmyslu, nicméně principiálně fungují obdobně, jako základní modely.

V práci se omezuji pouze na některé z nich. Patří mezi ně EtherNet/IP™, DeviceNet™, CompoNet™ a ControlNet™. Tyto čtyři průmyslové komunikační protokoly vycházejí ze standardu otevřené komunikace ISO/OSI [1].

2.1 Referenční model ISO/OSI

Model ISO/OSI [1] byl přijat jako mezinárodní norma ISO 7498[2] v roce 1984. Při jeho použití mohou účastníci komunikovat po příslušné sběrnici. Model reprezentuje 7 vrstev s definovanými funkcemi, které určují, jak zahájit a ukončit komunikační proces. Každá vrstva upravuje data, přidává další nezbytné informace pro úspěšný přenos a předává je vyšší vrstvě. Jednotlivé vrstvy mají přístup pouze do vrstev o jednu úroveň vyšší nebo nižší. Grafické znázornění vrstev se stručným popisem viz Obr. 2-1.

Fyzické (kabelové) propojení zdroje a cíle probíhá pouze v první vrstvě modelu, protože ostatní vrstvy jsou propojeny virtuálně, ale fyzická zařízení virtuálně komunikují pouze na úrovni sedmé aplikační vrstvy. Před zahájením komunikace je potřeba navázat spojení, provést synchronizaci, rozdělit data do rámců, průběžně kontrolovat chyby komunikačních/datových paketů, provést kompresi, kódování a mnoho dalších operací a úkonů pro přepravu dat do nadřazené aplikace.

[1] International standards organization/Open system interconnection.

[2] Mezinárodní norma pro propojení nesjednocených systémů.

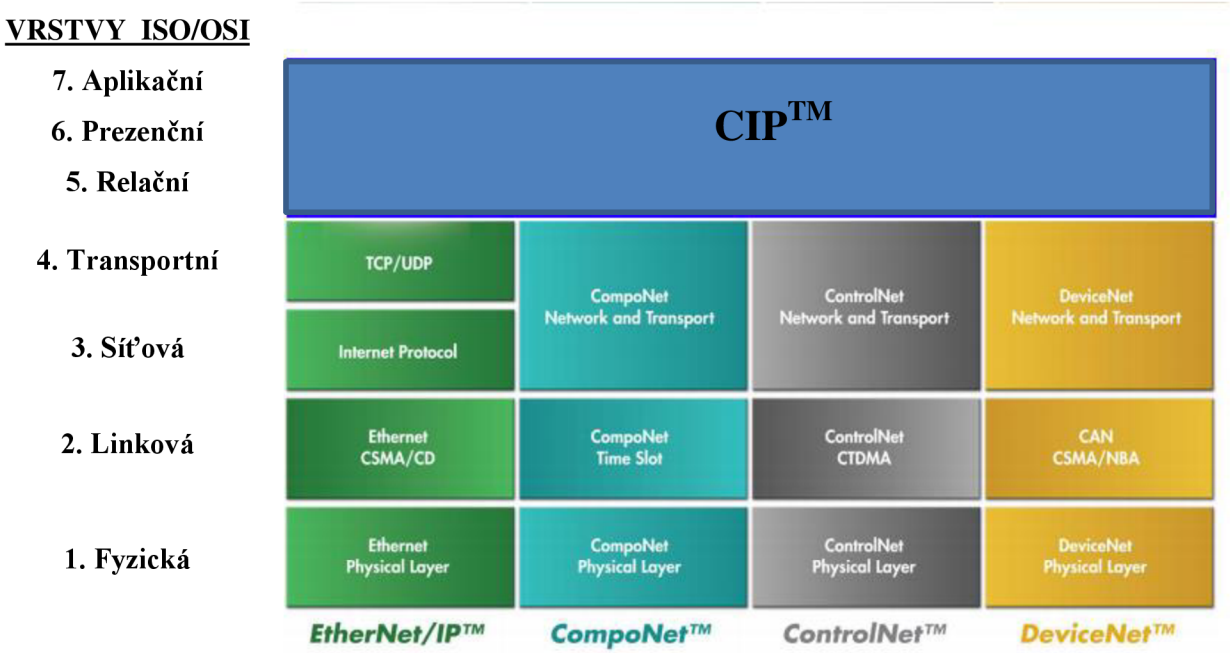
Obr. 2-1 Referenční model ISO/OSI [1].

Průmyslové komunikační protokoly [2] EtherNet/IP™, DeviceNet™, CompoNet™ a ControlNet™ používají v 7 – 5 vrstvě protokol CIP [3]. Ve zbylých vrstvách 4 – 1 se individuálně liší pro použití jiných standardů a funkcí viz Obr. 2-2.

Z Obr. 2-2 jsou na první pohled patrné rozdíly v rozložení jednotlivých vrstev, tak i v použitých standardech. U EtherNet/IP [2] je každá vrstva 1 – 4 reprezentována samotnou funkcí, kdežto u zbylých tří protokolů proběhlo sdružení třetí a čtvrté vrstvy.

Podrobnější popis principů a rozdílů byl pro přehlednost přesunut do následujících kapitol.

[3] Common industry protocol.



Obr. 2-2 Grafické znázornění komunikačních protokolů v modelu ISO/OSI [2].

2.2 EtherNet/IP™

EtherNet/IP[4] [3] byl vyvinut pro použití v průmyslové automatizaci a časově kritických aplikacích. Uživatelům umožňuje konfiguraci, sběr dat z jednoho nebo více zařízení. Lze použít i jako páteřní síť, podporuje fyzické vrstvy standardů IEEE[5]. Je flexibilní v možnostech kabelové, tak i bezdrátové instalace, obsahuje IP[6] sadu-stanardu TCP[7]/Ethernet.

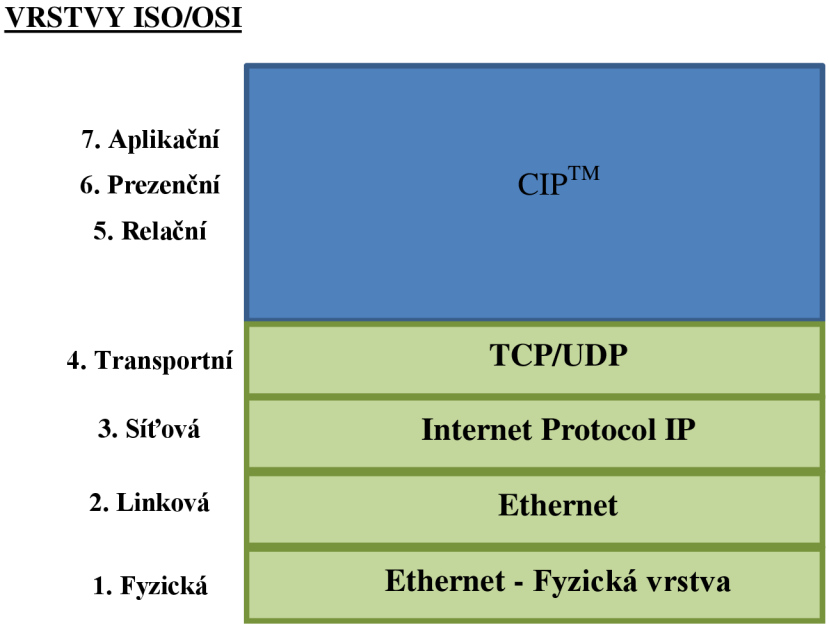
Podporuje [2] přenosové rychlosti 10, 100, 1000 Mbit/s, neomezené množství uzlů v síti, použití podsítí pomocí IP směrovačů, podporu adresování pomocí IP, komunikaci ve stejné podsíti v reálném čase. Dále umožňuje snadné začlenění často používaných zařízení do sítě, jako jsou roboti, měniče, automaty, řídící jednotky pohonů, akční členy atd. a je kompatibilní s komunikačními standarty HTTP[8], SNMP[9], DHCP[10].

Hierarchie EtherNet/IP ve standardizovaném sedmivrstvém modelu ISO/OSI [3] byla zobrazena na Obr. 2-3. Na obrázku jsou přehledně rozkresleny jednotlivé vrstvy

[4] Industrial protocol.
[5] Instituts of electrical and electronics engineers.
[6] Internet protocol.
[7] Transmission control protocol
[8] Hypertext tranfer protocol.
[9] Simple network management protocol.
[10] Dynamic host configuration protocol.

ISO/OSI modelu společně s komunikačními standardy a fyzickým vzhledem EtherNet/IP.

Komunikace a výměna [4] dat v sítí probíhá modelem *producent – konzument,* přičemž odeslaná data může konzumovat jedno nebo více zařízení současně. To je umožněno díky zapouzdření zprávy v síti. Zpráva od producenta není poslána na cílovou adresu, ale je odeslána pod jedinečným ID [3] do sítě. Přes toto ID může zprávu přečíst více uzlů zaráz, což je velice výhodné a komunikace je mnohonásobně rychlejší než, posílat stejnou zprávu každému uzlu zvlášť modelem *zdroj – cíl*, nicméně Ethernet/IP umožňuje použití obou modelů.



Obr. 2-3 EtherNet/IP v modelu ISO/OSI [3].

Následuje stručný popis jednotlivých částí modelu EtherNet/IP a přiblížení funkcí vrstev zobrazených na Obr. 2-3.

2.2.1 Ethernet

Fyzická i linková vrstva Ethernetu [2] jsou celosvětově standardizovány institutem IEEE[11] podle směrnice IEEE 802.3-2008[12].

Fyzická vrstva Ethernetu slouží k upravení, adresování a k celkové přípravě dat na přenos. Přes tuto vrstvu jsou datové rámce a pakety směřovány dalším účastníkům. Přenos bitů začíná startovací procedurou, která synchronizuje komunikaci zdrojové

[11] Institute of electrical and electronics engineers.

[12] Revize norem standardů ethernetu.

a cílové stanice. Následují adresy zdroje, cíle, typ zprávy (unicast[13], anycast[14], multicast[15]), dále pak data a kontrolní součet. Jestliže se kontrolní součet cíle v daném rámci shoduje, pošle jej do linkové vrstvy. Pokud se ovšem neshoduje, vyřadí daný rámec bez předání informace vysílači.

Linková vrstva zajišťuje přiřazení unikátní MAC[16] adresy, která slouží k zabezpečení přenosu a definuje metodu přístupu MAC. Metoda přiřazení CSMA/CD[17] pracuje na principu přístupových práv. Každý účastník má stejné přístupové právo v případě, že o médium nežádá jiný účastník. Kolizi rámce odhalí vyšší vrstvy modelu.

2.2.2 Internet protocol

Internet protokol [3], dále jen IP, tvoří základní síťovou vrstvu mezi-síťového směrování. Obsahuje chybové hlášení a datagramy, což jsou skupiny paketů a rámců pro přenos dat s různou maximální velikostí.

IP adresy můžeme dělit na veřejné a soukromé. Veřejné jsou celosvětově unikátní 32 bitová čísla vydaná institucí NIC[18]. Soukromé jsou unikátní pouze v rámci sítě. Dále IP adresy dělíme na několik tříd: A, B, C, D, E podle rozlehlosti sítě. V současnosti se dělení na sítě a podsítě používají tzv. masky podsítě. Maska podsítě je reprezentována ve stejném formátu jako IP adresa, ale používají se na rozlišení jednotlivých uzlů v síti s koncovými zařízeními. Tím se stává adresní prostor mnohem efektivnější.

PŘÍKLAD:

Plná síťová adresa:	192.168.5.10
Maska podsítě:	255.255.255.0
Síťová část:	192.168.5.0

2.2.3 Transmission control protocol

TCP [3] je komunikační protokol pro explicitní[19] odesílání zprávy. V síti EtherNet/IP se používá pro konfiguraci a odesílání nestrukturovaného proudu bajtů. Používá pořadová čísla a potvrzovací zprávy, tím poskytuje uzlu data o spolehlivém doručení. Přenáší více informací o přenosu => více zatěžuje síť.

---

[13] Zpráva jedinému příjemci.

[14] Zpráva většímu počtu příjemců, ale pouze v okolí vysílací stanice.

[15] Zpráva většímu počtu příjemců i vzdáleným stanicím.

[16] Medium acces control.

[17] Carrier sense multiple / Collision detection.

[18] Netvork information center

[19] Přímé, pro jeden uzel.

Při ztrátě dat ze zdroje k cíli umožňuje TCP neustále posílání telegramu, kontrolu chyb nebo rozeznání duplikát zprávy. Podporuje i regulaci průtoků dat a zasílání dat do vyšších vrstev modelu. V Tab. 2-1 byl zobrazen komunikační paket TCP protokolu s popisem jednotlivých bloků.

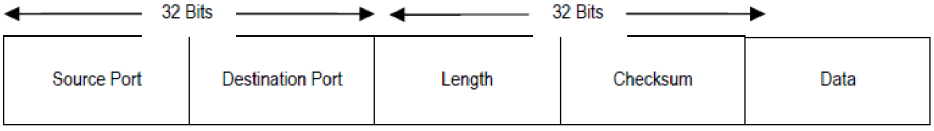
Tab. 2-1 TCP komunikační paket [3].

Source port			Destination port
Sequence number			
Acknowledgment number			
Data offset	Reserved	Flags	Window
Checksum			Urgent pointer
Options (+paddind)			
Data (variable)			

Source port *(Zdrojový port)* – určuje zdroj procesu.
Destination port *(Cílový port)* – určuje cíl procesu.
Sequence number *(Pořadové číslo)* – obsahuje pořadové číslo prvního bajtu.
Acknowledgment number *(Potvrzovací číslo)* - obsahuje pořadové číslo dalšího bajtu.
Data offset *(Offset dat)* – počet 32 bit slov v hlavičce protokolu.
Reserve *(Rezerva)* – rezerva pro budoucí použití.
Flag *(Příznak)* – řídící informace pro navazování/ukončování spojení.
Window *(Okno)* – velikost zásobníku pro příchozí data.
Checksum *(Kontrolní součet)* – indikátor poškození dat/záhlaví při přenosu.
Urgent pointer *(Naléhavý ukazatel)* – ukazatel na nenaléhavá data v paketu.
Options *(Nastavení)* – specifikace UTC nastavení.
Data *(Data)* – data pro horní vrstvy.

2.2.4 User datagam protocol

UDP [3] je jednoduší než TCP. Přináší nižší zatížení sítě, protože záhlaví obsahuje méně bajtů, ale nepřidává spolehlivost ani kontrolu chyb. Používá implicitní[20] odesílání zprávy. Používá se pro komunikaci v reálném čase. Komunikační paket UDP komunikačního protokolu byl zobrazen na Obr. 2-4 i s popisem jednotlivých bloků.



Obr. 2-4 UDP komunikační paket [3].

[20] Nepřímé, pro více uzlů.

Source port *(Zdrojový port)* – určuje zdroj procesu.
Destination port *(Cílový port)* – určuje cíl procesu.
Lenght *(Délka)* – délka záhlaví a dat.
Checksum *(Kontrolní součet)* – volitelný indik. poškození dat/záhlaví při přenosu.
Data *(Data)* – data pro horní vrstvy.

2.3 DeviceNet™

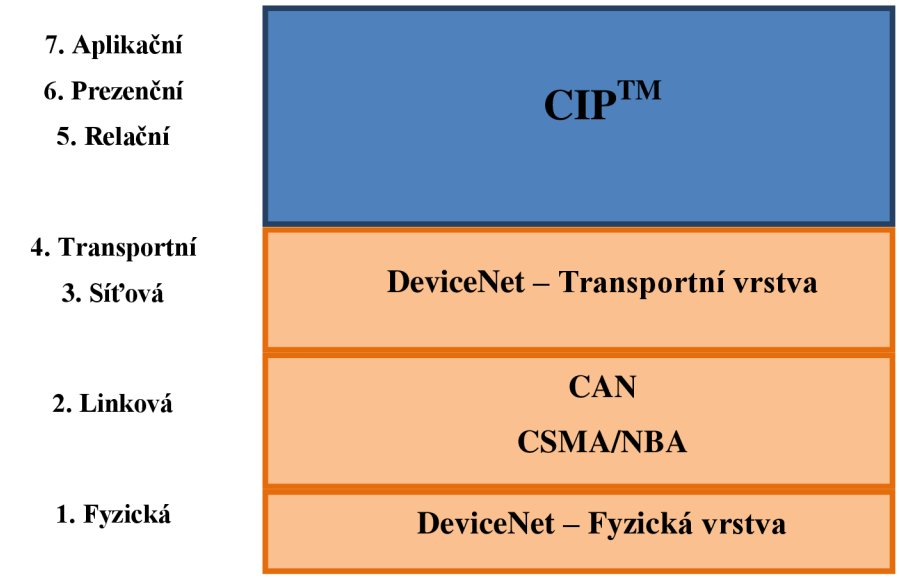
DeviceNet [2] je stabilní, spolehlivá průmyslová komunikační sběrnice propojující převážně koncové zařízení[21]. Poskytuje mnoho modulů určených pro rozšíření řídicích systémů[22], ale i I/O[23] zařízení. Na trh ji uvedena organizace ODVA[24], která se aktivně podílí na jejím dalším vývoji.

Sběrnice [5] kromě komunikace umožňuje i napájení zařízení. Pro komunikaci používá model poskytovatel/příjemce, což umožňuje vysokou datovou průchodnost. Taktéž lze sběrnici nastavit na model master/slave nebo peer to peer.

Konfiguruje hlavní vedení, podporuje maximálně 64 uzlů, umožňuje přidat/odebrat uzel do/ze sítě v plném provozu. Dále podporuje snadné začlenění často používaných zařízení do sítě, napájení koncových zařízení po sběrnici tak, i ze sítě, použití open style konektorů a volitelných rychlostí přenosu 125, 250, 500 kBaud. Umožňuje nastavitelní konfigurace dle potřeb aplikace s možností zatížení až 16 A. Dále podporuje připojení několika napájecích zdrojů s integrovanou ochranou proti přetížení atd.

Hierarchie DeviceNet v sedmivrstvovém modelu ISO je zobrazena na Obr. 2-5. Vrstvy 1 – 4 jsou tvořeny komunikačními standardy DeviceNet a 5 – 7 opět protokolem CIP, stejně jako u EtherNetu/IP viz předchozí kapitola 2.2.

[21] Akční členy, senzory.
[22] Programovatelných automatů.
[23] Imput / output.
[24] Open devicenet vendors association.



Obr. 2-5 DeviceNet v modelu ISO/OSI [3].

2.3.1 DeviceNet fyzická vrstva

Fyzická vrstva DeviceNet [5] definuje elektrické vedení a konektory, umožňuje použití kroucené dvojlinky pro řídící signály i pro napájení stanic.

DeviceNet používá topologii typu páteřové vedení s uzly a odbočkami. Napájecí uzel můžeme přidat kdekoliv v topologii sítě. Podporované přenosové rychlosti a maximální délky vedení se odvíjejí od použitého kabelu. Taktéž můžeme kombinovat několik druhů konektorů například terminálové, mikro nebo prořezávací patice na plochý kabel.

2.3.2 CAN

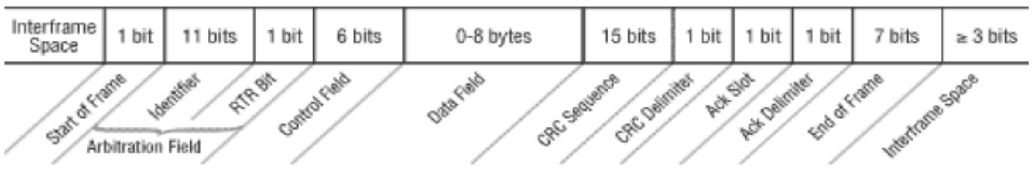
Standard CAN[25] [5] definuje linkovou vrstvu. Dle tohoto standardu jsou definovány logické úrovně dominantní level pro logickou 0 a neaktivní level pro logickou 1.

Pomocí těchto dominantních a neaktivních levelů vysílače sběrnice poznají uzly, které právě vysílají/nevysílají popřípadě kolize mezi nimi. Komunikaci tvoří 4 rámce (Remote[26], Data[27], Error[28], Overload[29]), ale pouze jeden přenáší samotná data. Datový rámec komunikační sběrnice DeviceNet je zobrazen na Obr. 2-6.

Při komunikaci více jednotek současně se všechny jednotky synchronizují hranou a pak se pomocí bitového algoritmu určí priorita a pořadí vysílání, tím jsou vyřešeny konflikty bez jakékoliv ztráty dat a informací. Při požadavku na komunikaci

[25] Controller area network.
[26] Rámec žádostí.
[27] Rámec dat.
[28] Rámec chyb.
[29] Rámec přetížení.

jediné jednotky lze komunikovat modelem peer-to-peer[30] , ale pouze za podmínky, že na sběrnici je klid[31].



Obr. 2-6 CAN komunikační paket [5].

Start of frame *(Začátek rámce)* – definuje začátek rámce.
Identifier *(Identifikátor)* – identifikátor rámce ID.
RTR Bit *(Žádost o vzdálený přenos)* – vzdáleném přenos dat/prázdného rámce.
Control Field *(Řídící pole)* – obsahuje identifikaci prodlouženého označení.
Data Field *(Datové pole)* – obsahuje samotná přenášená data.
CRC *(Kontrola cyklic. nadbytečnosti)* – bezpečnostní pole pro detekci chyb v datech.
ACK *(Potvrzení přijetí)* – přenáší informaci o přijetí rámce, až po jeho konec.
End of Frame *(Konec rámce)* – ukončovací bity rámce.
Interface Space *(Rozhraní)* – oddělovací znaky od další zprávy.

2.3.3 DeviceNet transportní vrstva

Pro sestavení spojení s výměnou dat [5] je potřeba identifikovat uzly I/O modulů pomocí zpráv a ID. Zprávy dělíme na explicitní[32] a implicitní[33].

ID nese informace o způsobu komunikace, adresy, charakter přenášených dat, model přenosu atd. Když jsou známé všechny předešlé informace u obou nebo více účastníků, může být zahájen přenos datových rámců. ID je reprezentováno 11 bity rozdělenými do čtyř skupin. První a druhá skupina definuje ID připojení, zbylé dvě definují priority a MAC ID. Díky systému jedinečných ID a kontrolnímu algoritmu na vyhodnocení, je zamezeno duplicitním adresacím, tudíž uživatel může přidávat/odebírat zařízení za provozu.

2.4 CompoNet™

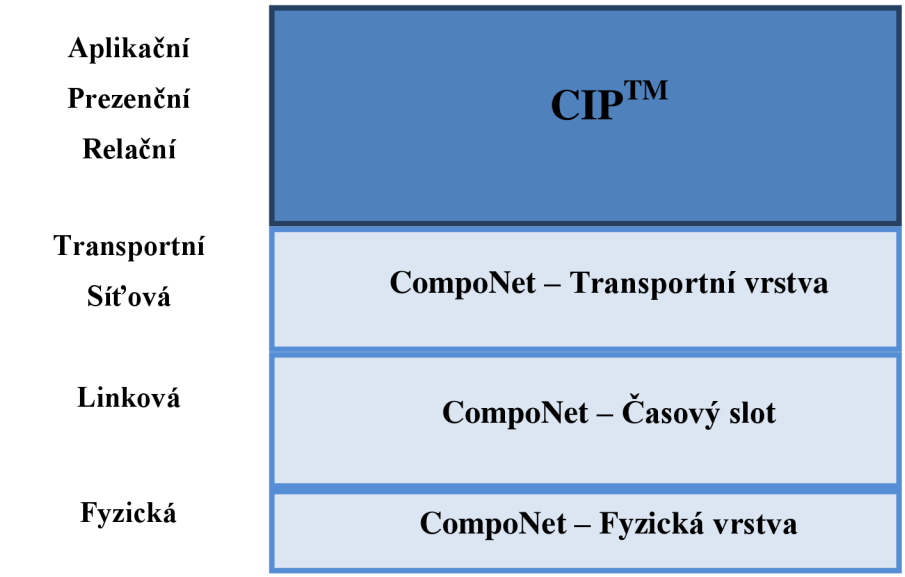
CompoNet [2], [6] představuje deterministickou[34] vysokorychlostní komunikační síť určenou pro transport dat z I/O modulů a explicitních zpráv v reálném čase. Podporuje více modelů hierarchií a priorit zpráv. Díky deterministickému přístupu do sítě brání kolizím a umožňuje časové plánování přenosu dat bez ztráty účinnosti dle předem

[30] Od účastníka k účastníkovi.
[31] Nikdo jiný nechce komunikovat.
[32] Přímé pro komunikaci žádost/odpověď.
[33] Nepřímé pro komunikaci I/O v reálném čase.
[34] Předvídatelnou.

daného rozvrhu. Dále obsahuje nástroje pro diagnostiku sítě, což urychluje řešení poruch a usnadňuje údržbu.

CompoNet nabízí vysokorychlostní cyklickou výměnu vstupních/výstupních dat o rozsahu bitů[35] až mezi 384 uzly. Umožňuje použití čtyř nebo dvou žilových kabelů s přenosovou rychlostí od 93,73 kbps – 4 Mbps[36] a s možností začlenění až 64 opakovačů v síti.

Základem je opět model ISO/OSI, který definuje použité komunikační rámce, viz Obr. 2-7. Vrstvy 1 – 4 jsou tvořeny komunikačními standardy CompoNet, které jsou poněkud zjednodušeny oproti jiným komunikacím, nicméně i přes tyto zjednodušení vyšší vrstvy 5 – 7 mohou být realizovány opět protokolem CIP, stejně jako u EtherNetu/IP i DeviceNetu, viz předchozí kapitoly.



Obr. 2-7 CompoNet v modelu ISO/OSI [6].

2.4.1 CompoNet fyzická vrstva

Fyzická vrstva CompoNetu [6] je odvozena z RS485[37] s použitím kódovaného signálu Manchester a impulsního transformátoru. Transformátor izoluje zařízení od komunikace a zdvojnásobuje vysílané napětí, tudíž zvyšuje velikost vysílaného napětí na přijímacím konci. Dále používá masku sítě na bázi digitálního filtrování. Díky těmto úpravám je možné použít pro vedení signálu dvouvodičové nestíněné kabely s různými elektrickými vlastnostmi.

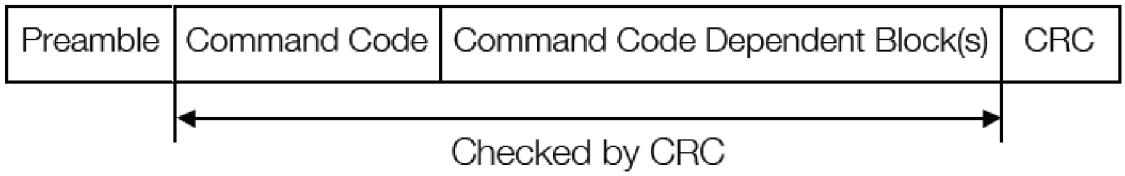
Hierarchie sítě může být díky použití opakovačů velice rozsáhlá a efektivní. Na páteřní vedení můžeme připojit několik podsítí s různými topologiemi i použitým

[35] Vhodné pro senzory a ovládaní pohonů.
[36] Široká škála umožňuje kompromis rychlost/vzdálenost.
[37] Standard dvouvodičové sériové komunikace.

druhem vedení[38] s velkým množstvím koncových uzlů. Délka vedení může být až trojnásobná. Zpoždění přenosu dat kvůli opakovačům je ošetřeno technologií TDMA[39], která udává polohu, kde se opakovač na síti nachází a s jakým předstihem musí data odeslat, aby byly na páteřní síti bez zpoždění.

2.4.2 CompoNet časový slot

Časový slot [6] je definován fyzickou vrstvou a udává strukturu rámce sítě CompoNet. Rámec zajišťuje přenos, kvalitu přenosu, rychlost, kódování a kontrolu dat. Skládá se ze startovacího kódu, příkazů, bloku závislých na předchozích příkazech a kontroly, viz Obr. 2-8.



Obr. 2-8 CompoNet komunikační paket [6].

Preamble *(Úvod)* – startovací kód rámce.
Command code *(Příkazy)* – zakódování typu použitého rámce.
Command code depandent block *(Blok závislí na příkazech)* – vlastní rámec.
CRC *(Kontrola cyklic. nadbytečností)* – bezpečnostní pole pro detekci chyb v datech.

Důležitou úlohu v této vrstvě má TDMA, protože řídí přenos. Existuje 7 typů rámců[40], které jsou zakódovány v 7 bitových kombinacích - Commnad code.

Každý z rámců [2] plní jiný úkol. OUT jde ze stanice Master do Slave nebo opakovače a poskytuje výstupní data. Slave blíže specifikuje podskupinu Slave nebo u opakovačů provádí jejich synchronizaci pro spuštění zesilovačů CN a IN rámců. Data jsou uspořádána v 16 bitových slovech.

TRG funguje jako rámec OUT s tím rozdílem, že Master jej odesílá, když nejsou výstupy k odeslání. CN používá Slave nebo opakovač pro hlášení stavu, žádostí a informací o odeslání stanici Master. IN slouží k přenosu vstupních dat slovo po slově ze Slave do Master. A_EVENT slouží k poslání acyklické zprávy[41], může jej odeslat kterýkoliv uzel. B_EVENT vytváří uzel Master, slouží k nastavení parametrů spojení nebo uděluje povolení na požadavek nebo odpověď rámce typu A_EVENT. BEACON slouží k určení přenosové rychlosti a k odeslání inicializačních parametru stanici Slave nebo opakovači.

[38] Kulaté nebo ploché kabely.
[39] Time devison multiple access.
[40] OUT, TRG, BEACON, CN, IN, A_EVENT a B_EVENT.
[41] Představují alarmy a datové záznamy.

Primární funkcí TDMA [6] je minimalizovat zpoždění komunikace. Princip spočívá v tom, že mezi rámce se vkládá mezera, které zohledňuje zpoždění ostatních rámců a zabraňuje tak vzájemné kolizi. Například při použití dvou opakovačů se vloží mezera rovná čtyřnásobku zpoždění opakovače.

2.4.3 CompoNet transportní vrstva

Pro transport zpráv v síti CompoNet [6] se používá UCMM[42] nebo explicitní protokol. Stanice Master musí znát místo doručení, nastavit časovou prodlevu, *IN* a *CN* rámce. Při detekci stanice Slave pomocí rámce *CN*, se naváže spojení a začne probíhat přenos pomocí TDMA a rámců. Pokud přijde žádost o navázání spojení s nezúčastněnou stanicí, tak ji Master automaticky zapracuje do komunikace.

Explicitní zprávy spravuje a monitoruje správce událostí, dlouhé zprávy rozděluje na kratší a ty pak zpracovává. Taktéž sleduje pokusy a reakce na tento druh zpráv. Vyšším vrstvám je odeslána celá zpráva a ne jednotlivé fragmenty.

2.5 ControlNet™

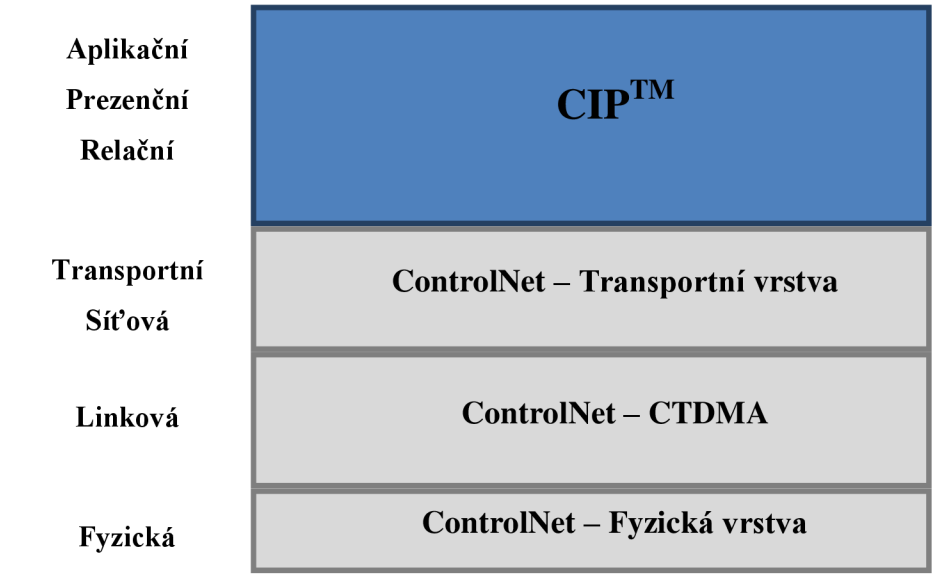
ControlNet [2], [7] je deterministická komunikační síť pro vysoko rychlostní výměnu dat v časově kritických I/O aplikacích s předvídatelným způsobem. Umožňuje komplexně shromáždit, řídit a konfigurovat toky data v síti při výrobním procesu.

Jeho flexibilita topologie sítě s použitím různých kombinací zapojení do hvězdy, stromové struktury, lineární sběrnice nebo možnost použití opakovačů a tím spjaté prodloužení přenosové trasy. Umožňuje použít až 99 uzlů s rychlostí 5 Mbit/s. Dále nabízí možnost přidávat/odebírat uzly v plném provozu s podporou klasického koaxiálního kabelu, který se používá pro přenos televizního signálu a redundantního vedení[43]. Pro svoje unikátní vlastnosti a podporu norem v průmyslu umožňuje použití ControlNetu ve výbušném prostředí.

ControlNet opět vychází ze základního modelu ISO/OSI. Vrstvy 1 – 4 jsou tvořeny komunikačními standardy ControlNetu a vrstvy 5 – 7 jsou realizovány protokolem CIP, stejně jako u EtherNetu/IP, DeviceNetu a CompoNetu, viz předchozí kapitoly. Hierarchie rozložení modelu komunikace viz Obr. 2-9.

[42] Unconnected message manager

[43] Primární i sekundární vedení, při poruše lze volně přecházet z jednoho na druhé.



Obr. 2-9 ControlNet v modelu ISO/OSI [7].

2.5.1 ControlNet fyzická vrstva

ConrolNet používá jako přenosové médium koaxiální kabel[44] [2]. Tento kabel je sice levný, velice odolný vůči rušení a dostupný, nicméně každý terminál je na konci zakončen odporem 75Ω. Toto zakončení vnáší do sítě útlum a to má za následek snížení délky hlavního vedení s každou odbočkou o cca 16,3 m. Pro dosažení vyšší délky vedení je nutno použití opakovačů.

ControlNet umožňuje použití až 20 opakovačů v sérii, čímž můžeme dosáhnout efektivní délky vedení až 20 km. Koaxiální kabel může být zakončen buď BNC konektorem s IP 20[45] nebo TNC s IP 67 a dalšími.

2.5.2 ControlNet CTDMA

ControlNet používá protokol CTDMA[46] [7], který zajišťuje přesný čas dodání zprávy. Princip je založen na pravidelném, neměnném opakování cyklu pro aktualizaci sítě[47]. Při opakování se neustále opakují sekvence pro plánované, neplánované a pásové přístupové časy. Každý uzel v síti obsahuje časovač synchronizovaný se sítí, s možností konfigurace cyklu opakování 2 – 100 ms. Přiřazení času synchronizace cyklu opakování do jednotlivých uzlů provádí moderátor pomocí MAC rámce.

---

[44] RG-6

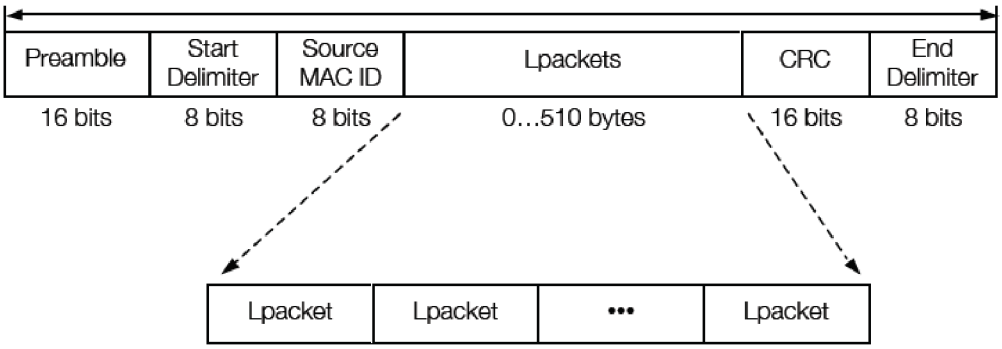
[45] Stupeň ochrany proti vniknutí cizího předmětu a kapaliny.

[46] Concurrent time domain multiple access.

[47] NUT (Netvork update time).

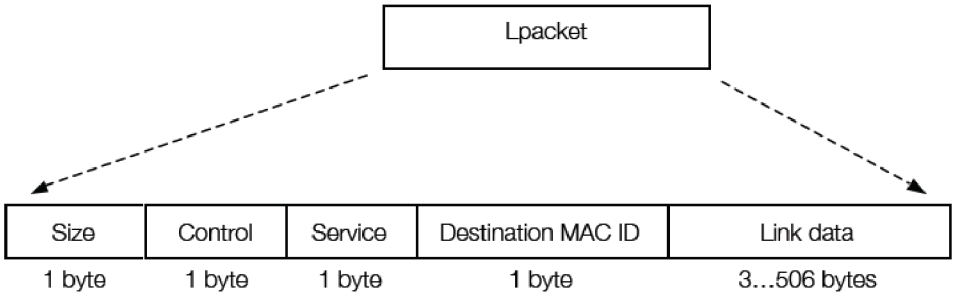
Každý MAC rámec obsahuje až 510 bitů pro data, která jsou vyplněna link packety. Link packety nesou specializované zprávy I/O nebo CIP. Všechny uzly v síti vždy slyší. Všechny MAC rámce umožňují multitaskingový přenos malého objemu dat, viz Obr. 2-10.

Link packetů existují dva druhy. Pevný tag link paket, který umožňuje zaslání zprávy na určité MAC ID, tento druh se používá například na správu sítě, viz Obr. 2-11 Druhý typ je generovaný tag link paket s určitým ID uzlu, při shodě ID se data předají další vrstvě, když se ID neshoduje s ID uzly, zaslaná data jsou ignorována, viz Obr. 2-12.



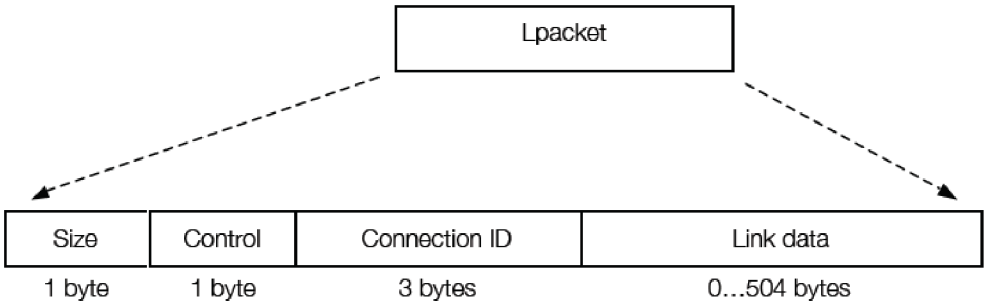
Obr. 2-10 MAC rámec ControlNet [2].

Preamble *(Úvod)* – startovací kód rámce.
Start Delimiter *(Začáteční oddělovač)* – usnadňuje identifikaci nového rámce.
Source MAC ID *(Zdrojové ID)* – MAC ID uzlu.
Lpackets *(Lrám)* – rámec pro přenos dat nebo zpráv.
CRC *(Kontrola cyklic. nadbytečnosti)* – bezpečnostní pole pro detekci chyb v datech.
End Delimiter *(Koncový oddělovač)* – odděluje konec rámce od začátku dalšího.



Obr. 2-11 Pevný tag-link paket [2].

Size *(Velikost)* – počet slov v rámci.
Control *(Nastavení)* – určuje typ Lpacketu.
Service *(Servis)* – nastaveni konfigurace.
Destination MAC ID *(Lokalita MAC ID)* – MAC adresa cíle přenosu dat.
Link data *(Data)* – obsahuje slova/data.



Obr. 2-12 Generovaný tag link paket [2].

Size *(Velikost)* – počet slov v rámci.
Control *(Nastavení)* – určuje typ Lpacketu.
Connection ID *(Lokalita MAC ID)* – určuje, zda přijmout nebo ignorovat data.
Link data *(Data)* – obsahuje slova/data.

2.5.3 ControlNet transportní vrstva

Transportní vrstva ControlNetu [7] slouží stejně jako u modelu ISO/OSI k přepravě zpráv do vyšších vrstev. Pro vytvoření spojení jsou potřeba minimálně dva účastníci autorizátor[48] a cíl.

Spojení můžou být nespojené a spojené. Nespojené má malou prioritu, může je číst každý účastník a zpracovává je správce nespojených zpráv. Druhým typem je spojené spojení, používá se pro přímé spojení pomocí identifikátoru pro častý přenos mezi dvěma uzly.

ControlNet dělí zprávy na síti do tří tříd [7] zpráv, adaptérů a skenerů. Každá z těchto tří tříd má své specifikace. Třída zpráv slouží k podpoře neplánovaných explicitních zpráv obou typu spojení z I/O modulů[49]. Třída adaptérů zahrnuje moduly, které dostávají neplánovaně data z modulů[50] ostatních tříd a mohou neplánovaně data odesílat. Třída skenerů slouží k plánování přenosu dat z real-time modulů[51].

[48] Účastník, který žádá o vytvoření spojení.
[49] Karty PLC, rozhraní počítače, roboti, SW aplikace bez odpovědí v reálném čase.
[50] Adaptér I/O, svářečky, pohony, HMI.
[51] Řídící jednotky PLC, karty pro ovládání PC, I/O adaptéry a karty pro ovládání robotů.

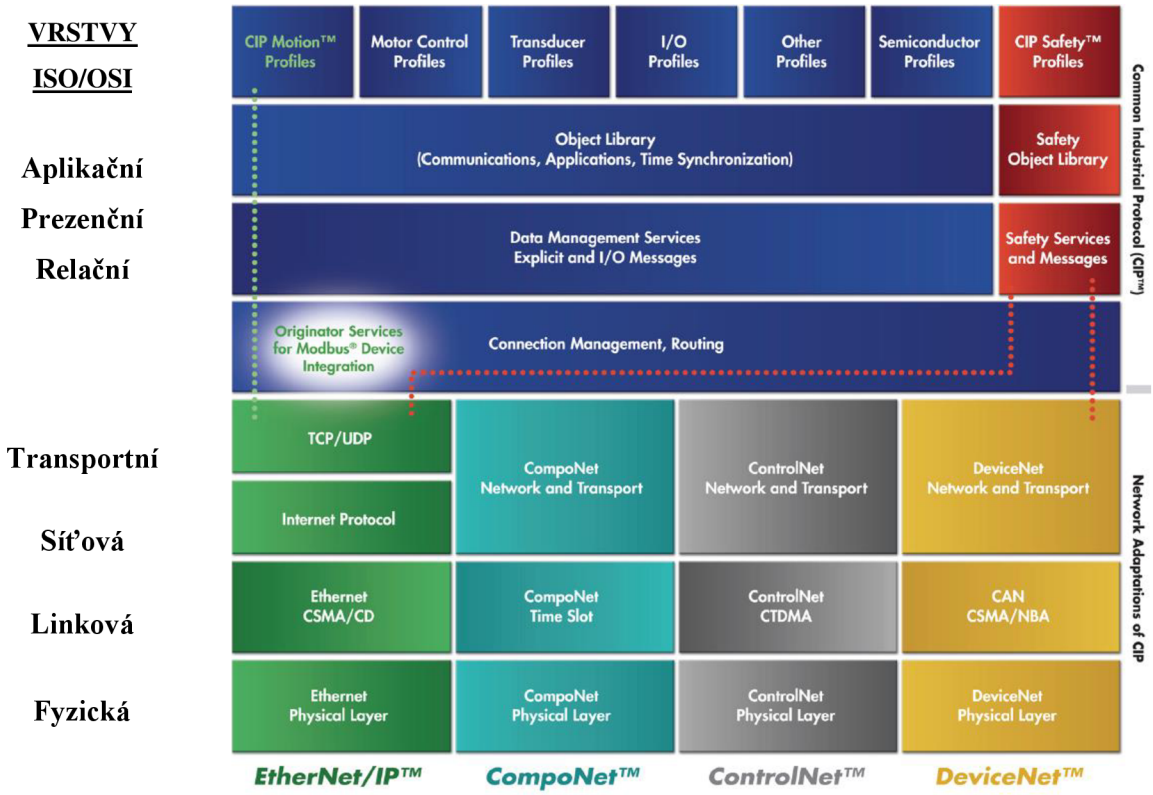
3 COMMON INDUSTRIAL PROTOCOL™

Common industrial protocol [8] dále pouze CIP, vyvíjí a zpravuje organizace ODVA[52]. ODVA je asociace složená z předních firem zabývajících se průmyslovou automatizací. Cílem organizace je vývoj norem a použití komunikačního protokolu CIP v síťových komunikacích EtherNet/IP™, DeviceNet™, CompoNet™ a ControlNet™. Neustálý vývoj a nárůst potřeb uživatelů má za následek komplexní rozšiřování samotného protokolu.

Hlavní myšlenkou [2] CIP je vzájemné propojení všech čtyř, výše uvedených, síťových komunikací jedním komunikačním protokolem se zahrnutím zpráv pro sběr dat, řízení, bezpečnost, energii, synchronizaci, pohyb, diagnostiku atd. Tyto a další vlastnosti dělají protokol CIP velice univerzálním.

3.1 Popis vrstev

Protokol CIP reprezentuje tři nejvyšší vstvy [2] modelu ISO/OSI a propojuje všechny čtyři výše uvedené síťové komunikace viz Obr. 3-1. Díky využití standardu ISO/OSI je možné protokol snadno rozšířit o nové síťové spojení a protkoly na bázy prvních čtyř vrstev modelu.



Obr. 3-1 CIP v modelu ISO/OSI [2].

[52] Open DeviceNet vendors association.

3.1.1 Spojení a směrování

Spojení [2] mezi různými objekty v CIP protokolu probíhá za pomocí ID nebo CID[53]. Formát CID závisí na síti, které se to týká. Při obousměrné výměně dat jsou potřeba CID uzly cíle i zdroje.

Při vytvoření prvotního spojení je zaslána UCMM Fovard_Open zpráva. Tato zpráva se odešle všem zařízením, obsahuje informace pro vytvoření spojení s cílovým uzlem. Nezbytnými informacemi je myšlena délka časového limitu spojení, CID cíle, ID zdroje, maximální velikost zprávy, spouštěcí mechanizmy, elektronické klíče, cesta k datům a objektům, konfiguraci spojení a směrovací informace při spojením s uzly v jiné síti.

Směrování zpráv [2] je proces dopravy zprávy ze zdroje do cíle. Můžeme použít dva druhy směrování zpráv, nesouvisející směrované zprávy a související směrované zprávy. Související směrované zprávy neobsahují trasu k cílové stanici, ale pouze adresu cílové stanice.

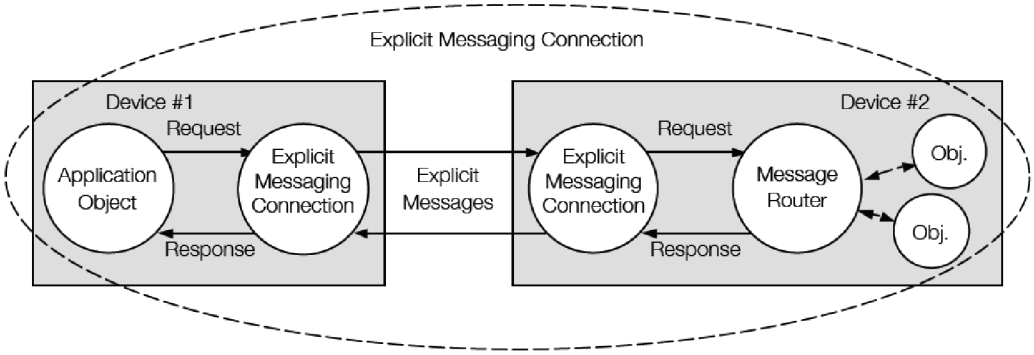
Nesouvisející směřované zprávy můžou být směřovány a odeslány z jednoho uzlu CIP sítě do jiné CIP sítě. Uvnitř explicitních zpráv je zakódován mechanizmus transportu, který obsahuje veškeré informace o přenosu a trasu směrování. Tyto informace putují společně se zprávou z routeru do routeru. Při přijetí zprávy routerem je vždy kousek trasy k cílové stanici odmazán, ale router čeká na potvrzení přijetí od další stanice. Po přijetí zprávy cílovým uzlem odesílá potvrzení zpět do předchozího routeru a kaskádovitým způsobem se informace o přijetí dostane k prvnímu odesílateli.

3.1.2 Komunikační objekty

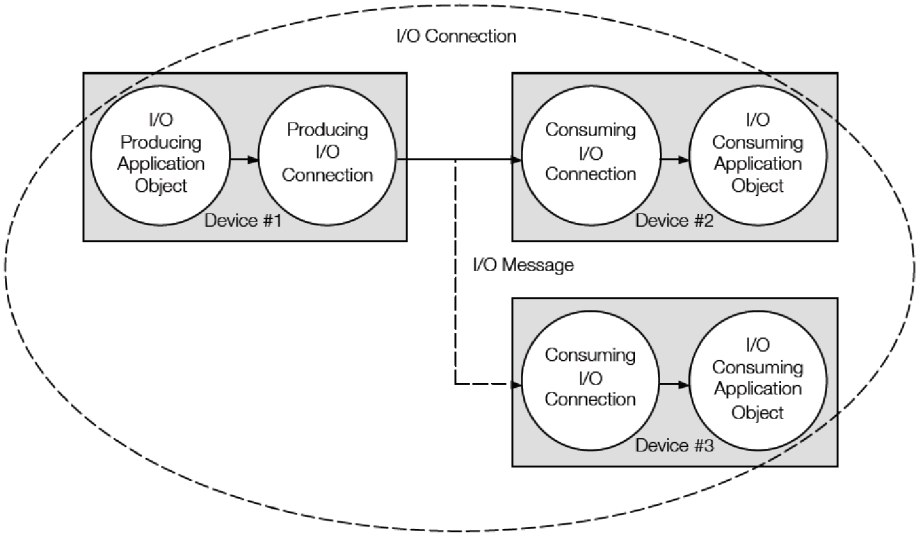
Komunikační objekty [2] jsou při zasílání zpráv jediným bodem přístupu do celé CIP sítě, obsahují část producent, konzument nebo obojí. Důležitý je typ spojení, který definuje mechanizmy zprávy. Můžeme mít připojení explicitní nebo I/O.

Explicitní spojení udává cesty mezi dvěma zařízeními s možností více účelů. Standardně je komunikace orientována typem požadavek/odpověď. Zpráva striktně stanovuje jakému zařízení a s jakou službou má být doručena. Tento druh zprávy vždy prochází přes směrovač, viz Obr. 3-2. Mechanismus odesílání I/O zprávy více zařízením viz Obr. 3-3.

[53] Connection identifier.



Obr. 3-2 Schéma explicitního přenosu zprávy [2].



Obr. 3-3 Schéma I/O zasílání zprávy více zařízením [2].

3.1.3 Knihovna objektů

Základem protokolu je tzv. knihovna objektů [2] díky, které spolu mohou různé systémy spolupracovat. Jednotlivé uzly v síti jsou modelovány jako skupiny objektů, když uzel není namodelován tak, pro protokol neexistuje. Objektů existují dva druhy, veřejné objekty[54] a specifické objekty[55]. Objekty se dále dělí do tříd dle jejich vlastností a funkce v síti. Tyto třídy se dále dělí na instance a příznaky[56]. Instance ve třídě obsahují objekty se stejnými příznaky, avšak obsahují i svoje vlastní příznaky. Taktéž třída obsahuje vlastní příznaky samotné třídy, které nesou informace o počtu objektů, instancí a příznaků třídy.

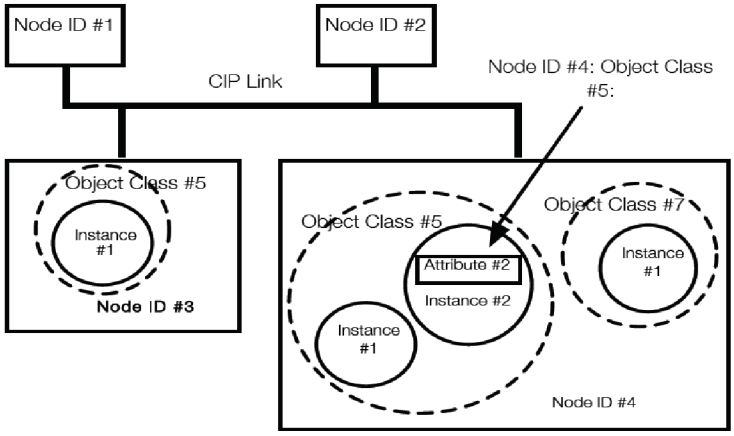
Identifikace objektů je závislá na druhu použité sítě. Používá se MAC nebo IP adresace, viz předchozí kapitoly. Každá třída, objekt, instance a příznak má své identifikační celočíselné ID pro identifikaci. Tyto parametry, společně s kódem služby,

[54] Objekty předefinované v knihovně ODVA.

[55] Specifické objekty, které si uživatel definuje sám.

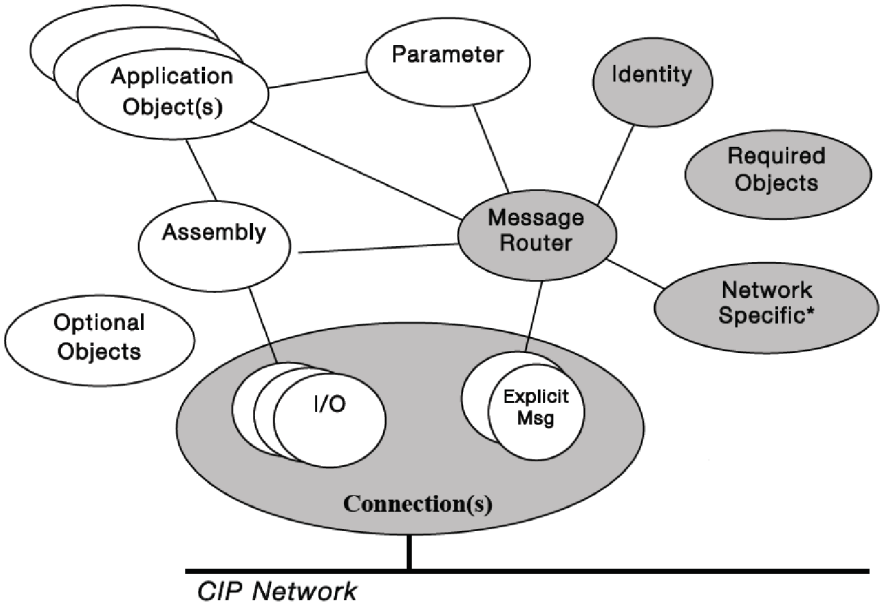
[56] Atributy.

který určuje činnost objektu, slouží k adresaci a řízení činnosti objektů. Adresování je buď 8, 16 nebo 32 bitové, obvykle stačí 8 nebo 16 bitů. Grafické znázornění struktury adresace viz Obr. 3-4.



Obr. 3-4 Struktura rozdělení adresace a tříd CIP [2].

Třídy dělíme na tři skupiny [2]. Těmi jsou objekty obecného, aplikačního a síťového použití. Mezi objekty obecného použití patří například message router, konfigurace připojení, identita, port, registr atd., jednoduše objekty, které jsou v typické CIP síti. Další třídou jsou aplikační objekty, které si uživatel volí sám na základě projektu nebo aplikace, pro kterou je síť vytvářena, například analogové nebo diskrétní I/O výstupy, motor data, motion device osy, safety komponenty atd. Poslední třídou jsou síťové objekty, kde spadají různé opakovače, switche, TCP/IP interface, EtherNet/CompoNet/ControlNet linky atd. Typický objektový model CIP sítě byl zobrazen na Obr. 3-5.



Obr. 3-5 Objektový model CIP sítě [2].

Optional Objects *(Volitelné obj.)* – bíle podbarvené objekty jsou nepovinné.
Requied Object *(Povinné obj.)* – šedě podbarvené objekty jsou povinné.

Connection(s) *(Spojení)* – spravuje druhy spojení přijímaných/odesílaných zpráv.
Network Specific *(Síťové specifikace)* – objekty definují konfiguraci dané sítě.
Application Object *(Aplikační obj.)* – specifické objekty daného projektu/aplikace.
Message Router *(Router zpráv)* – specifikuje předání žádostí explicitních zpráv ostatním objektům.

Assembly *(Shluk)* – objekt pro mapování dat z příznaků jiných tříd. Využívá se pro nalezení maximální účinnosti řídících dat ve třídách I/O zpráv. Jinými slovy, mapuje instance s méně objekty a příznaky, které nepotřebují rozsáhlé přenosy dat [2].

Parametr *(Parameter)* – objekt spravující parametry pro konfiguraci, existuje několik reprezentací a to v tištěné podobě, EDS[57] zkrácené/plné verzi nebo kombinací těchto metod. EDS je ASCII[58] textový soubor poskytující informace o prvotní konfiguraci a I/O připojení zařízení, který je uložen v interní paměti. Tyto parametry se dají ze zařízení vyčíst pomocí specializovaného software, čímž usnadňují sledování, konfiguraci a řízení [2].

Identity ***(Idetita)*** – objekt spravující identifikaci zařízení v síti, každé zařízení musí mít alespoň jeden, obsahuje povinné parametry (status, sériové číslo, jméno výrobku, revizi, kód produktu, typ zařízení, vendor ID[59]) [2].

3.1.4 Profily

Na Obr. 3-1 jsou viditelné různé druhy profilů [2] aplikační vrstvy CIP protokolu např. CIP Motion, Motor Controler, I/O, Order, CIP Safety atd. Tyto profily vznikly seskupením zařízení s podobnými vlastnostmi do skupin. Takové seskupení mnohonásobně zjednodušilo algoritmus přidělování ID. Profily obsahují komplexní popis datové i řídící struktury sdružení.

Rozdělení do kategorií se provádí pomocí ID dodavatele zařízení, které je dostupné v knihovnách protokolu. Při neznámém ID musí být zařízení přiřazeno do profilu Generic nebo Vendor-specific. Informace typu do jakého profilu zařízení přidělit, s jakými povinnými parametry atd. musejí být dohledatelné v dokumentaci k danému zařízení.

[57] Electronic data sheet.
[58] American standard code for information interchange.
[59] ID dodavatele, který prodává dané zařízení.

Profily se skládají z několika objektů s různými typy datových formátů a struktur. Ovšem neustálý vývoj nelze zastavit, proto mají uživatelé možnost vytvořit si vlastní profil v libovolném rozsahu. Tuto funkci podporuje i samotná organizace ODVA, která založila samostatnou skupinu SIGs[60] zabývající právě rozšiřováním protokolu o nové profily a podporovaná zařízení.

3.2 CIP rozšíření

CIP komunikační protokol nabízí spoustu funkčních rozšíření, které byly odvozeny z potřeb průmyslové automatizace.

Mezi tyto rozšíření patří nástavby určené pro řízení akčních členů a pohonů CIP Motion společně s CIP sync pro řízení v reálném čase. Dále také nástroj pro optimalizaci a úsporu energií CIP Energy. Předposlední částí je CIP Specification library, což jsou velmi podrobné technické texty o rozšířeních, úpravách a novinkách protokolu CIP. Celou skupinu uzavírá CIP Security, který řeší zabezpečení na úrovni všech vrstev, ovšem toto rozšíření je teprve ve vývoji.

3.2.1 CIP Energy

Rozšíření CIP Energy [2] slouží k optimalizaci toku energie při řízení procesu. Umožňuje diagnostiku a přenos komplexních informací o energetických tocích na úrovni všech vrstev. Slovem energie jsou myšleny elektrické veličiny i neelektrické[61] veličiny. Existují čtyři základní skupiny dělení objektů, kterými jsou základní energetický, elektrický, neelektrický a napájecí objekt.

Základní energetický objekt poskytuje energii do sítě CIP. Rozděluje, mapuje a měří různé energetické hladiny. Dále informuje o jejich stavech v síti. Umožňuje měření výkonu, napěťových úrovní a délky řídících pulzů na několika místech současně. Přistupuje k objektu jako k celku.

Elektrický objekt dodává data o stanici a data určená pro diagnostiku stanice na úrovni všech vrstev. Použití v kombinaci se základním energetickým objektem uživateli poskytne širokou škálu čtení veškerých informací o energii.

Neelektrické objekty mají stejnou funkci jako elektrické objekty s tím rozdílem, že se používají pro měření a diagnostiku neelektrických veličin.

Napájecí objekt umožňuje zpravovat napájení stanic v síti pomocí standardizovaných služeb. Zpravuje různé energetické profily, jako jsou režimy spánku, různé úsporné stavy, kontroly I/O odběrů, pozastavení, úplné vypnutí, či optimální nabití atd.

---

[60] Special interest groups.

[61] Páry, plyny, kapaliny, stlačený vzduch, oleje paliva a jiné.

3.2.2 CIP Sync

CIP Sync [2] se používá pro real-time aplikace s absolutní synchronizací a rychlostí komunikace menší než 250 ns. Typickým použitím jsou senzorové vstupy, koordinace pohybu v reálném čase včetně přenosu dat mezi master a slave stanicí.

Funkčnost zařizuje prioritní rozdělení zpráv. Sync zprávy mají vyčleněny časově přesné prioritní rámce pro komunikaci, viz předcházející kapitoly. Díky tomu se mohou přenášet přes běžná média a v jedné síti společně s běžnými zařízeními.

Rozšíření vychází ze standardu IEEE-1588-2008[62] a je s ním plně kompatibilní. Zmíněný standard funguje na principu předání přesné časové struktury ze stanice master do stanic slave po celé hierarchii sítě pomocí multicasting zprávy. Kompenzace vzniklého zpoždění vůči vzdálenějším stanicím je možná, protože v nižších vrstvách zachytíme informaci o dokončení přenosu zprávy. S touto informací pak můžeme aktualizovat přesný čas z master stanice.

CIP sync podporuje pouze UDP/IP zprávy, jelikož rámec je jednoduchý a umožňuje rychlý přenos, viz předchozí kapitoly. Zároveň je dané rozšíření zapracováno pouze do sítě Ethernet/IP. Do zbylých CIP sítí bude zapracován v budoucnu.

3.2.3 CIP Motion

CIP Motion [2] slouží k řízení pohonů, motorů, servopohonů, měničů, krouticích momentů atd. Řízení probíhá pomocí Motion Profile, což je struktura, která nese základní parametry o diagnostice, inicializaci a konfiguraci daného pohonu, viz předcházející kapitoly.

Pohyby lze řídit pomocí moderních technologií s přesností na setiny. Podpora deterministického řízení komponentů pro řízení v reálném čase se CIP Motion spojí s technologií CIP sync. Podpora je zatím pouze u zařízení s Ethernet/IP.

3.2.4 CIP Security

Za vznikem CIP Security [9] stojí neustále se zvyšující hrozba útoku neznámým softwarem na samotná zařízení. CIP Security je založeno na principu ochrany na více vrstvách zároveň, tím pádem je daleko složitější prolomit obranu, až k samotnému řízení procesu.

Zařízení s tímto bezpečnostním protokolem by mělo být schopno odmítnout data a zprávy z nedůvěryhodných zdrojů, čili by mělo docházet k ověřování pravosti a kontrole integrity. Podporu tzv. bezpečnostního profilu, ve kterém budou definovány

[62] Standard for a precision clock synchron. protocol for networked measurem. and control sys.

bezpečnostní funkce, oprávnění přístupů a rozpoznání úrovní zabezpečení u jiných zařízení.

V současnosti je CIP Security ve fázi vývoje, který se zaměřuje na zařízení připojené pomocí EtherNet/IP. Zabezpečení spočívá v autentizaci a integritě koncových bodů[63], šifrování zpráv a ochraně proti jejich zneužití nebo vnějšímu zásahu.

3.2.5 CIP Specification libraly

CIP specification libraly [10] je soubor článků pojednávajících o rozšíření technologií vzniklých na podmět odběratelů.

Články má na starost již výše uvedená zájmová skupina SIG. Tato skupina přednese návrh rozšíření vedení ODVA a po jeho schválení na něm začne pracovat. Po dokončení práce je daná specifikace opět předložena expertům ODVA a po opětovném schválení se teprve doplní do knihovny specifikací. Tuto knihovnu mají odběratelé k dispozici pouze po jejím předplacení. Je aktualizována 2x ročně a obsahuje podrobné popisy nových rozšíření CIP protokolu.

[63] Porovnání pomocí certifikátů (klíčů) cíle/zdroje.

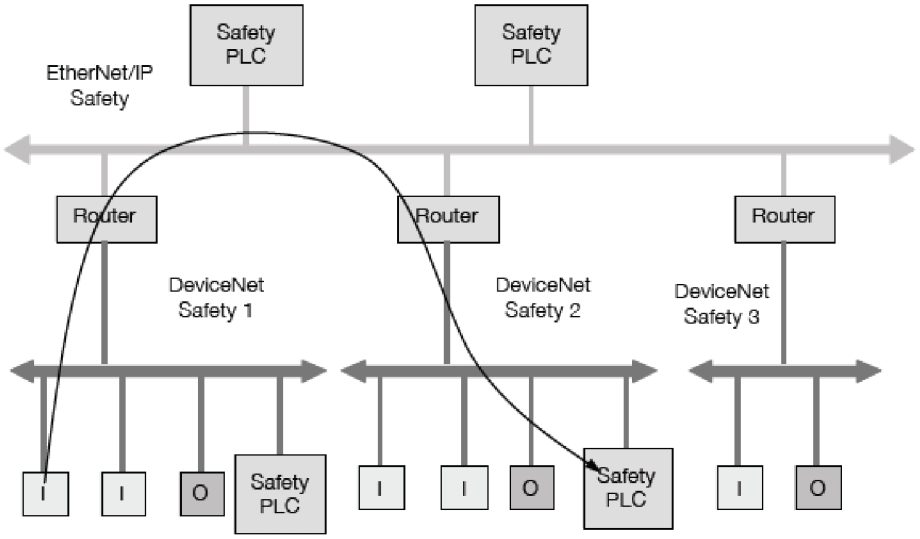
4 CIP SAFETY

S neustále se zvyšujícími nároky na bezpečnost obsluhy i strojů v průmyslu, byl komunikační protokol CIP rozšířen o CIP Safety [2]. Rozšíření je prozatím podporováno pouze v sítích EtherNet/IP, DeviceNet. CIP Safety vkládá do komunikačního protokolu přesně definované, nezávislé vrstvy s bezpečnostními funkcemi, bez nutnosti složitého nastavování a řízení bran. Vrstvy obsahují několik bezpečnostních profilů a objektů s implementovanými funkcemi.

Rozšíření zároveň umožňuje současně použít standardní zařízení a zařízení s bezpečnostními funkcemi v jedné síti. Při použití zařízení s CIP Safety stroj splňuje nároky na normy ČSN EN 62061 (Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností SIL[64] 3) a ISO 13849-1 (Bezpečnost strojních zařízení – Bezpečnost části ovládaných systémů Část 1: Všeobecné zásady pro konstrukci kategorie 4, PL[65] e).

CIP Safety [2] vyžaduje redundantní zapojení všech kanálů, jediné neredundantní zapojení je možné u datových linek komunikačního rozhraní a to z důvodu zachování integrity standardních CIP sítí. Díky tomu je možné použití standardních směrovačů k přenosu dat týkajících se bezpečnosti.

Při vzniku chyby přenosu nebo údajů musí koncové zařízení přijmout opatření, protože je zodpovědné za detekci chyb a integritu přenášených dat. Tento způsob směrování umožňuje vytvoření bezpečnostních buněk v různých sítích, zachování rychlých reakčních časů, snížení šířky pásma a zasílání multicast bezpečnostních zpráv napříč sítěmi. Grafické znázornění směrování buněk napříč více sítěmi viz Obr. 4-1.



Obr. 4-1 Směrování bezpečnostních buněk [2].

[64] Safety integrity level.

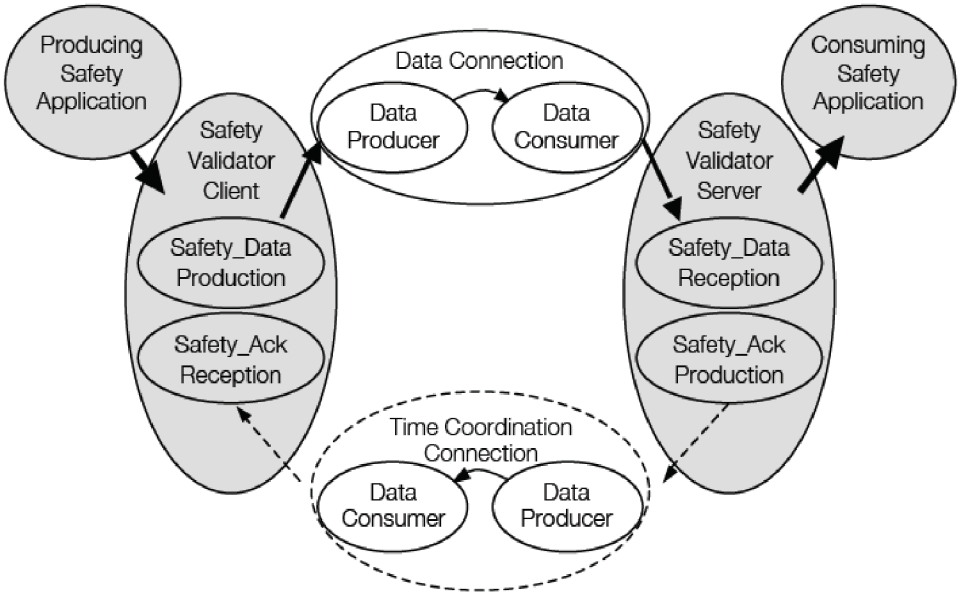
[65] Performance level.

4.1 Validátor

Jak bylo uvedeno výše, základní funkce a principy CIP komunikačního protokolu jsou zachovány, tudíž je nutné rozlišit safety objekty. Toto rozlišení a další specifikaci zajišťuje validátor.

Validátor [2] je mezi prvek, který realizuje spojení mezi safety objekty a spojovou vrstvou klasické CIP sítě. Jeho funkcí je vyrábět bezpečnostní data, zajistit dobu koordinace objektů, dat a časových zpráv. Dále provádí kontrolu údajů, přijímaní údajů, zajišťuje, aby výrobci odkazů a spotřebitelé neměli znalosti o bezpečnostním paketu. Celkově má validátor zodpovědnost za vysokou integritu, kontrolu dat a detekci chyb uvnitř bezpečnostní části sítě.

Na Obr. 4-2 byla znázorněna funkce validátoru. Producent bezpečnostní aplikace použije objekt klient validátor pro vytvoření bezpečnostních dat a zajištění doby koordinace. Přes producenta dat se zajistí časová koordinace a přenos dat do stanice konzument. Objekt klient server zkontroluje integritu časové koordinace a dat, při bezchybném přenosu odešle data do cílové stanice.



Obr. 4-2 Znázornění funkce validátoru [2].

CIP Safety nezabrání chybám komunikace [2], ale zajišťuje integritu přenosu. Odhaluje tyto vzniklé chyby a umožňuje zařízením patřičně reagovat. Validátor pomocí pěti prostředků detekuje 9 základních chyb. Tyto chyby a jejich detekce daným prostředkem jsou uvedeny v tabulce Tab. 4-1.

Tab. 4-1 Tabulka Znázornění opatření pro detekci chyb [2].

Chyby	Opatření pro detekci				
	Čas očekávání (časové razítko)	ID odesílatele a příjemce	Bezpečnostní CRC	Redundance s kontrolou	Jiná opatření
Opakování zprávy	x		x		
Ztráta zprávy	x		x		
Vložení zprávy	x	x	x		
Sekvence zprávy	x		x		
Korupce zprávy			x		
Zpoždění zprávy	x		x	x	
Spojování bezpečnostních a bezpečných dat		x			
Spojování bezpečnostních a standardních dat	x	x	x	x	x
Zvýšení stáří dat	x				

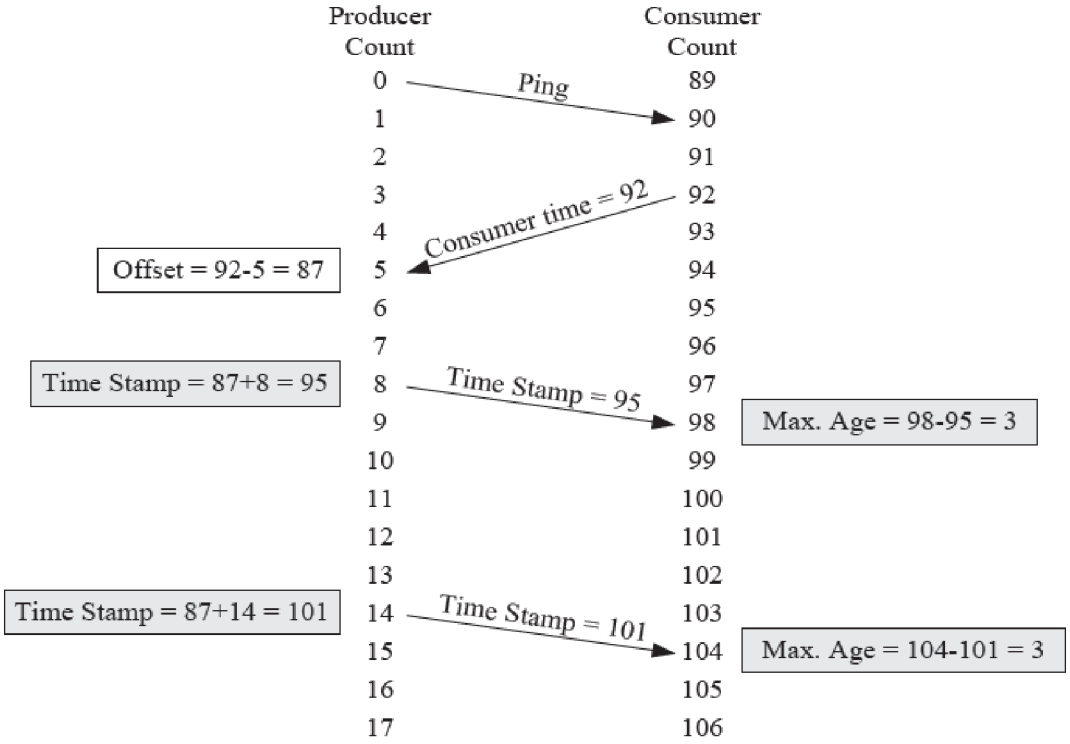
4.1.1 Čas očekávání

Doba neboli čas očekávání [2] je monitorován prostřednictvím časového razítka. Všechny bezpečnostní data obsahují časovou značku (časové razítko). Tato časová značka umožňuje přenos dat, sledování stavu fronty, sledování počtu opakování, detekci zpoždění směrovačů, určení stáři dat atd.

Přenosy a jiné aktivity v síti jsou koordinovány tzv. požadavkem na ping[66] mezi producentem a konzumentem. Producent naváže spojení s konzumentem, poté producent odešle požadavek na ping konzumentovy a uloží tuto odezvu jako offset[67]. Producent takto získaný offset přičte ke svému internímu času a tato hodnota je vystavena jako časové razítko, které se váže k přenosu. Stáří dat určuje konzument odečtením svého interního času od časové značky, jestliže je aktuální stáří dat je vyšší než maximální povolené stáří dat, konzument vyhodnotí chybový stav a provede příslušná opatření. Grafické znázornění koordinace času a určení stáří dat je uvedeno na Obr. 4-3.

[66] Doba odezvy stanice.

[67] Posun (odezva – čas přijetí odezvy).



Obr. 4-3 Časové razítko producent / konzument [2].

4.1.2 Produkční identifikátor

Produkční identifikátor [2], dále jen PID, reprezentuje jedinečný elektronický kód bezpečnostního zařízení v síti. Může být složen například ze sériového čísla, elektronického klíče, výrobního čísla a podobně. PID je přenášeno u veškerých dat a udává ID cílového zařízení.

Při obdržení dat stanicí s rozdílným PID nebo neobdržení dat v předepsaném časovém intervalu jsou tyto stavy vyhodnoceny jako chyby. Slouží ke kontrole zpráv v síti.

4.1.3 Bezpečnostní CRC a kontrola

Bezpečnostní CRC [2] zajišťuje detekci možného poškození dat v přenášeném paketu. Tato kontrola je prováděna pouze u producenta a konzumenta[68], v průchozích směrovačích nikoliv. Umožňuje detekci chyb rušením, fragmentací nebo nekvalitním spojením.

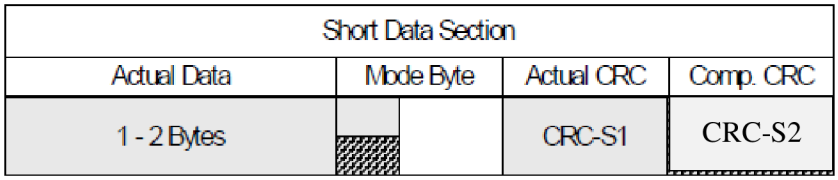
Datové pakety jsou zabezpečeny 1 CRC a 2 CRC, které zajistí vysokou integrity přenosu a dostačující mechanismus zabezpečení. Ke kontrole [2] dat slouží zvláštního sektoru paketu s obráceným obrazem dat.

[68] Metoda: End-to-end.

4.1.4 Bezpečnostní telegram

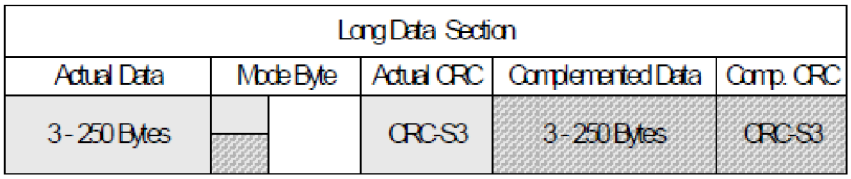
Bezpečnostní telegramy [11] se skládají ze čtyř dílčích paketů (data, časové razítko, časová korekce a časová koordinace). Tyto části jsou za sebou řazeny a vzniká bezpečnostní telegram. Každá část obsahuje data a své CRC.

Datové pakety [11] mohou mít dvě podoby, krátký formát a dlouhý formát. Krátký formát slouží jako primární a skládá se z 1-2 bytů bezpečnostních dat, mode bytu, 8 bitů CRC a 8 bitů obráceného obrazu CRC. Grafické znázornění viz Obr. 4-4.



Obr. 4-4 Bezpečnostní paket krátký formát [11].

Dlouhý formát přenáší 3 až 250 bytů dat s vysokou integritou přenosu. Skládá se z 3 - 250 bytů dat, mode bytu, 16 bitů sloučeného CRC a obráceného CRC, obráceného obrazu dat a obráceného obrazu sloučených CRC. Grafické znázornění viz Obr. 4-5.



Obr. 4-5 Bezpečnostní paket dlouhý formát [11].

Časové razítko [11] má jednotný formát a obsahuje pouze byty nesoucí samotný čas a byty CRC. Paket obsahující časovou korekci se používá pouze u multicast zpráv, obsahuje individuální nastavení korekce násobků časů spotřebitelů a kontrolní CRC. Poslední částí je paket časové koordinace, který nese taktéž časové údaje od producentů a konzumentů.

5 LABORATORNÍ ÚLOHA

V následující kapitole budou uvedeny základní komponenty dostupné v bezpečnostní laboratoři, ze kterých následně vytvořím laboratorní úlohu. Cílem návrhu úlohy bude seznámení se s technickou dokumentací komponentů podporujících komunikační protokol CIP Safety, vyhledání příslušných elektrických zapojení, formulace zadání, fyzická montáž, propojení komponentů tak, aby studenti měli k dispozici funkční laboratorní panel osazený dostupnými komponenty a následně mohli vytvořit vlastní SW řešení úlohy.

5.1 Komponenty

V bezpečnostní laboratoři jsou k dispozici komponenty výhradně od firmy Rockwell a Allen-Bradley. Základním prvkem celého řízeného systému je bezpečnostní automat.

K realizaci úlohy mi byl přidělen model 1756-L62S od firmy Allen-Bradley. Jedná se o starší model modulárního automatu, který je osazen GuardLogix procesorem s 4MB klasické paměti a 1MB safety paměti. Celý automat je vsazen do kovového, čtyř modulového rámu opatřeného vlastím stejnosměrným 24V zdrojem. Moduly, tzv. karty se dají v rámu libovolně měnit dle potřeby a nabídky výrobce. Protože je automat opatřen připojením přes EtherNet/IP, budou použity komponenty výhradně s tímto rozhraním.

Řízený systém se bude skládat z několika hlavních komponentů s podporou sítového rozhraní EtherNet/IP a to z: modulu pro připojení bezpečnostních POINT I/O, multifunkčního přístupového bloku, bezpečnostních relé, frekvenčního měniče a 8 portového switche. Dále mám k dispozici třífázový motor, bezpečnostní zámek, optickou závoru a bezpečnostní tlačítko.

Kompletní seznam použitých komponentů byl, pro vyšší přehlednost, uveden v Tab. 5-1 a Tab. 5-2. Bližší popis a rozbor bude uveden v kapitole č. 6.

Tab. 5-1 Tabulka použitých komponentů bez EtherNet/IP

Komponenta	Katalogové označení
Bezpečnostní závora	450L-APU-UN-8
Zámek	440G-LZ
Bezpečnostní tlačítko	Nouzové tlačítko hříbek NO/NC
3 fázový motor	4AP90L (nástupce 1LE1002)
Laboratorní zdroj 24V	DIAMETRAL P230R51D

Tab. 5-2 Tabulka použitých komponentů s EtherNet/IP

Hlavní - komponenta	Pod - komponenta	Slot	Katalogové označení
Automat	-	-	1756-L62S
	Procesorová karta	(00)	1756-L62S Logix5562
	Bezpečnostní partner	(01)	1756-LSP
	Ethernetová karta 1	(02)	1756-ENBT/A (1 port)
	Ethernetová karta 2	(03)	1756-EN2TR/C (2 porty)
EtherNetová karta relé	-	-	440R-ENETR
	DIS Safety relé	(01)	440R-D22R2
	EM Safety relé	(02)	440R-EM4R2
Bezpečnos. POINT I/O modul	-	-	1734-AENTR 24V DC
	8 bezpeč. vstupů	(01)	1734-IB8 24V DC 8 Point
	8 bezpeč. výstupů	(02)	1734-OB8 24V DC 8 Point
Multifunkční přístupový blok	-	-	442G-MABR-UT-C03
Frekvenční měnič	-	-	PowerFlex525 1P 240V
Switch 8 portů	-	-	Hirshmann RS2-FX/FX

5.2 Software nástroje

V laboratoři mám k dispozici SW RSLogix 5000 a RSLinx, což jsou SW nástroje potřebné k navržení HW konfigurace a SW řešení.

5.2.1 RSLinx a RSLogix 5000

SW RSLinx slouží k mapování komponentů připojených do sítě. Díky tomuto nástroji získáme přesné informace o HW připojeném na síti, které jsou potřebné k vytvoření funkční HW konfigurace. Zobrazuje informace typu IP adresa, přístupová brána, výrobce, sériové číslo, revize a typové označení produktu, umístění modulu, typ komunikace, počet portů atd. Získané informace se liší od typu použitého HW. Některé z nich lze samozřejmě editovat a konfigurovat. Zjednodušeně RSLinx pracuje tak, že odešle broadcast zprávu do sítě s žádostí o autorizaci viditelných zařízení. Dostupná zařízení zašlou zpět potřebné informace a RSLinx podle nich vyhledá produkt ve své interní databázi.

SW RSLogix 5000 slouží k tvorbě logiky programu pro řízení systému. Je to stěžejní SW pro programování automatů. Tvoří se v něm HW konfigurace, logika

klasického i safety programu, definice proměnných, mapování I/O modulů a další procedury. Můžeme zde nastavovat a parametrizovat jednotlivé periferní komponenty. Podporuje programování v ladder diagramu, funkčních blocích, strukturovaném textu, tak i sekvenčním grafu. K usnadnění programování se používají předdefinované bloky funkcí. Uživatel si taky může funkce definovat sám. Celý program jedním kliknutím nahrajete do automatu a v online režimu můžete sledovat jeho průchod.

5.2.2 Factory I/O

Úlohu je potřeba vhodně vizualizovat. Ve školní laboratoři je k dispozici SW FactoryTalk. Nicméně tento SW nástroj neumožnuje nějakou pokročilejší a interaktivní 3D vizualizaci. Proto jsem na webu hledal vhodnější variantu.

Při hledání jsem objevil SW „Factory I/O" [12] od společnosti Real Games. Společnost sídlí v Portugalsku a přes 10 let vyvíjí 3D SW pro vzdělávací účely. Zároveň spolupracuje s více než 30 světovými distributory nejen v oblastech průmyslové automatizace.

Produkuje SW nástroje „Home I/O", což je 3D simulace inteligentního domu v reálném čase. Dále pak „It´s PLC", což je vývojové prostředí na programování a simulování PLC, „Exercise book", která slouží jako příručka s příklady a cvičeními jak programovat PLC v „It´s-PLC" a v poslední řadě „Factory I/O".

„Factory I/O" slouží k 3D simulaci výrobní linky. SW lze propojit s širokou paletou řídicích prvků a automatů, například od společnosti Allen-Bradley nebo Siemens. Dále umožňuje propojení přes OPC DA[69] server, takže SW spojíte takřka s jakýmkoliv řídícím prvkem. Na webových stránkách SW je umístěno značné množství návodů i hotových ukázkových projektů, které jsou volně stažitelné. Uživatel si může vše ozkoušet a pak vytvořit vlastní výrobní linku.

Samotná linka se tvoří v tzv. scéně. Scéna je tvořena halou s pevně definovanou šířkou a výškou. Do této haly se umisťují prvky linky. SW prozatím obsahuje cca 90 interaktivních prvků, bohužel se tyto prvky nedají nijak editovat. Prvky jsou rozděleny do 8 skupin: předměty, prvky pro manipulaci s paletami, prvky pro manipulaci s předměty, senzory, ovládací prvky, stanice, výstražné předměty a pěší cesty. Veškeré dostupné prvky uživatel může libovolně otáčet, rotovat, posouvat a umisťovat do jakékoliv výšky. U aktivních prvků a prvků určených k manipulaci je možné si zvolit typ ovládání (digitální, analogové, digitálně-analogové). Dostupné prvky jsou zobrazeny na Obr. 5-1. Podrobnější popis tvorby vizualizace viz nadcházející kapitoly.

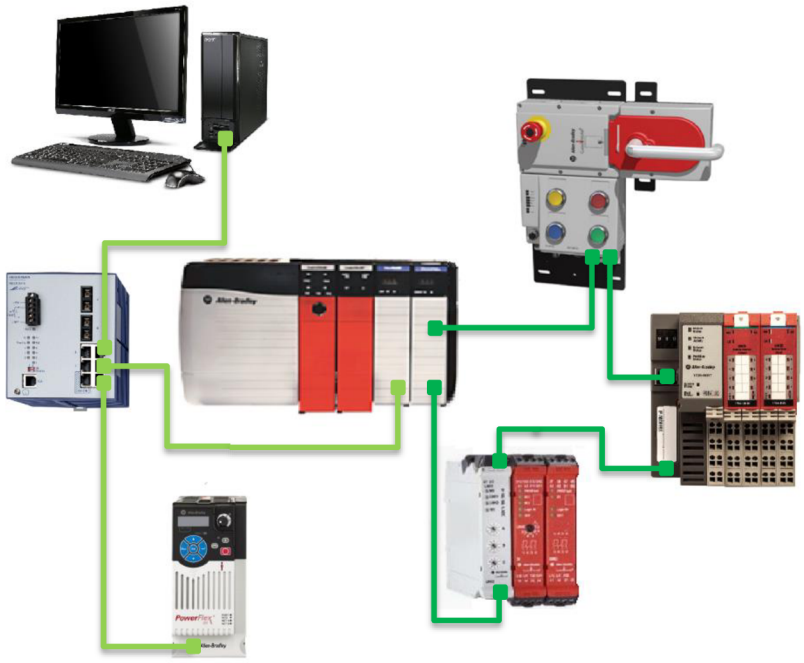
[69] Open platform communications data access.

Obr. 5-1 Dostupné prvky ve Factory I/O [12].

5.3 HW řešení

Prvním krokem při HW řešení laboratorní úlohy je navržení topologie sítě, blokových schémat hierarchie a schémat elektrického zapojení.

Je vhodné zvolit kruhovou topologii sítě, protože je spolehlivější a v případě výpadku signálu mezi dvěma sousedními stanicemi se data transportují druhou stranou. Téměř všechny hlavní komponenty v Tab. 5-1 jsou osazeny dvěma ethernetovými porty. Pouze frekvenční měnič disponuje jedním portem. Počítač ve školní laboratoři obsahuje dvě síťové karty, ale bohužel neumožňují vzájemné přemostění a připojení PC do kruhové topologie. Z toho důvodu byla zvolena kombinovaná topologie. Frekvenční měnič, PC a první ethernetová karta automatu, umístěna ve slotu (02) jsou připojeny přes 8 portový switch na topologii typu sběrnice. Zbylé komponenty s dvěma porty jsou zapojeny do topologie typu kruh a připojeny do druhé ethernetové karty automatu ve slotu (03). Takové zapojení přináší spolehlivost a zároveň snadné monitorování sítě. Je nutné podotknout, že ethernetové karty automatu musí mít nastavené rozdílné podsítě. Jestliže není tato podmínka splněna, kruhová topologie indikuje chybový status. Znázornění topologie zapojení komponentů je uvedeno na Obr. 5-2.



Obr. 5-2 Znázornění topologie úlohy

Po zvolení topologie jsem mohl začít tvořit HW konfiguraci. Z mých zkušeností usuzuji, že ideálním postupem je prvně vytvoření tzv. „čisté" konfigurace. Tím myslím HW konfiguraci bez jakéhokoliv uživatelského programu. Tímto se eliminují možnosti chyb a do budoucna budu vědět, že chyba je v programu nebo vznikla nestandardním stavem na HW např. špatným připojením, kolísáním napájení, znehodnocením

kabelu atd. Jednotlivé komponenty jsem nastavoval a přidával do HW konfigurace, jednu po druhé tak, aby byla konfigurace bez chyb.

IP adresy jednotlivých komponentů byly přenastaveny nebo ponechány v adresovém prostoru 192.168.xxx.xxx. Přehled nastavených IP adres viz Tab. 5-3.

Většina ethernetových komponentů je certifikována na úroveň bezpečnostní integrity SIL 3 a PL e. Jediný frekvenční měnič disponuje úrovní SIL 2 a PL d. Tím pádem vytvořené bezpečnostní aplikace dosáhne maximální úrovně integrity SIL 2 a PL d. Ovšem tyto úrovně jsou podle ČSN EN 61508 a ČSN EN ISO 13 849-1, plně dostačující, protože jsou určováni typem a účelem použití strojního zařízení.

Tab. 5-3 Tabulka s přehledem použitých IP adres

Hlavní - komponenta		IP	Katalogové označení
Automat	Ethernetová karta 1(Hvězda)	192.168.2.140	1756-ENBT/A (1 port)
	Ethernetová karta 2 (Kruh)	192.168.1.100	1756-EN2TR/C (2 porty)
Frekvenční měnič		192.168.2.62	PowerFlex525 1P
Bezpečnos. POINT I/O modul		192.168.1.139	1734-AENTR 24V DC
Multifunkční přístupový blok		192.168.1.135	442G-MABR-UT-C03
EtherNetová karta relé		192.168.1.123	240V440R-ENETR

5.3.1 Programovatelný automat

Jako první jsem nastavil programovatelný automat, což je hlavní člen celé aplikace. Do rámu jsem vložil všechny příslušné karty a připojil zdroji napájení 230V AC. Do první síťové karty v automatu se připojí ethernetový kabel, který vede do síťové karty v PC. V počítači se nastaví statická IP adresa, aby nevznikl konflikt IP adres na síti. Proto jsem použil IP s vysokým číslem síťového rozhraní 192.168.2.250. Poté se spustí RSLinx, který prohledá síť a poskytuje informace o automatu podle kterých se pak vytvoří HW konfigurace v RSLogix5000.

V případě, že RSLinx automat nevidí, má pravděpodobně nastavenou jinou podsíť než PC nebo nemá nastavenou žádnou IP adresu, protože se jedná o nové zařízení. Problém s přidělením adresy novému zařízení řeší program BOOTP/DHCP Server. Tento program pracuje na úrovni linkové vrstvy a vyhledává MAC adresy dostupných zařízení. Po prohledání dostupných MAC adres, může uživatel pohodlně přidělit zařízení IP adresu.

Při přenastavení IP adresy již používaného zařízení nastává problém v případě, když není známa jeho podsíť. Existují SW nástroje, které prohledají celý adresní prostor, ale tento proces je velice zdlouhavý. Proto je dobré na viditelné místo napsat IP adresu příslušného zařízení. Síťové karty programovatelného automatu byly nastaveny

na rozdílné segmenty, kvůli využití kruhové topologie. První síťovou kartu jsem nastavil na IP 192.168.2.140 a druhou na IP 192.168.1.100.

Po přenastavení IP adres a zviditelnění automatu v RSLinx přišla na řadu konfigurace karet na příslušné topologie a další nastavení (povolení portů, nastavení rychlostí přenosu atd.). Poté lze automat přidat do HW konfigurace, nastavit všechny parametry a přehrát. Po přehrání jsem vyzkoušel přepnout automat do RUN režimu, popřípadě odstranil chyby v konfiguraci, tak aby byl RUN režim aktivní. Automat je zobrazen na Obr. 5-3.

Obr. 5-3 Bezpečnostní automat.

5.3.2 Bezpečnostní POINT I/O

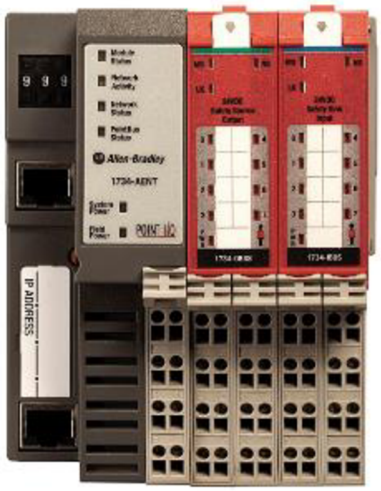
Dalším prvkem přidaným do HW konfigurace byl bezpečnostní POINT I/O modul s katalogovým označením 1734-AENTR 24V DC. Tento modul byl osazen první kartou 1734-IB8S 24V DC s 8 bezpečnostními vstupy a druhou kartou 1734-OB8S 24V DC s 8 bezpečnostními výstupy. Bezpečnostní POINT I/O i s kartami je zobrazen na Obr. 5-4.

První karta disponuje 8 digitálními vstupy, 4 svorkami COM a 4 testovacími vstupy. Úroveň přechodu z logické 0 do 1 je 11V. Druhá karta je téměř totožná, s tím rozdílem, že se jedná o digitální výstupy. Při konfiguraci je použito nastavení dual-channel z důvodů splnění nároků na bezpečnost. Všechny vstupy/výstupy z karet jsou automaticky přiřazeny do safety proměnných. Popis konfigurace je uveden v technické dokumentaci v seznamu literatury [13], [14].

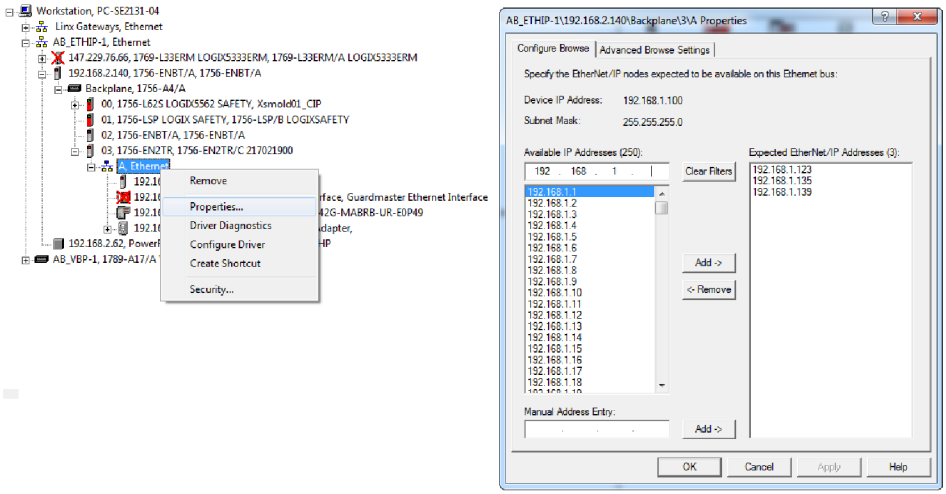
Při konfiguraci jsem narazil na dva problémy. Prvním bylo nezobrazení POINT I/O modulu v RSLinx, které bylo způsobeno připojením na druhou síťovou kartu. Program RSLinx rozešle broadcast zprávu do sítě. Při topologii typu sběrnice se mu ozvou všechny zařízení. Nicméně při mém zapojení a použití dvou sítových karet přijdou autorizační data pouze od druhé síťové karty, které už dál broadcast zprávu nepošle. Pro zobrazení je potřeba ručně přidat IP, na kterou se má doptávat viz Obr. 5-5. Další možností řešení by bylo použití jedné síťové karty a managementovatelného switche např. model Stratix 5700 nebo zařízení Etap.

Druhým problémem byla nefunkční komunikace automatu s I/O kartami. V HW konfiguraci v RUN režimu u karet byly žluté vykřičníky a v „error buffer", chyba

indikující špatné nastavení parametrů. Tento problém byl odstraněn opětovným přiřazením „ownership" (vlastnictví) oběma kartám s následným restartováním modulu.



Obr. 5-4 Bezpečnostní POINT I/O



Obr. 5-5 Ruční zadávání IP adresy RSLinx.

5.3.3 Multifunkční přístupový blok

Dalším prvkem začleněným do kruhové topologie byl multifunkční přístupový blok s katalogovým označením 442G-MABR-UT-C03 [15], [16].

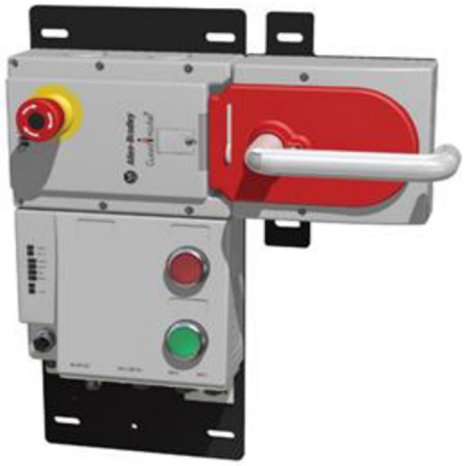
Blok slouží k omezení přístupu do nebezpečných prostor pomocí blokování nebo uzamčení. Tento blok se skládá ze tří částí: kliky, zámku se stop tlačítkem a třetího bloku, ve kterém je vnitřní bezpečnostní logika a dvě tlačítka. Funkci tlačítek si může uživatel libovolně naprogramovat. Zámek se vyznačuje přídržnou sílou až 2000 N a klika je opatřena unikátním RFID[70] čipem k její identifikaci. Multifunkční přístupový blok je zobrazen na Obr. 5-6.

[70] Radio frequency identification.

Pro připojení bloku k napájení je potřeba čtyř pinový M12 konektor. K připojení do sítě je potřeba ethernetový kabel s konektory M12 a RJ45. DIP switche umístěné ve třetím bloku nebylo potřeba měnit. Zůstaly nastaveny v defaultních pozicích, viz technická dokumentace [15]. Po připojení kabelů můžeme blok začleňovat do HW konfigurace. Postup je stejný, jak u předchozí kapitoly.

Bohužel jsem narazil na další problém, kterým bylo, že RSLinx nemá multifunkční blok ve svojí databázi. Řešením tohoto problému byla potřeba stáhnout tzv. EDS file[71], který umožní identifikaci příslušného HW. Po updatu EDS jsem přešel k nastavení IP adresy, portů. IP adresa je defaultně nastavena na podsíť 192.168.1.xxx. Nastavení podsítě zůstalo defaultní, změnil jsem pouze adresu síťového rozhraní, takže IP adresa multifunkčního bloku je 192.168.1.135.

Dalším krokem bylo začlenění bloku do HW konfigurace v RSLogix 5000. Ani tento SW neměl ve svojí databázi soubory potřebné pro integraci bloku. Z technické dokumentace [16], jsem se dozvěděl, že je potřeba z webových stránek Rockwell Automation stáhnout ADD-ON profil pro příslušný modul. Ovšem, aby uživateli bylo umožněno stahování, musí být registrován. Absence multifunkčního boxu v interních databázích SW nástrojů je způsobena faktem, že se snažím o propojení starého SW s novým HW a to se dá očekávat i u ostatních novějších komponentů. Při nastavování a parametrizování jsem postupoval podle dostupných technických dokumentací v seznamu literatury [16]. SW vstupy/výstupy bloku jsou automaticky přiřazeny do safety proměnných.



Obr. 5-6 Multifunkční přístupový blok.

5.3.4 Bezpečnostní relé

Dalším prvkem začleněným do kruhové topologie je ethernetová karta relé [17] s katalogovým označením 440R-ENETR. Karta slouží k přemostění komunikace bezpečnostních relé Guardmaster v síti EtherNet/IP. K jednomu síťovému modulu může

[71] Electronic data sheets file.

být připojeno maximálně 6 bezpečnostních relé. Karta podporuje relé typu DI[72], DIS[73], EM[74], EMD[75], GLP[76], GLT[77] a umožňuje vytvoření komplexní diagnostiky všech připojených modulů s detekcí poruch, chybových stavů, nadměrných proudů atd.

Typ topologie sítě může být nastaven jako hvězda, kruh a sběrnice. Na přední straně je umístěno několik status indikátorů včetně tří potenciometrů pro nastavení IP adresy. Při zadání neplatného síťového rozhraní (hodnota vyšší než 255), se modul přepne do režimu, ve kterém nebere v úvahu fyzicky nastavenou adresu na předních potenciometrech, ale za validní IP adresu bere SW nastavenou programem BOOT/DHCP Server. IP adresa byla nastavena pomocí potenciometru na 192.168.1.123.

K dispozici mám dvě relé DIS a EM [18]. Relé typu DIS s katalogovým označením 440R-D22S2 je bezpečnostní dvoukanálové relé, které disponuje dvěma elektromechanickými nebo polovodičovými výstupy. Dále umožňuje režim logiky AND/OR nebo kombinaci obojího, čímž standardní výstupy můžeme konfigurovat takřka na libovolné bezpečnostní funkce pro vypínání nebo rozdělení pracoviště na oddělené zóny. Pomocí otočného potenciometru, umístěného na čelní straně relé, lze zvolit režim logiky bezpečnostních vstupů. Relé typu EM s katalogovým označením 440R-EM4R2, slouží pouze jako rozšiřující modul pro spínání pomocných kontaktů výstupu řízeným vstupem z předchozího relé. Blok bezpečnostních relé je zobrazen na Obr. 5-7.

Zvolil jsem režim 6 „(IN1 AND IN2) OR L12". Relé sepne výstup a své pomocné kontakty pouze, když bude aktivní bezpečnostní vstup 1 a 2, nebo pomocný vstup L12. Signál L12 slouží jako řídicí signál z předchozího relé a musí obsahovat přesně dané parametry (nelze jednoduše simulovat automatem). Pro přenastavení režimu se musí potenciometr nastavit na hodnotu „0", provést reset napájení 24V. Po spuštění relé se změní pozice potenciometru např. na hodnotu 6 a provede se reset napájení. Pokud se ani po této sekvenci kroků relé nepřenastaví a nezhasne „fault" indikátor je potřeba celou sekvenci zopakovat.

U začlenění modulů do HW konfigurace musel opět proběhnout update EDS file a stažení ADD-ON profilu. Je nutné podotknout, že ethernetová karta 440R-ENETR není bezpečnostní, čili se všechny SW vstupy/výstupy připojených relé přiřadí do proměnných programu a do safety proměnných se musí přemapovat. I přesto je splněna úroveň bezpečnosti SIL 3, protože bezpečnostní logika je v samotných relé a ethernetová karta slouží pouze k přemostění komunikace. Při nastavování

[72] Dual input.
[73] Dual input solid-state.
[74] Expansion module.
[75] Expansion module delayed.
[76] Guardlocking proximity module.
[77] Guardlocking witch time-delay.

a parametrizování jsem postupoval podle dostupných technických dokumentací v seznamu literatury [17], [18].

Obr. 5-7 Bezpečnostní relé.

5.3.5 Osmiportový switch

Pro připojení měniče bylo potřeba vytvořit topologii typu sběrnice. K tomuto účelu slouží osmiportový switch vyrobený firmou Hirshmann [23] s katalogovým označením RS2-FX/FX. Switch je zobrazen na Obr. 5-8.

Jedná se o switch použitelný v průmyslových aplikacích. Obsahuje 6 metalových ethernetových portů a dva optické. Switch umožňuje redundantní zapojení optických portů napájení i řídících signálů pro zvýšení spolehlivosti celé aplikace. Tyto možnosti nebyly využity a switch byl použit standardním způsobem. Pouze bylo připojeno napájení a zapojeny ethernetové porty z PC, automatu a měniče.

Obr. 5-8 Osmiportový switch Hirshmann [23].

5.3.6 Frekvenční měnič

Posledním komponentem s podporou rozhraní EtherNet/IP je frekvenční měnič [21] s katalogovým označením PowerFlex525 1P 240V. Měnič se používá k řízení střídavých motorů. Nabízí rozsah výkonu 0,4 - 22kW při 100 - 600V. Disponuje SW nástroji pro

usnadnění konfigurace a parametrizování měniče. Umožňuje ovládání měniče z displeje nebo pomocí rozhraní Ethernetu/IP. Bezpečnost je certifikována na úroveň SIL 2, PL d. Dále umožňuje připojení 3fázového motoru na výstupy měniče, připojení snímače otáček a zapojení bezpečnostních kontaktů. Frekvenční měnič je zobrazen na Obr. 5-9.

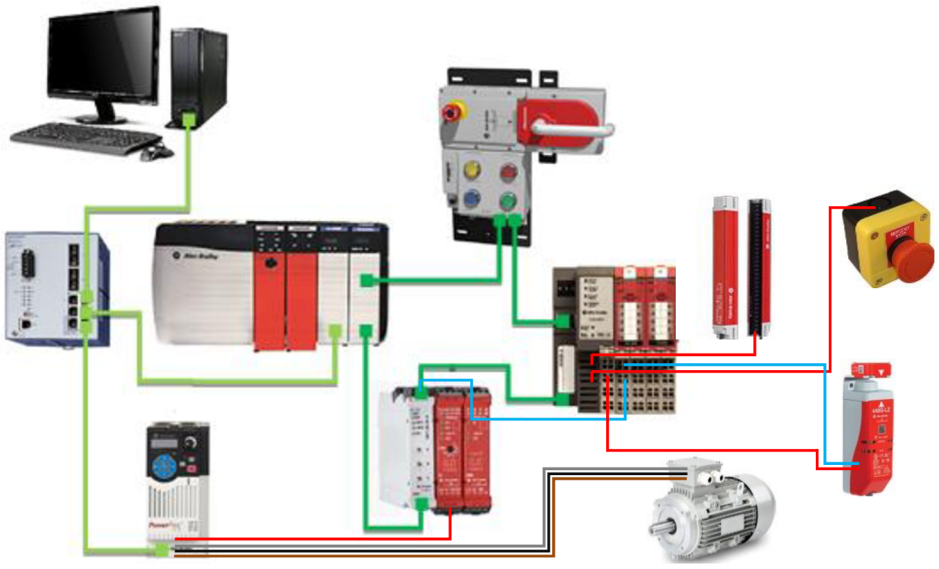
Při začleňování měniče do sítě bylo zapotřebí nejdříve přenastavit IP adresu ručně pomocí displeje a tlačítek, protože RSLinx frekvenční měnič nezobrazoval v topologii. Dále následoval update EDS souboru a přidání ADD-ON profilů do RSLogix 5000. IP adresa měniče byla nastavena na 192.168.2.62. Pro povolení bezpečnostních funkční měniče se musí odstranit zkratovací propojka z kontaktů S1, S2 a S+, na které se pak připojí bezpečnostní signály. Dále se musí propojit svorka 01 a 11 pro HW povolení bezpečnostní funkce. Parametry měniče při HW konfiguraci byly nastaveny pomocí průvodce konfigurací, tak aby korespondovaly se štítkovými parametry dostupného motoru, který je popsán nadcházející kapitole.

Obr. 5-9 Frekvenční měnič [21].

5.3.7 Periferie

V následující kapitole jsou popsány periferní komponenty bez rozhraní EtherNet/IP, které jsou zapojeny do výše zmíněných komponentů s podporou EthernNet/IP. Tyto komponenty ovládají safety logiku programu a uživatel může ovlivnit jejich stav. Z použitých komponentů budou popsány bezpečnostní závora, zámek, bezpečnostní tlačítko a 3-fázový motor.

Bezpečnostní závora, tlačítko a zámek jsou zapojeny na vstupy POINT I/O modulu. Signál zamčeno/odemčeno, řídící zámek, vede z bezpečnostního výstupu POINT I/O modulu. Při korektním zamčení je nastavována dvojce bezpečnostních výstupů POINT I/O modulu, která je připojena na relé DIS. Po sepnutí bezpečnostního relé DIS, se sepne relé s pomocnými kontakty EM. Na těchto kontaktech je připojeno napětí + 24V a ovládají bezpečnostní vstupy frekvenčního měniče. Po sepnutí safety vstupů začne měnič budit motor a ten se rozpohybuje frekvencí 50 Hz. Pro lepší představu jsem vytvořil kompletní hierarchii zapojení i s topologií sítě, viz Obr. 5-10. Celkové elektrické schéma zapojení je uvedeno Příloha 1.

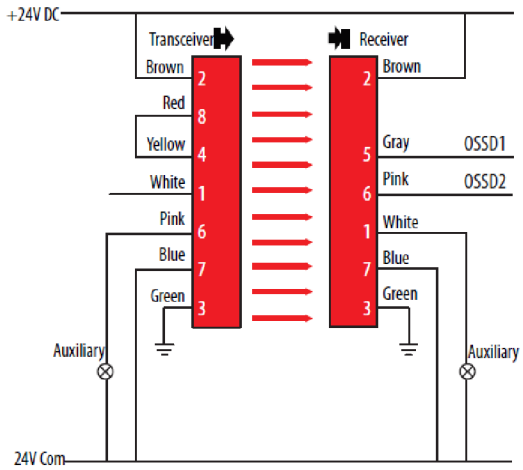


Obr. 5-10 Kompletní hierarchie zapojení komponentů.

Bezpečnostní závora

Bezpečností infračervená závora [20] s katalogovým označením 450L-APU-UN-8 slouží k monitorování a detekci přístupu do nebezpečných prostor. Mnou použitá závora má efektivní výšku snímaného prostoru 300 mm. Závora se skládá z přijímače, vysílače a dvojce čipů, které se vkládají vně závor. Bezpečnostní závora je zobrazena na Obr. 5-12.

Označení UN znamená univerzální. Každý modul může plnit funkci vysílače nebo přijímače, který se volí elektrickým zapojením, viz Obr. 5-11. DIP switchem na modulech vkládaných do závory se konfigurují reset módy, možnosti monitorování atd.



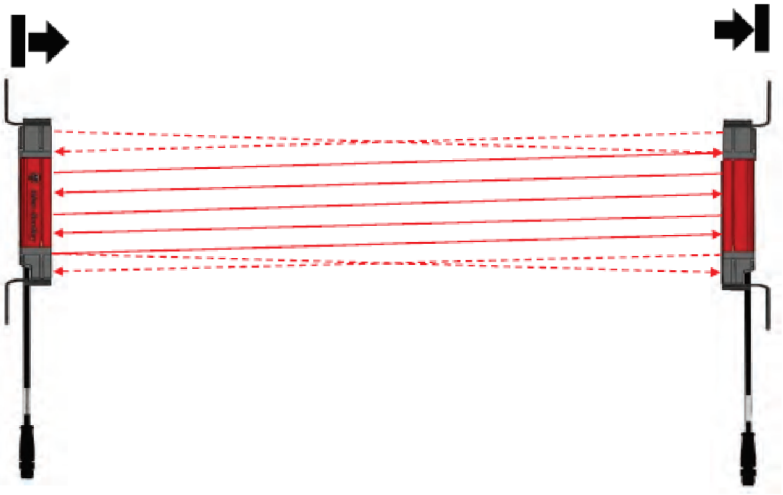
Obr. 5-11 Zapojení vysílače a přijímače [20].

Závora snímá prostor po celé délce optického závěsu, tím je možné detekovat ruce, dlaně i prsty apod. Vysílače infračerveného paprsku nevyzařují záření vodorovně, ale pod mírným úhlem, viz Obr. 5-13. Navíc vysílač i přijímač mají minimální vzájemnou

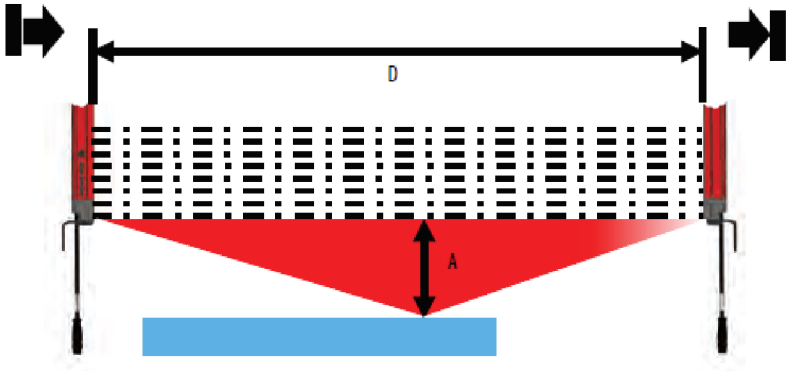
vzdálenost „D" 300 mm a minimální vzdálenost od reflexních ploch „A" 135 mm, viz Obr. 5-14 . Důvodem těchto omezení je eliminace možnosti demontování závory z určeného místa, následné přiložení vysílače i přijímače na sebe a omotání páskou. Takové počínání by mělo následek obejití bezpečnostní funkce.

Pro usnadnění montáže jsou na spodní části vysílače a přijímače dvě LED pro signalizace ideálního vyrovnání dopadajících paprsků horní a spodní části. Při stálém svícení těchto diod je nastavení perfektní, při neustálém problikávání nastavení není ideální, ovšem stačí ke správné funkčnosti. U obou těchto stavů proběhne setování bezpečnostních signálů.

Obr. 5-12 Bezpečnostní závora [20].



Obr. 5-13 Úhel paprsků vysílače [20].



Obr. 5-14 Minimální vzdálenosti bezpečnostní závory [20].

Bezpečnostní zámek

Bezpečnostní zámek [19] s katalogovým označením 440G-LZ slouží k blokaci přístupu do nebezpečných prostor. Skládá se ze dvou částí. První částí je hlavní tělo zámku, ve kterém je umístěna logika. Druhou částí je kovové očko osazené RFID čipem. Při setování signálu k uzamčení, zámek detekuje RFID čip a vysune zamykací kolík, sloužící k blokaci pozice kovového očka pouze v případě, že je ochranný kryt uzavřený. Po uzamčení a detekci RFID čipu se setují bezpečnostní výstupy. Tyto výstupy v případě mého zapojení sepnou bezpečnostní relé a ty povolí frekvenčnímu měniči buzení motoru.

Zámek neustále poskytuje obsluze vizuální informace o jeho stavu dvojicemi LED indikátorů umístěných na přední straně. Stálé zelené světlo naznačuje uzavřený a uzamčený stav. Blikající zelené světlo naznačuje požadavek na zamčení, které ale není možné protože RFID čip není přítomen a kryt není na svém místě. Plné červené světlo značí odemčení a blikající červené světlo značí chybový stav např., že zámek je uzamčen, ale nějakým způsobem byl kolík manuálně zastrčen zpět nebo odebrán RFID čip. Tento stav je nestandardní a modul se v tomto případě zasekne. Zpět do normální činnosti se vrátí až po resetu (odpojení napájení 24 V). Pokyny pro montáž, popis vývodů a příklady zapojení jsou uvedeny v technická dokumentaci [19].

Obr. 5-15 Zámek 440G-LZ [19].

Bezpečnostní tlačítko

Bezpečnostní tlačítko je použité tzv. klasické s dvěma kontakty a s katalogovým označením nouzové tlačítko hříbek NO/NC. Jeden kontakt je rozpínací, druhý spínací. Při přivedení +24 V na oba kontakty a následném zamáčknutí tlačítka jeden signál, který vede do POINT I/O, bude v logické úrovni 0 a druhý v logické úrovni 1. Pro toto zapojení nemohou být POITN I/O vstupy nastaveny jako dual-channel, ale jen single mode. Navíc signál v logické 0 musí být SW invertován. Bezpečnostní tlačítko je zobrazeno na Obr. 5-16.

Obr. 5-16 Bezpečnostní tlačítko.

Třífázový motor

Jedná se o klasický asynchronní trojfázový motor s kotvou, statorem a rotorem. Motor má katalogové označení 4AP90L (nástupce 1LE1002) [22]. Z jeho štítku jsem získal informace, že jde o 6-pólový motor příkonem 1,1kW a 930 otáčkami za minutu při 50 Hz. Dále jsem podle štítkového označení vyhledal katalog s náhradou motoru. Z katalogu byly doplněny potřebné informace do průvodce nastavení frekvenčního měniče pro jeho správné řízení. Dále je motor opatřen kontakty pro snímač vibrací, který ovšem není osazen. Motor je znázorněn, viz Obr. 5-17.

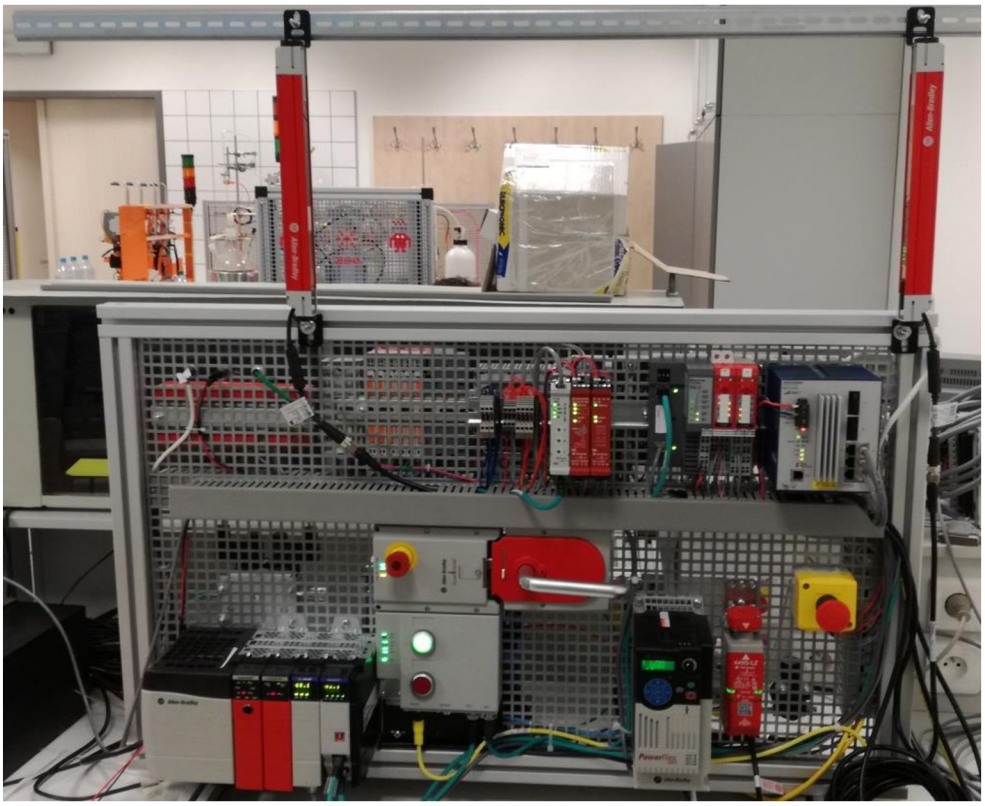
Obr. 5-17 Třífázový motor 4AP90L.

5.4 Konečné umístění na panel

V předchozí kapitole byly popsány jednotlivé dostupné komponenty a nastínění několika vzniklých problému při tvorbě HW konfigurace. Dalším krokem byla montáž komponentů na panel.

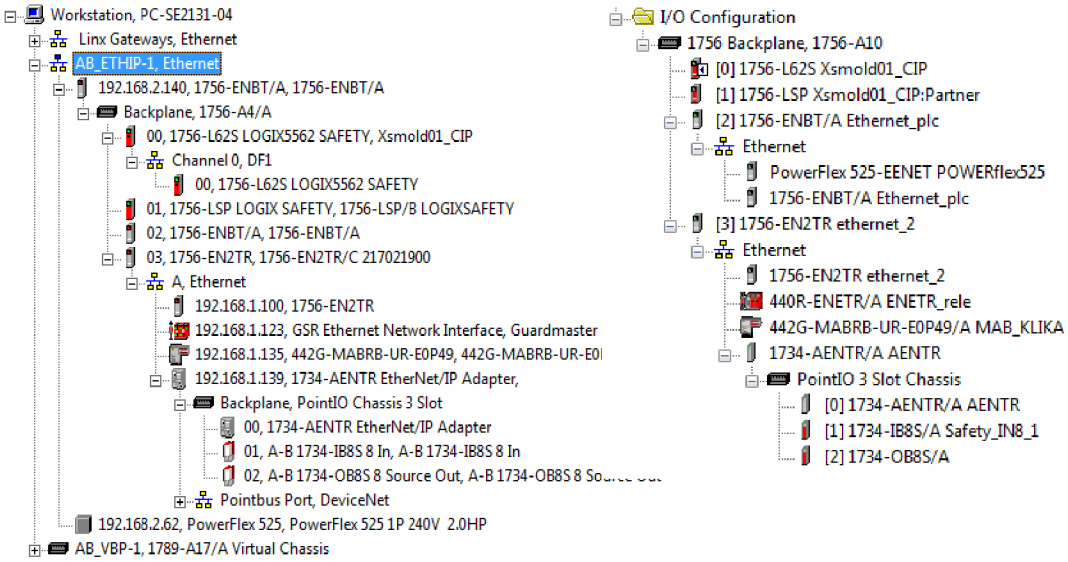
Při montáži zařízení na laboratorní panel jsem byl limitován faktem, že z druhé strany panelu jsou umístěna zařízení z jiného projektu. Musel jsem tak využívat prostor i šrouby, které šly skrz panel, aby na sobě oba projekty nebyly závislé a zároveň byly plně funkční.

Největší problém bylo nastavení bezpečnostní závory. Musel jsem dodržet limitní vzdálenosti a zároveň nastavit paprsky tak, aby závora byla plně funkční. Z tohoto důvodu byla umístěna na horní část celého panelu. Bohužel nebyl v laboratoři dostupný dostatečně dlouhý profil, tak bylo přichycení horních částí závory vyřešeno montáží k DIN liště. Toto řešení není úplně ideální, protože při otřesu nebo pohybu se DIN lišta krouti a paprsky nedopadají, jak mají, tím pádem se poruší bezpečnost. Z toho důvodu je potřeba průběžně kontrolovat nastavení závory. Fotografie celého panelu je uvedena na Obr. 5-18. Topologie z dostupných SW nástrojů jsou takřka totožné, viz Obr. 5-19 a elektrické schéma se zapojením komponentů je uvedeno v Příloha 1.



Obr. 5-18 Fotografie laboratorního panelu.

RSLinx **RSLogix 5000**



Obr. 5-19 Topologie z programu RSLinx A RSLogix 5000.

6 VLASTNÍ ŘEŠENÍ

V následující kapitole bude popsáno mé vlastní SW řešení laboratorní úlohy. Celé řešení je rozděleno do několika kapitol, ve kterých budou popsány postupy a řešení vzniklých problémů.

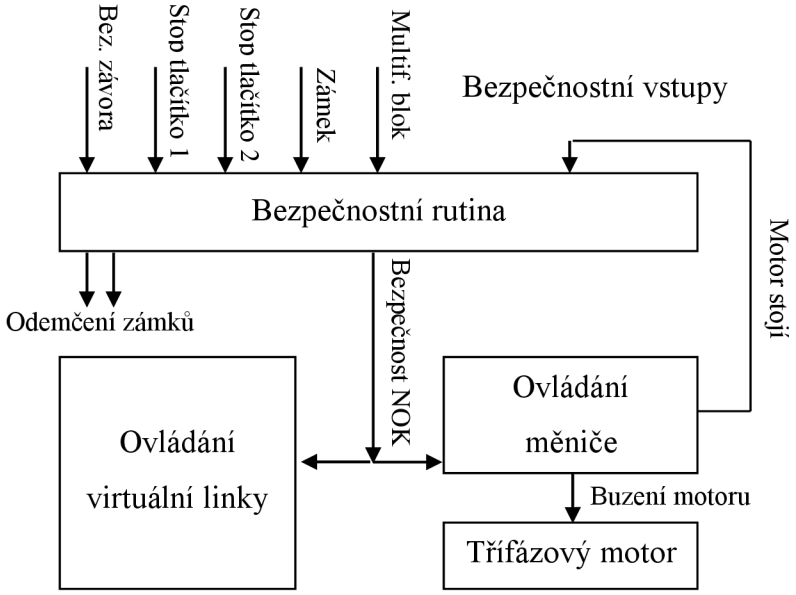
6.1 Zadání laboratorní úlohy

Seznamte se s instrumentací a zapojením dostupných bezpečnostních komponentů podporujících CIP safety. Z uvedených tabulek safety komponentů Tab. 5-1 a Tab. 5-2, vytvořte bezpečnostní aplikaci se SW řešení obsluhy bezpečnostních rutin a řízení virtuální výrobní linky. Aplikace bude obsahovat bezpečnostní funkce:

a) Bezpečnostní závora (auto potvrzení).
b) Bezpečnostní stop tlačítka (manuální potvrzení z vizualizace).
c) Bezpečnostní zámky (odemčení až po zastavení pohybujících se částí).

6.2 Safety SW řešení

Při tvorbě SW řešení bezpečnostních rutin je třeba si ujasnit, jak má obsluha rutin fungovat. K dispozici mám bezpečnostní závoru, zámek, dvě stop tlačítka (1x externí, 1x na multifunkčním bloku a samotný multifunkční blok). Všechny tyto prvky budou přímo řídit bezpečnostní rutinu. Když budou všechny bezpečnostní signály v pořádku, předdefinován proměnná spustí měnič i virtuální výrobní linku. Při porušení bezpečnosti nebo požadavku k odemčení se pohyblivé prvky ve vizualizaci zastaví a odemčení proběhne až po té, co otáčky motoru budou nulové. Pro lepší porozumění byl vytvořen zjednodušený vývojový diagram, uvedený na Obr. 6-1.



Obr. 6-1 Vývojový diagram řízení bezpečnosti.

6.2.1 Bezpečnostní rutina

V předchozí kapitole bylo uvedeno, že vstupní a výstupní proměnné použité v modulech se automaticky deklarují jako safety. Poté s nimi lze pracovat v safety části programu, kde obyčejné proměnné užívat nelze.

Prvním krokem bylo zmapování fyzického zapojení vstupy a výstupy, viz Příloha 1. Z dostupného schématu elektrického zapojení jsem zjistil, že dvojce safety vstupů z bezpečnostní závory je zapojena do první karty v POINT I/O modulu na svorku IN 0 a IN 1. Dalším připojeným prvkem do tohoto modulu je bezpečnostní stop tlačítko. Tlačítko je připojeno do stejné karty na svorky IN 4 a IN 6. Posledním periferním komponentem připojeným do této karty je zámek, jehož dvojce bezpečnostních kontaktů je připojena na svorky IN 6 a IN 7. Na svorku IN 2 je připojen signál z relé DIS, ten je ovšem navíc a v bezpečnostní rutině nebude používán.

Z výstupní karty v POINT I/O modulu je připojen kontakt pro ovládání odemknutí zámku na svorku OUT 0 a signály, které spustí frekvenční měnič, vedoucí na bezpečnostní svorky relé DIS, jsou připojeny do svorek OUT 2 a OUT 3.

Signály z multifunkčního bloku nemusely být nikam připojovány, protože jsou transportovány po ethernetu přímo do watch tabulky v automatu.

Bezpečnostní rutina je realizována v SafetyTask s názvem MainRoutine. V rutině byly použity předdefinované bezpečnostní funkce a zakomponována nezbytná logika pro správou funkčnost. Výstupem z této rutiny je globální proměnná, která řídí vizualizaci a buzení motoru. Proměnná se nazývá RUN_NOK_Saf a má negativní logiku, když je v logické 1, tak je porušena bezpečnost.

6.2.2 Použité bezpečnostní funkce

V následující kapitole jsou popsány a rozebrány použité předdefinované bezpečnostní funkce LC, ESTOP, RIN a popsána logika SW řešení bezpečnosti multifunkčního bloku.

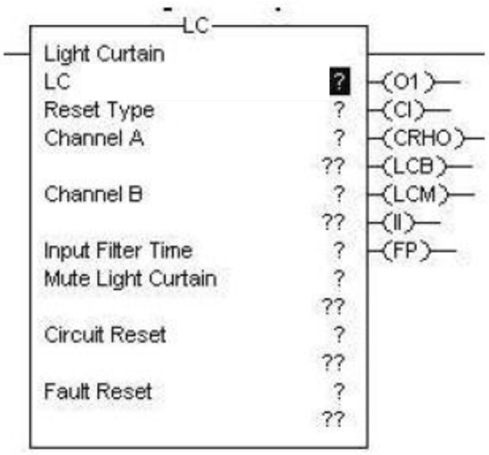
LC - Light Curtain

Předdefinovaná funkce LC [24] byla použita pro ovládání bezpečnostní závory. Jediná bezpečnostní závora nebude vyžadovat potvrzení bezpečnosti. Jinými slovy, při porušení bezpečnosti (protnutí clony) dojde k zastavení všech akčních členů. Po jejím opětovném nahození se akční členy automaticky rozběhnou bez jakékoliv nutnosti potvrzování.

K obsluze závory byla využita funkce Light Cutain. Tato funkce v ladder diagramu je zobrazena na Obr. 6-2. Na obrázku jsou viditelné konfigurovatelné vstupy, do kterých si lze přidávat proměnné příslušných datových typů a na pravé straně řízené výstupy z bloku. Každý výstup má svůj specifický význam. Popis vstupů a výstupů viz Tab. 6-1.

Tab. 6-1 Popis vstupů a výstupů bloku LC [24]

Parametr	Zkratka	Typ	Dat. typ	Popis
LC	-	-	Před. typ	Předdefinovaný typ sloužící k uchování výstupních inf.
Reset type	-	Vstup	Bool	Manuální / Automatický reset pro O1
Channel A	-	Vstup	Bool	Bezpečnostní signál 1
Channel B	-	Vstup	Time	Bezpečnostní signál 2
Imput filter time	-	Vstup	Bool	Volitelný čas 0 – 250 ms, pro testování světelné závory
Mute light curtain	-	Vstup	Bool	Vypnutí světelné závory při nepoužívání
Circuit reset	-	Vstup	Bool	Obnovení vstupního obvodu: Man. - nastavuje O1při přechodu z 0 na 1 a přitom Circuit reset přechází z 1 na 0 Automatický.- nepoužívá se
Fault reset	-	Vstup	Bool	Vymaže chybové instrukce po přivedení logické 1
Output 1	O1	Výstup	Bool	Výstup, který je v logické 1 při splnění vstupních podmínek (bezpečnost OK)
Cycle inputs	CI	Podmíněný výstup	Bool	Indikuje stav kdy je O1 v logické 0 ale bezpečnostní vstupy přešli z 0 do 1 (do bezpečného stavu)
Circuit reset held on	CRHO	Podmíněný výstup	Bool	Obnovení obvodu: Manuální - nastaví se na 1 po opětovném přechodu bezpečnostních vstupů z 0 do 1, k resetování odjde az po přechodu CI z 1 do 0. Automatický - nepoužitý
Light curtain blocked	LCB	Indikátor výstupu	Bool	Indikátor blokování závory, nebo ztráty napájení
Light curtain muted	LCM	Indikátor výstupu	Bool	Indikátor vypnutí závory (režim nepoužití)
Input inconsistent	II	Chyb. výstup	Bool	Indikuje nekonzistentní stav, nekonzistentní čas 500ms
Fault present	FR	Chyb. výstup	Bool	Indikace poruchy



Obr. 6-2 Blok LC [24].

Pro korektní použití funkce LC - Light Curtian je potřeba deklarovat proměnnou typu Light Curtian, v mém programu se tato proměnná jmenuje „závora". Proměnná se deklaruje jako struktura obsahující všechny výstupní proměnné, které pak lze snadno monitorovat. Protože byl použit reset type - AUTOMATIC, stačí připojit bezpečnostní kanály a ostatní vstupní proměnné nastavit na 0.

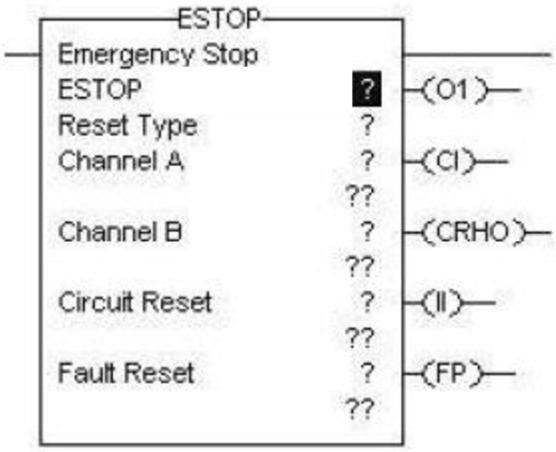
ESTOP - Emergency Stop

K vyřešení bezpečnosti stop tlačítek byla použita funkce Emergency Stop [24]. Tento blok je podobný jako blok LC. Podstatným rozdílem je nutnost použití proměnnou typu ESTOP a samotný blok obsahuje méně vstupních/výstupních parametrů. Parametry, které jsou stejné a mají i stejnou funkčnost, jsou uvedeny na Obr. 6-3 a Tab. 6-1.

Blok funguje následujícím způsobem, při zamáčknutí tlačítka výstup O1 se nastaví do 0. Tímto výstupem se řídím proměnnou pro indikaci porušení bezpečnosti. Po následném vymáčknutí tlačítka se opět nastaví bezpečnostní vstupy a zároveň proměnná CRHO. V případě automatického resetu by se blok resetoval a nastaví se výstup O1. Byl použit MANUÁLNÍ režim, ve kterém se musí signál Circuit reset přejít z 1 na 0 a zároveň se musejí resetovat případné chyby. U manuálního resetu nastal problém. Signál Circuit reset nelze nastavit při nastavení bezpečnostních vstupů, ale musí být nejméně o 50 ms zpožděn. Zpoždění signálu bylo vyřešeno timerem. Po opětovném sepnutí bezpečnostních vstupů byl nastaven Circuit reset na úroveň 1. Po nastavení se čekalo na signál z vizualizace pro potvrzení bezpečnosti. V okamžiku když přijde tento signál, resetuji se chyby a Circuit reset se nastaví na 0. Tím se resetuje celý blok a aktivuje se výstup O1.

U obou bezpečnostních tlačítek je blok použit stejným způsobem. Externí stop tlačítko má jeden bezpečnostní kontakt rozpínací, proto musí být jeden signál SW invertován. Druhé bezpečnostní tlačítko umístěné na multifunkčním bloku není dvou

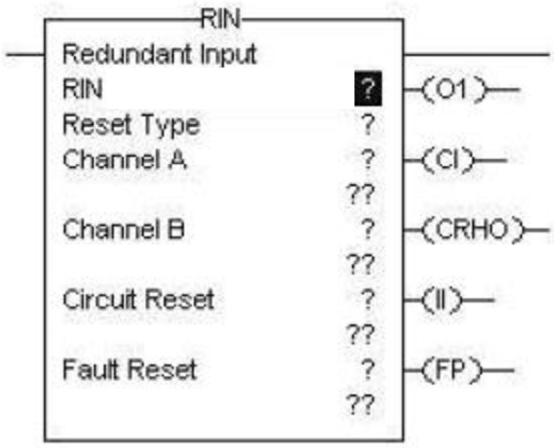
kontaktní, ale má pouze jeden bezpečnostní signál, proto je tento signál přiveden na Channal A i Channel B.



Obr. 6-3 Blok ESTOP [24].

RIN - Reduntant Input

Funkce RIN [24] je téměř totožná jako ESTOP, s tím rozdílem, že se musí definovat proměnnou typu Reduntant Input. Popis parametrů je uveden Obr. 6-4 a Tab. 6-1. Funkci jsem využil pro ovládání bezpečnosti zámku 440G-LZ a lze s ní pracovat úplně stejným způsobem jako ESTOP, viz předcházející kapitola.

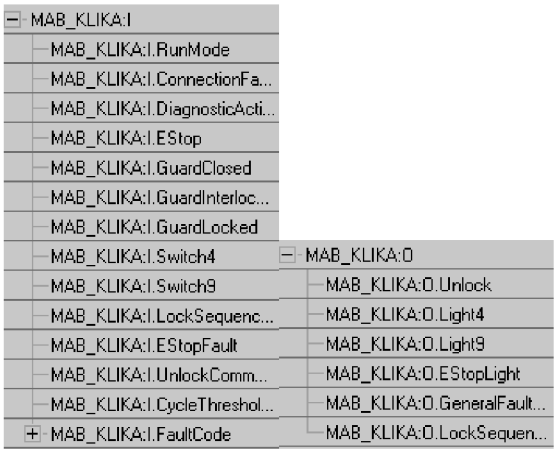


Obr. 6-4 Blok RIN [24].

Logika Multifunkčního bloku

Logika části programu pro ovládání multifunkčního bloku je velice jednoduchá. Po ethernetu do automatu se přenáší předdefinované vstupní/výstupní signály viz Obr. 6-5 a složité vnitřní bezpečnostní zapojení neřeším. V závislosti na těchto signálech jsou nastavovány/resetovány pomocné proměnné. Logiku programu multifunkčního bloku řeší network 13 až 18.

Po stisknutí červeného tlačítka (požadavek na odemčení) začnou obě tlačítka blikat a po zastavení motoru se nastavuje proměnná povolení odemčení. Následně je zámek odemčen. Při odemčení je červené tlačítko stále rozsvícené a zelené zhasnuté. Při požadavku na uzamčení začne blikat zelené tlačítko a červené zhasne. Zelené bude blikat tak dlouho, dokud není klika uzavřena a uzamčena poté se rozsvítí nepřerušovaným zeleným signálem pro signalizaci uzamčení nebezpečného prostoru. Z frekvenčního měniče do automatu nedostávám žádnou informaci o aktuálních otáčkách motoru, proto tento signál simuluju timerem. Timer nastaví proměnnou k povolení odemčení, až po uplynutí času 15 sekund, který je dostačující k úplnému zastavení motoru.



Obr. 6-5 Vstupní a výstupní signály multifunkčního bloku.

6.3 Řízení virtuální výrobní linky

Poslední částí mé diplomové práce je vizualizace výrobní linky. K tomuto účelu byl využit dříve zmíněný program Faktory I/O od společnostní RealGames.

Linka slouží k třídění materiálu a beden. Po prvním pravém pásu jezdí materiál bedny XL. Po levém pásu jezdí dva druhy beden. Při detekování materiálu na pravém pásu jej dvouosý překladač přendá na levý pás (pouze když v zóně založení není žádný předmět). Bedny XL jsou pouštěny dál. Po dopravě bedny nakonec pravého pásu je bedna pomocí tříosého překladače umístěna na předpřipravenou paletu. Po založení dvou beden na paletu je povelen transport k výtahu, který palety zakládá do volných pozic. Před výtahem jsou umístěna 4 čidla. Tyto čidla slouží k vytváření fronty z palet.

Na levém pásu probíhá další třídění materiálu a beden. Materiál je odsunut do leva pomocí výsuvného ramene a bedny jsou pouštěny rovně na další pás.

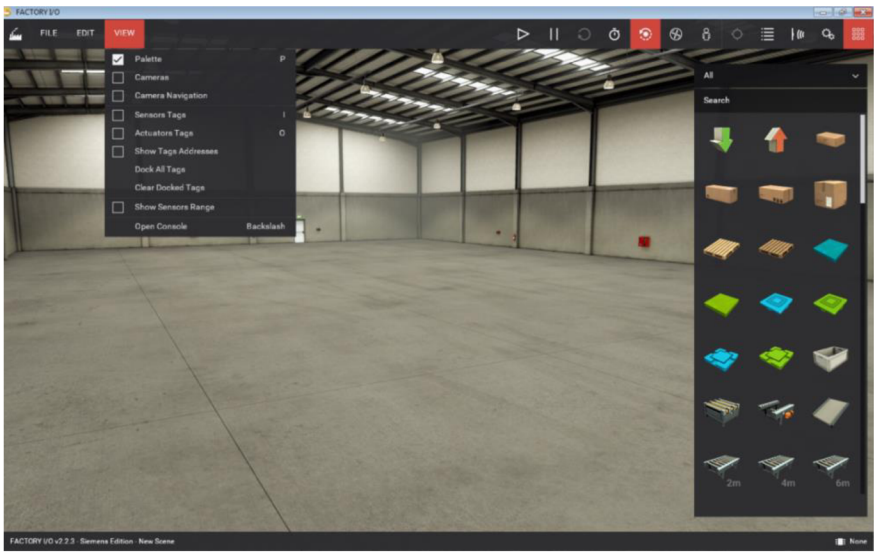
Hlavní ovládací panel je umístěn v popředí u plotu. Tento panel slouží k signalizaci stavů linky a jejímu ovládání. Jsou zde umístěny tlačítka pro potvrzení bezpečnosti, restování hlavních pracovišť a odemčení zámku.

6.3.1 Popis scény

Pracovní scéna Factory I/O je virtuální hala do které se umisťuji předdefinované prvky. V horní liště jsou umístěny tři záložky: FILE, EDIT a VIEW. Záložka FILE, slouží k otevírání souborů, ukládání konfiguraci ovladače a správě nastavení. Záložka EDIT slouží ke kopírování vkládání a výběru prvků. Poslední záložka VIEW umožňuje volby zobrazování palet, kamer, předefinovaných pohledů, názvů senzorů a akčních členů, adres tagů atd.

Po pravé straně jsou umístěny ovládací prvky vizualizace. Je tu tlačítko run, pause a reset. Dále následuje tlačítko pro zpomalení simulace na 0,1 násobek normální rychlosti. Poté následují dvě tlačítka pro volbu druhu kamery a poslední čtyři tlačítka slouží na zpravování tagů vizualizace.

Při spuštěné vizualizaci můžeme uchopit jakýkoliv interaktivní prvek nebo zmáčknout tlačítko. Dále je zde dostupná fyzika, čili prvky mohou padat, hromadit a lze je i přenášet posouvat atd. Zároveň je ale SW jednoduchý a HW nenáročný. Pracovní scéna je zobrazena na Obr. 6-6.



Obr. 6-6 Pracovní scéna Factory I/O.

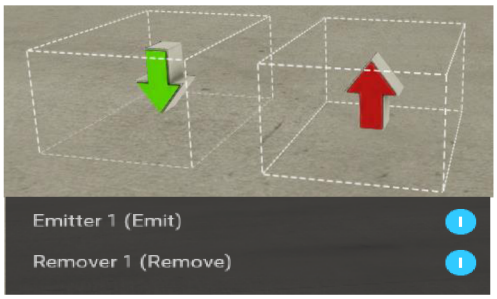
6.3.2 Použité prvky

Výrobní linka by se dala rozdělit na tři hlavní části: třídění materiálu a beden, skládání beden na palety a zakládání palet do policového systému. V této podkapitole jsou popsány ty nejzajímavnější prvky použité při modelování mojí výrobní linky.

Emitter a remover

Prvními prvky jsou tzv. emitter a remover, viz Obr. 6-7. Emitter slouží k vytváření prvků, které má výrobní linka zpracovávat (modrý/zelený materiál, různé velikosti

beden, palety, boxy atd.). Po kliknutí pravým tlačítkem můžeme prvkem parametrizovat a volit si maximální/minimální periodu vytváření prvků, náhodnou pozici prvků, druh prvků, zda mají být umístěny na paletu, nebo nikoliv, popřípadě prvkem rotovat, otáčet a posouvat. Remover slouží pouze k odstraňování prvků, aby se ve vizualizaci nehromadili. Dále je možné nastavit u prvků řízení pomocí proměnné z automatu, nebo stálý statický stav.



Obr. 6-7 Znázornění emitteru a removeru s ovládáním.

Pásy a rollery

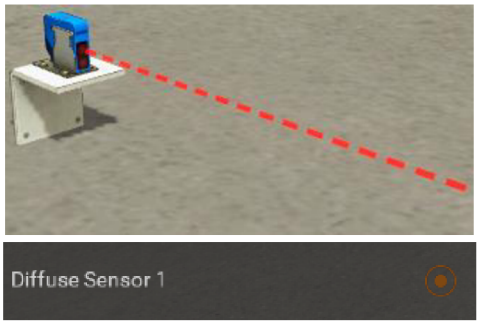
Nyní už se vytváří prvky a v tuto chvíli se musejí nějakým způsobem transportovat. K tomu slouží dopravníkové pásy a rollery, viz Obr. 6-8. Jsou k dispozici délky 2, 4 a 6 metrů. U každého pásu si po kliknutí pravým tlačítkem volíme možnost řízení digitálním, analogovým nebo kombinovaným způsobem.

V řízení mojí linky u dopravníků používám digitální režim a u rollerů analogový. U analogového řízení je dán rozsah -10 až 10 V a při maximálním napětí se roller točí rychleji, než u hodnoty logické 1. Směr otáčení u digitálního řízení určuje dvojice šipek na boční straně pásu.

Obr. 6-8 Znázornění dopravníku a rolleru s ovládáním.

Optické senzory

K detekci prvků na lince používám výhradně difuzní senzory. Reálný senzor je konstruován s přijímačem a vysílačem v jednom pouzdru. Vysílaný paprsek se odrazí od detekovaného předmětu zpět do přijímače a tím sepne senzor. Ve vizualizaci se výstup ze senzoru propojí s proměnnou v automatu. Znázornění senzoru z vizualizace viz Obr. 6-9.



Obr. 6-9 Znázornění difuzního senzoru.

Překladač dvouosý

Pomocí senzorů lze rozpoznávat materiál i bedny (každý prvek má rozdílnou výšku), ale je potřeba prvky třídit a přemisťovat. K tomu slouží dvouosý překladač, který je použit k přendání materiálu na druhý pás. Překladač je osazený přísavkou pro uchycení předmětu. Před samotným uchycením musí být předmět na správném místě. Přesun předmětu zajistí zasunující rameno. Opět si lze zvolit režim ovládání. V tomto případě jsem si zvolil analogové řízení, protože mohu obě osy přesně řídit signály 0 – 10 V a eliminuji potřebu zachycování hran při dokončení pohybu. Překladač je znárodněn na Obr. 6-10.

Obr. 6-10 Znázornění dvouosého překladače s ovládáním.

Překladač tříosý

Materiál z prvního pásu je přeložen na druhý a bedny jsou transportovány dál. Na konci pásu je umístěn tříosý překladač, který bedny horizontálně otáčí a umisťuje po dvou na předpřipravenou paletu. Opět jsem využil přesnosti analogového řízení překladače, protože u použití digitálního řízení, byl pohyb os řízen pomocí určeného počtu pulzů a při špatně zvolené synchronizaci osy nepřijely přesně nad určité místo. Znázornění tříosého překladače viz Obr. 6-11.

Obr. 6-11 Znázornění tříosého překladače s ovládáním.

Výtah

Posledním prvkem výrobní linky je výtah, který palety osazené krabicemi zakládá do 54 pozic. U tohoto prvku je použito analogově-digitální ovládání. Digitální řízení je využito pro navážení a vyvážení palet z výtahu, protože jsou sledovány pouze krajní pozice. Analogové řízení používám k pohybu os X a Z pro zakládání palet do polic. Znázornění výtahu viz Obr. 6-12.

Obr. 6-12 Znázornění výtahu s ovládáním.

Ovládací panel

K ovládání vizualizace slouží řídicí prvky Factory I/O: pauza, start vyčistění prvků atd. Nicméně bylo potřeba přidat několik základných prvků pro řízení a to: tlačítko pro potvrzení bezpečnosti (levé horní tlačítko, bliká při požadavku na potvrzení), signalizace stavu a řízení zámku (signálky pod ním a tlačítka vlevo dole, zelené uzamče, červené odemče zámek), tlačítka pro resetování kroků překladačů a výtahu (první pravé- reset dvouosý překladač, pravé prostřední-reset tříosý překladač a pravé spodní-reset výtah). Dále byl na panel umístěn výstražný maják, který se rozsvítí při poruše bezpečnosti a signálky pro určení stavu linky. K tomuto panelu by v reálném provozu měla přístup proškolená obsluha. Proto je umístěn před ochranným plotem. Panel je zobrazen na Obr. 6-13.

Obr. 6-13 Znázornění ovládacího panelu.

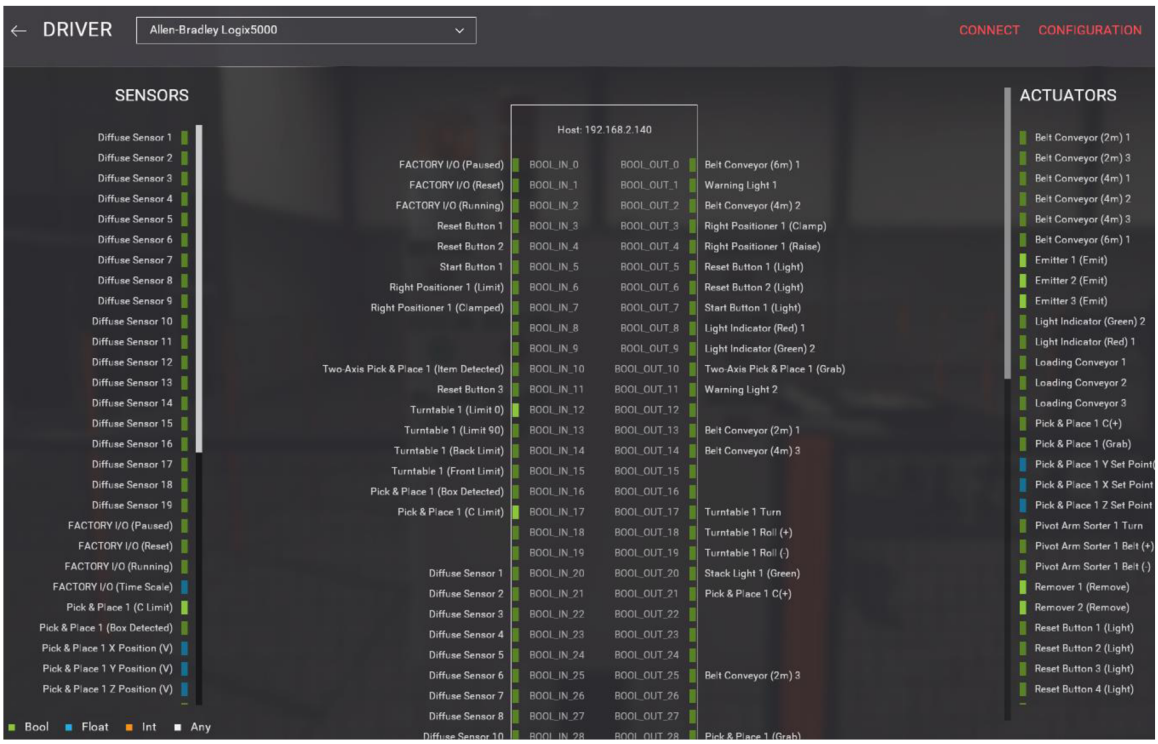
6.3.3 Propojení vizualizace s automatem

Propojení vizualizace s programovatelným automatem je velice jednoduché. Prvním krokem je v SW Factory I/O kliknout na záložku FILE >> DRIVER, poté se otevře okno pro konfiguraci ovladače, viz Obr. 6-14. Po rozkliknuti se otevře záložka CONFIGURATION a otevře se okno, viz Obr. 6-15. V tomto okně si zvolím, s jakým zařízením chci SW Factory I/O propojit, v mém případě je to Allen-Bradley Logix5000. Dále vyplním IP adresu a nadefinuji počty potřebných I/O signálů. Při tvorbě mojí vizualizace bylo nutné nadefinovat přes 100 vstupních a výstupních signálů. SW Factory I/O se v podstatě nepřipojuje k automatu, ale k SW RSLogix5000.

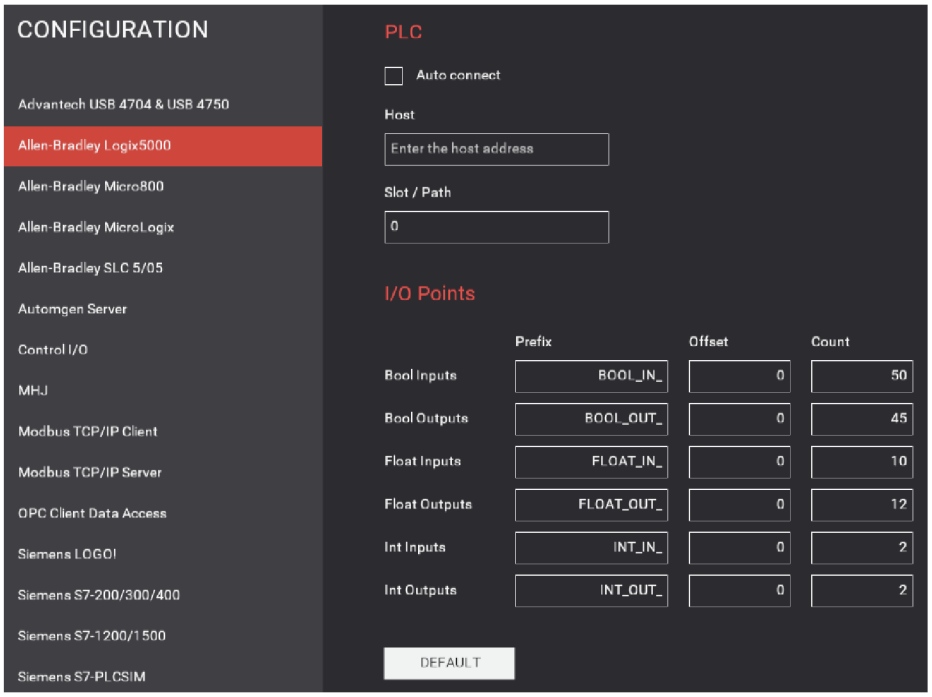
Poté se vrátí zpět na předchozí okno driver, ve kterém probíhá mapování vstupů a výstupů všech použitých prvků na scéně. Jednoduchým přesunutím k některému portu, ze zobrazeného pouzdra DIL, se přiřadí příslušnou ovládanou proměnnou.

Podmínkou správné funkčnosti je mít v automatu pojmenovány proměnné typu boolean vstupní - BOOL_IN_X, výstupní BOOL_OUT_X nebo proměnné typu real pod názvem FLOAT_OUT_X, viz Obr. 6-16. Po downloadu programu do automatu lze dát ve Factory I/O CONNECT, a tím vizualizaci propojit s automatem. Je nutné

podotknout, že po každém přehrání konfigurace programovatelného automatu je potřeba odpojit a zase připojit DRIVER Factory I/O, viz Obr. 6-15.



Obr. 6-14 Otevření záložky DRIVER.



Obr. 6-15 Okno CONFIGURATION.

BOOL_IN_0	0		Decimal	BOOL	Standard	Fackt i/o pause
BOOL_IN_1	0		Decimal	BOOL	Standard	Fackt i/o reset
BOOL_IN_2	0		Decimal	BOOL	Standard	Fackt i/o start
BOOL_IN_3	0		Decimal	BOOL	Standard	Potvrzeni_bezpečnosti
BOOL_IN_4	0		Decimal	BOOL	Standard	Zamek_odemčeni
BOOL_IN_5	0		Decimal	BOOL	Standard	Zamek_zamčit
BOOL_IN_6	1		Decimal	BOOL	Standard	Stlač_hode/dole_limit_6m_P
BOOL_IN_7	0		Decimal	BOOL	Standard	Stlač_stlačeno_6m_P
BOOL_IN_8	0		Decimal	BOOL	Standard	
FLOAT_IN_0	0.0		Float	REAL	Standard	Vytah__aktual_pozice_X
FLOAT_IN_1	0.0		Float	REAL	Standard	Vytah_Z
FLOAT_IN_2	0.0		Float	REAL	Standard	Skladani_beden_S_Y

Obr. 6-16 Příklad mapování proměnných z Factory I/O.

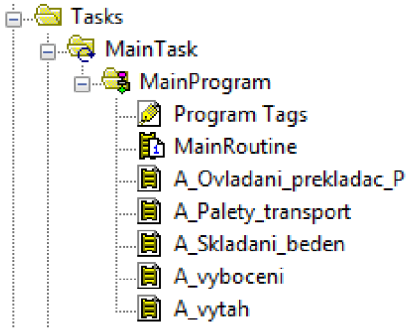
6.3.4 Program řízení linky

Program pro řízení linky byl rozdělen do několika podprogramů, které jsou aktivovány z hlavního programu. V hlavním programu jsou řízeny signály pro pohyb pásů, aktivace podprogramů a vložena nezbytná logika pro řízení.

Program obsahuje celkem 5 podprogramů (SubRoutine), které běží paralelně. Jedná se o rutiny, viz Obr. 6-17. Každá rutina slouží k činnosti dle jejího názvu. Všechny použité proměnné jsou globální, čili řízení lze navzájem prolínat. Řízení probíhá přes mapované signály z vizualizace Factroy I/O.

K řízení sekvenčních části jako je překládání materiálu z jednoho pásu na druhý, skládání beden na paletu, nebo zakládání palet do pozic v regálovém systému byla využita sekvence kroků. Po dokončení dané činnosti se prvek z vizualizace nastaví do „home“ pozice. Po jejím dosažení se kroky resetují a cyklus začíná znovu. Výhodou takového řízení je fakt, že při zastavení vizualizace porušením bezpečnosti lze přesně zjistit, kde se stroj zastavil a následně se program znovu spustí z tohoto místa.

Všechny podprogramy jsou aktivovány pouze v případě, že je bezpečnost v pořádku. V opačném případě se neaktivují. Problém však nastane v okamžiku, když se deaktivuje bezpečnost a program je v podprogramu. V takovém případě se program vykonává dál. Proto byl do každého podprogramu přidán vstupní parametr, který je realizován proměnnou řídicí bezpečnost. Tento parametr je přidán jako rozpínací kontakt ke každému networku, tím se zajistí zastavení programu při porušení bezpečnosti. Celý výstup z programu RSLogix5000 je uveden jako elektronická Příloha - 2.



Obr. 6-17 Podprogramy pro řízení vizualizace.

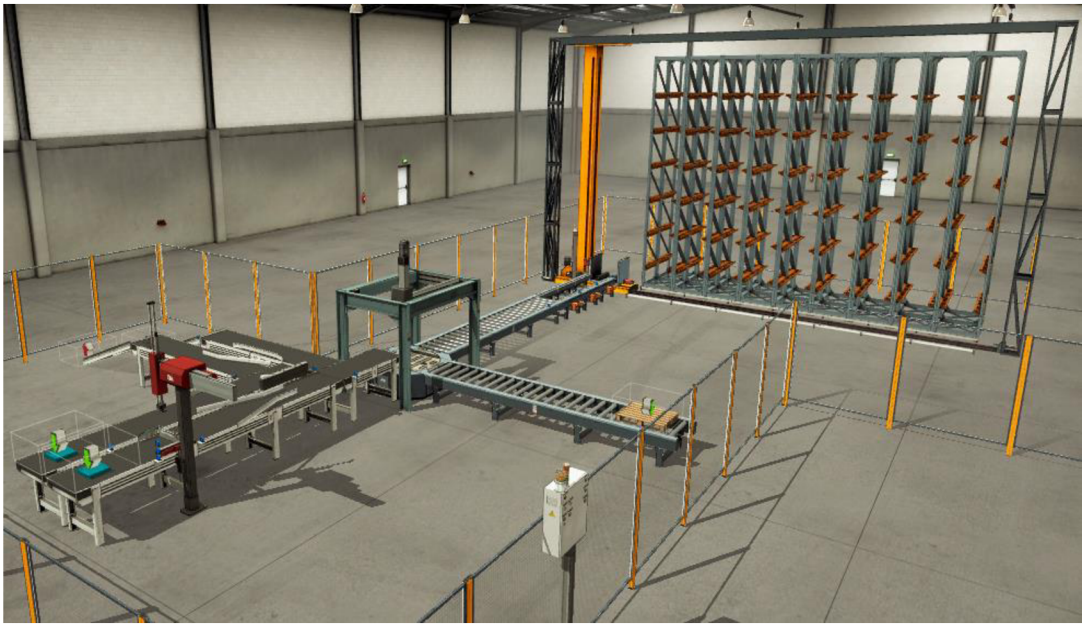
6.4 Zhodnocení realizace laboratorní úlohy

Obsluha bezpečnostních funkcí zadaných v zadání laboratorní úlohy, viz podkapitola 6.1, byla vytvořena v safety části programu.

Výrobní linka reaguje na porušení bezpečnosti zastavení akčních členů. Po následném potvrzení bezpečnostního okruhu akční členy odstartují svůj pohyb v té pozici, ve které se zastavily. Jelikož nemonitorují pohyb prvků v každé pozici na lince a u některých čidel jsou použity nástupné nebo sestupné hrany. Může nastat případ, že se nějaký prvek linky zasekne. V průmyslu by tento stav řešila obsluha, popřípadě proškolený personál. V mém řešení úlohy se buď může restartovat vizualizace i s překladači a výtahem, nebo pouze zaseknutý segment v poruše. V případě zaseknutého materiálu, se může tento materiál pomocí myši uchytit a odebrat.

Při testování odpojení některého z bezpečnostního signálu, nebo přerušení ethernetového spojení s jakýmkoliv modulem dojde k zastavení linky. Reakce je očekávána, protože tím dojde k poruše bezpečnosti nebo nestandardnímu stavu. Opětovná aktivace je možná pouze obnovením spojení signálu a následovným restartováním automatu nebo modulů v poruše.

Fotografie vizualizace viz Obr. 6-18. Videozáznam z demonstrace reakce na safety komponenty, viz Příloha - 3.



Obr. 6-18 Model výrobní linky

7 ZÁVĚR

Prvním bodem zadání bylo popsat technologii CIP. Tento bod byl rozdělen na dvě hlavní kapitoly s číslem dvě a tři. Druhá kapitola s názvem průmyslové komunikační sítě pojednává o modelu ISO/OSI a o průmyslových komunikačních sítích EtherNet/IP™, DeviceNet™, CompoNet™ a ControlNet™, které z již zmíněného modelu vycházejí a přímo souvisejí s univerzálním komunikačním protokolem CIP.

Třetí kapitola obsahuje popis technologie CIP, který je používán pouze v horních vrstvách modelu ISO/OSI. Rozebrány byly jeho vnitřní principy, funkce a rozšíření CIP Energy, CIP Sync, CIP Motion, CIP Security a CIP Specification libraly.

Ve čtvrté kapitole byl vytvořen podrobnější popis rozšíření CIP Safety. CIP Safety, jak již název napovídá, přímo souvisí s technologií CIP. Čtvrtá kapitola podrobněji vysvětluje vnitřní princip, návaznosti a rozdíly CIP Safety.

V páté kapitole byly popsány dostupné SW nástroje a komponenty s podporou komunikačního protokolu CIP Safety. Následně byl vytvořen rozbor s popisem komponentů, a možností připojení I/O periferií. Po seznámení se s komponenty následuje podkapitola o vytvoření topologie a samotného schéma zapojení laboratorní úlohy. Kapitoly jsou pro lepší představu doplněny o obrázky a bloková schémata. Po rozboru bylo provedeno fyzické zapojení komponentů a vytvoření funkční HW konfigurace.

V šesté kapitole této práce bylo formulováno zadání laboratorní úlohy. Po jeho formulaci následuje vlastní SW řešení laboratorní úlohy. Je zde popsáno rozdělení programu, proměnných a nastínění logiky celého pracoviště. Popis začínám rozborem bezpečnostní části programu, která je stěžejní návrh řízení vizualizace. Následuje kapitola s popisem tvorby vizualizace a propojení automatu s vizualizačním programem. Poslední podkapitolou je popis vlastního řešení SW ovládání virtuální linky realizované v programu Factory I/O.

Zadání diplomové práce bylo splněno v plném rozsahu. Výstupem mojí diplomové práce jsou: obsáhlá literární rešerše o technologii CIP, osazení, zapojení, oživení laboratorního panelu dostupnými komponenty, zformulování zadání laboratorní úlohy a její následné SW vyřešení. V elektronických přílohách je umístěn kompletní výstup mého SW řešení z programu RSLogix5000 a demonstrační video s reakcemi vizualizace linky na porušení bezpečnosti.

Moji práci by bylo možné v budoucnu rozšířit o další bezpečnostní komponenty, použití managerovatelného switche pro vytvoření topologie typu kruh a následného odposlouchávání CIP Safety telegramů, rozšíření vizualizace o další dostupné prvky nebo vytvoření ovládání a signalizace stavu linky pomocí interaktivního dotykového, či simulovaného panelu v prostředí např. InTouch nebo FactoryTalk.

Literatura

[1] ZEZULKA, František a Ondřej HYNČICA. Průmyslový Ethernet II: Referenční model ISO/OSI. *AUTOMA* [online]. Praha: FCC Public, 2007, 13 (č. 3), 86-90 [cit. 2017-10-23]. Dostupné z: http://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-ii-referencni-model-iso/osi-2007_03_34209_3890/

[2] SCHIFFER V., VANGOMPEL D. J., ROMITO R. A., VOSS K., The Common Industrial Protocol (CIP™) and the Family of CIP Networks. *ODVA, Inc.* [online]. ODVA: 2016, (PUB00123R1), 134 [cit. 2017-10-17]. Dostupné z: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00123R1_Common-Industrial_Protocol_and_Family_of_CIP_Networks.pdf

[3] ODVA. Network infrastructure for EtherNet/IP: Introduction and consideration. *ODVA, Inc.* [online]. ODVA, 2007, (PUB00035R0), 118 [cit. 2017-10-20]. Dostupné z: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf

[4] ZEZULKA, František a Ondřej HYNČICA. Průmyslový Ethernet IX:EtherNet/IP, EtherCAT. *AUTOMA* [online]. Praha: FCC Public, 2008, 14 (č. 10), 60-65 [cit. 2017 10-17]. ISSN 1210-9592. Dostupné z: http://automa.cz/Aton/FileRepository/pdf_articles/37910.pdf

[5] ODVA. DeviceNet™ – CIP on CAN Technology. *ODVA, Inc.* [online]. 2016, (PUB00026R4), 8 [cit. 2017-11-07]. Dostupné z:https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00026R4_Tech-Adv-Series-DeviceNet.pdf

[6] ODVA. CompoNet™ – CIP on TDMA. *ODVA, Inc.* [online]. 2016, (PUB000131R1), 8 [cit. 2017-11-11]. Dostupné z: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00161R1_Tech-Series-CompoNet.pdf

[7] ODVA. ControlNet™ - CIP on CTDMA Technology. *ODVA, Inc.* [online]. 2016, (PUB00200R1), 8 [cit. 2017-11-12]. Dostupné z: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00200R1_Tech-Series-ControlNet.pdf

[8] ODVA. About ODVA. *ODVA, Inc.* [online]. ODVA: 2017 [cit. 2017-10-10]. Dostupné z: https://www.odva.org/About-ODV

[9] CIP Security. *ODVA, Inc.* [online]. [cit. 2017-12-05]. Dostupné z: https://www.odva.org/Technology-Standards/Common-Industrial-Protocol-CIP/CIP-Security

[10] CIP Specification Library. *ODVA, Inc.* [online]. [cit. 2017-12-05]. Dostupné z: https://www.odva.org/Technology-Standards/Common-Industrial-Protocol-CIP/CIP-Specifications-Library

[11] VASKO, David. CIP Safety: Safety networking for today and beyond. *ODVA, Inc.* [online]. ODVA, (PUB00110R1), 8 [cit. 2017-12-26]. Dostupné z: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00110R1_CIP_Safety_White_Paper.pdf

[12] RealGames [online]. Portugalsko, ©2006-2018 [cit. 2018-04-19]. Dostupné z: https://realgames.co/

[13] ROCKWELL, Automation. POINT I/O Modules: Publication 1734-SG001F-EN-P. *Rockwell Automation*[online]. 2015, Září 2015, 72 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/sg/1734-sg001_-en-p.pdf

[14] ROCKWELL, Automation. POINT Guard I/O Safety Modules: Publication 1734-UM013N-EN-P. Rockwell Automation [online]. 2017, Září 2017, 231 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1734-um013_-en-p.pdf

[15] ROCKWELL, Automation. 442G Multi-functional Access Box: Publication 442G-UM001A-EN-P. *Rockwell Automation* [online]. 2015, 1.5.2015, 52 [cit. 2018-04-21]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/442g-um001_-en-p.pdf

[16] ROCKWELL, Automation. Multifunctional Access Box with CIP Safety over EtherNet/IP: Publication 442G-UM002A-EN-P. Rockwell Automation [online]. 2016, Prosinec 2016, 60 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/442g-um002_-en-p.pdf

[17] ROCKWELL, Automation. Guardmaster® EtherNet/IP Network Interface: Publication 440R-UM009B-EN-P. *Rockwell Automation* [online]. 2014, Únor 2014, 64 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/440r-um009_-en-p.pdf

[18] ROCKWELL, Automation. Guardmaster Safety Relays: Publication 440R-UM013E-EN-P. Rockwell Automation [online]. 2017, 1.3.2017, 100 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/440r-um013_-en-p.pdf

[19] ROCKWELL, Automation. Guardmaster Guard Locking Switch: Publication 440G-UM001B-EN-P. Rockwell Automation [online]. 2017, Únor 2017, 44 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/440g-um001_-en-p.pdf

[20] ROCKWELL, Automation. GuardShield Safety Light Curtain: Publication 450L-UM001B-EN-P. Rockwell Automation [online]. 2018, Únor 2018, 144 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/450l-um001_-en-p.pdf

[21] ROCKWELL, Automation. Střídavý frekvenční měnič řady PowerFlex 520: Publikace 520-UM001D-CS-E. Rockwell Automation [online]. 2013, Září 2013, 238 [cit. 2018-04-20]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/520-um001_-cs-e.pdf

[22] SIEMENS. SIMOTICS nízkonapěťové trojfázové asynchronní motory nakrátko podle IEC: D 81.1 CZ. *Siemens, s.r.o.* [online]. 2016, 250 [cit. 2018-04-20]. Dostupné z: http://www.elektromotory.net/upload/file/katalog_1le1.pdf?s=21020730

[23] HIRSCHMANN. RS2-../.. Management Manual: Industrial ETHERNET Rail Switch 2. Hirschmann [online]. 2004, 334 [cit. 2018-04-20]. Dostupné z: ftp://ftp.hirschmann-usa.com/INET-IndustrialNetworking/Manuals/Discontinued%20Products/RS2-XX_XX/HB_RS2_90_us.pdf

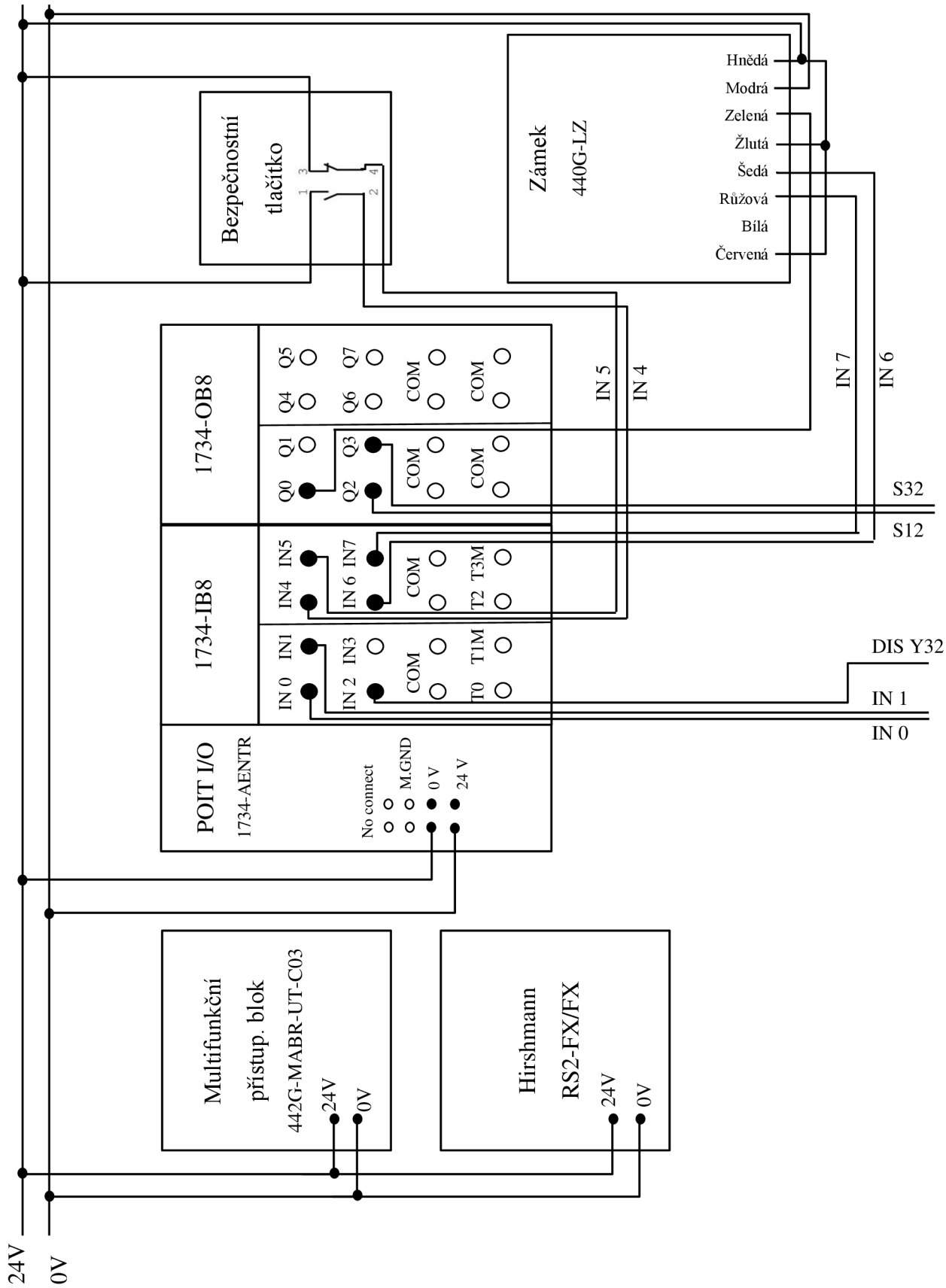
[24] ROCKWELL, Automation. GuardLogix Safety Application Instruction Set: 1756-RM095I-EN-P. Rockwell Automation [online]. 2018, Únor 2018, 602 [cit. 2018-05-02]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pd

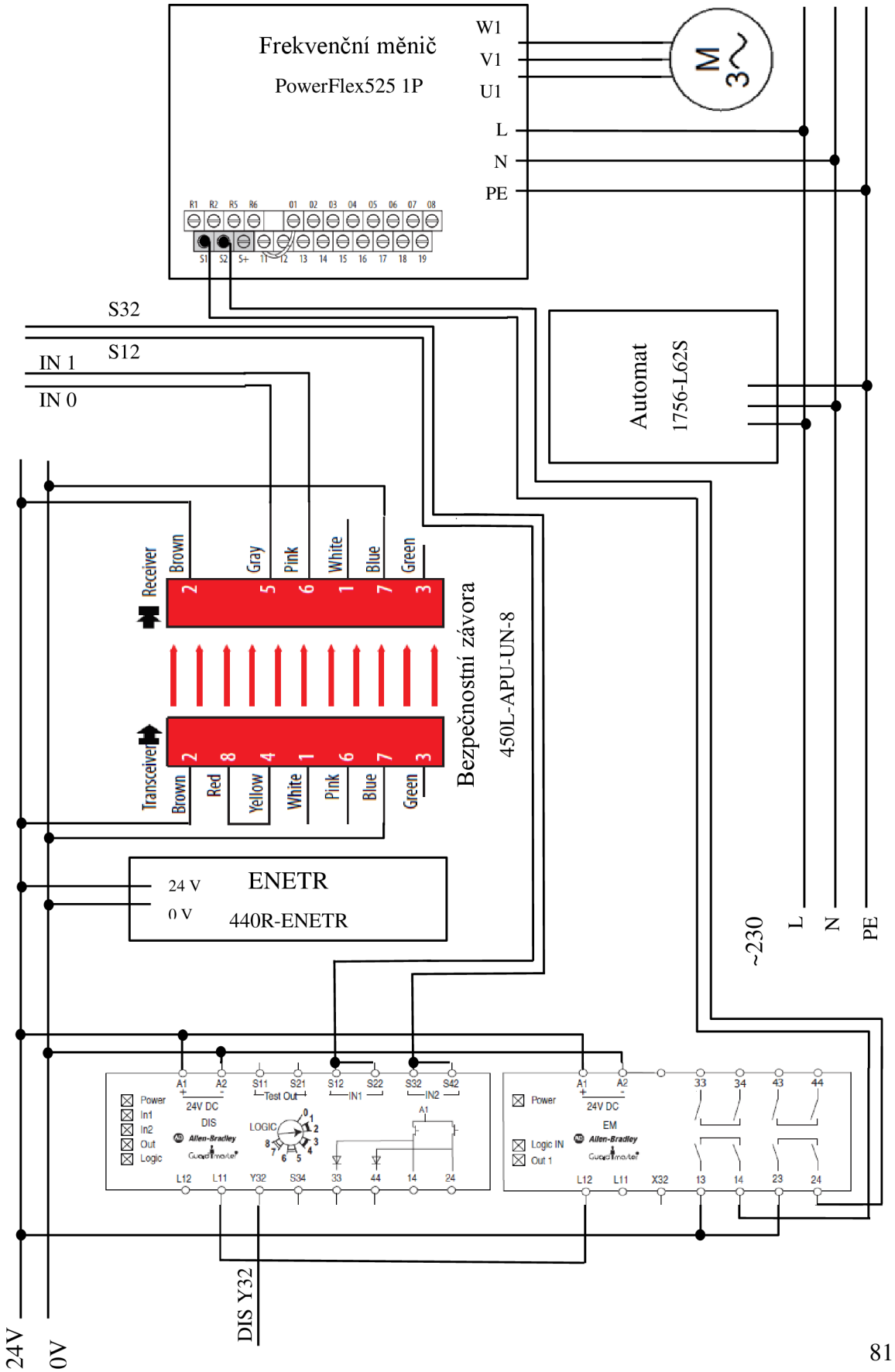
Seznam příloh

Seznam elektronických příloh na DVD

Příloha 2 - Zdrojový kód programu.
Příloha 3 - Demonstrační video.
Příloha 4 - Projekt z SW RSLogix5000
Příloha 5 - Simulace linky ve Factory I/O

Příloha 1 - Elektrické schéma zapojení komponentů




Frekvenční měnič
PowerFlex525 1P
W1
V1
U1
L
N
PE
M
3~
S32
S12
IN 1
IN 0
Automat
1756-L62S
Receiver
Brown
Gray
Pink
White
Blue
Green
Transceiver
Brown
Red
Yellow
White
Pink
Blue
Green
Bezpečnostní závora
450L-APU-UN-8
ENETR
24 V
0 V
440R-ENETR
~230
L
N
PE
Power
In1
In2
Out
Logic
24V DC
DIS
Test Out
IN1
IN2
LOGIC
Logic IN
Out 1
EM
DIS Y32
24V
0V