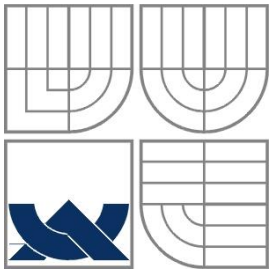
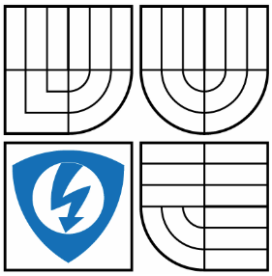


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF CONTROL AND INSTRUMENTATION

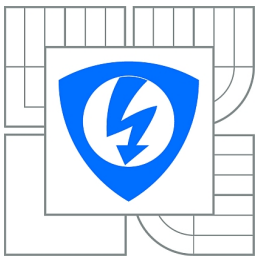
CIP SAFETY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS.-

AUTOR PRÁCE
AUTHOR
Bc. MILAN ŠINDELEK

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. RADEK ŠTOHL, Ph.D.

BRNO 2016



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav automatizace a měřicí techniky

Diplomová práce

magisterský navazující studijní obor
Kybernetika, automatizace a měření

Student:	Bc. Milan Šindelek	***ID:***	146109
Ročník:	2	***Akademický rok:***	2015/2016

NÁZEV TÉMATU:

CIP Safety

POKYNY PRO VYPRACOVÁNÍ:

1. Proveďte literární rešerši o technologii CIP a především CI Safety.
2. Navrhněte a realizujte dvě výukové bezpečnostní laboratorní úlohy s použitím CIP Safety technologií.
3. Proveďte zhodnocení rizik dvou demonstračních úloh.
4. Vytvořte demonstrační programové vybavení pro Safety PLC.
5. Vytvořte příslušnou vizualizaci dvou laboratorních úloh.
6. Ověřte funkčnost svého řešení.

DOPORUČENÁ LITERATURA:

CIP Common Specification. ODVA.
CIP Safety Specification. ODVA.
Dle vlastního literárního průzkumu a doporučení vedoucího práce.

Termín zadání:	8.2.2016	***Termín odevzdání:***	16.5.2016

Vedoucí práce: Ing. Radek Štohl, Ph.D.
Konzultanti diplomové práce:

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

UPOZORNĚNÍ:

Abstrakt

Diplomová práce se zabývá zabezpečením strojního zařízení pomocí dostupných technologií. Obsahuje postup posouzení a snížení rizika stroje, návrh bezpečnostních opatření a jejich aplikaci. V jednotlivých částích jsou uvedeny popisy použitých norem, komunikace pomocí CIP Safety technologii, návrh a realizace bezpečnostních opatření stroje na dvou demonstračních výukových úlohách.

Klíčová slova

Funkční bezpečnost, CIP Safety, posouzení rizik, bezpečnostní prvky, Safety Automation Builder, SISTEMA

Abstract

This master's thesis deals with the security machinery using available technologies. It contains a description to assess and reduce the risk of machine design of security measures and their application. In each section are provides descriptions of the standards, using the CIP Safety communication technology, design and implementation security measures of machine at two demonstration learning tasks.

Keywords

Functional safety, CIP Safety, risk assessment, safety components, Safety Automation Builder, SISTEMA

Bibliografická citace:

ŠINDELEK, M. *CIP Safety*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2016. 73s. Vedoucí diplomové práce byl Ing. Radek Stohl, 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: **16. května 2016** ……

podpis autora

Poděkování (nepovinné)

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

V Brně dne: **16. května 2016** …….

podpis autora

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

1 ÚVOD

V současné době se v průmyslové výrobě rozmáhá masivní automatizace výrobních procesů. I přes tento technologický pokrok jsou i nadále do výrobního procesu zapojeni lidé, buď jako obsluha strojů, nebo jako jejich servis. Vedle morálního závazku nikomu neublížit, existuje legislativa vyžadující zajištění bezpečnosti strojů a prevenci nehod. Z těchto důvodu je nutné pří návrhu automatizovaných procesů myslet na strojní bezpečnost, to se týká jak návrhu technologického procesu výroby, tak ochrany pracovníků obsluhy strojních zařízení a jejího servisu.

Při návrhu a realizaci bezpečnostních opatření postupují konstruktéři podle příslušných norem. První fází návrhu je posouzení rizik, která musí být zpracována pro každé strojní zařízení. V tomto kroku nalezená rizika je nutné snížit na minimum pomocí bezpečnostních opatření a následně ověřit správnost návrhu. Tomuto procesu se věnuje první část diplomové práce.

Moderní automatizace se stále vyvíjí a současně s ní i řešení bezpečnosti výroby, která již dávno není řešena pouze STOP tlačítkem s funkcí centrálního vypnutí stroje. Je to soubor rozsáhlých bezpečnostních opatření, které na sebe vzájemně navazují a zahrnují nejen bezpečnost pracujících osob ale také bezpečnost výrobních zařízení (zabezpečení kolizních stavů).

V současné době jsou jednotlivé bezpečnostní funkce (systémy) tvořeny podle architektury: Vstupní zařízení – Logické zařízení – Výstupní zařízení. Požadavkem na zařízení je jistá míra spolehlivosti, která se určuje podle propojení mezi zařízeními (jednožilové, více žilové nebo zpětnovazební propojení). Množství a typ propojení těchto systémů se volí podle složitosti celkového projektu stroje. Výrobce bezpečnostní instrumentace Rockwell Automation nabízí dva typy logických zařízení. Pro jednodušší, 1 až 2 zónové projekty výrobce doporučuje použít levnější variantu s použitím bezpečnostních relé, pro více zónové projekty pak bezpečnostní PLC. Zde jsou jednotlivé bezpečnostní komponenty propojeny na síťové úrovni.

V této diplomové práci budou používány jak bezpečnostní relé tak bezpečnostní PLC. Jednotliví komponenty budou propojeny sítěmi EtherNet/IP nebo DeviceNet. Aby po těchto sítích mohly komunikovat i bezpečnostní moduly, byl společnostní ODVA vytvořen speciální protokol CIP Safety. Zařízení komunikující tímto protokolem garantují bezpečnou komunikaci a při poruše sítě se uvedou do bezpečného stavu.

Poslední část obsahuje popis vizualizaci druhé demonstrační úlohy.

2 STROJNÍ BEZPEČNOST

2.1 Legislativa

Jak již bylo zmíněno v úvodu, automatizovaný stroj není nikdy plně automatizován, ale vždy je do nějaké míry ovládán obsluhou. Již při navrhování stroje je třeba brát bezpečnostní opatření v úvahu. Správná volba bezpečnostních prvků a software může ochránit operátora od úrazu nebo samotný stroj proti nežádoucímu poškození. Opatření ke snížen rizik můžou dokonce vést ke zvýšení produktivity a ekonomickému přínosu, jakou jsou např. nižší léčebné náklady související s nehodami, zjednodušení obsluhy a tím zrychlení výroby, minimalizace odstávek spojených s údržbou a menší pravděpodobnost kolize stroje.

Výrobci, dovozci a distributoři mají podle legislativy České republiky povinnost uvádět na trh pouze bezpečné výrobky. Bezpečnost těchto výrobků se posuzuje podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů. V tomto zákoně jsou definovány „stanovené výrobky“, které jsou rozděleny do 33 skupin. Strojních zařízení se týkají především následující nařízení vlády, které jsou přejaté ze směrnic EU.

- NV 176/2008 Sb. O technických požadavcích na strojí zařízení.
- NV 17/2003 Sb. Technické požadavky na elektrická zařízení nízkého napětí.
- NV 616/2006 Sb. O technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility.

V těchto nařízení vlády jsou vyjmenovány normy, které musí výrobky splňovat, aby mohly získat prohlášení o shodě - CE. Tuto shodu posuzuje tzv. notifikovaná osoba.

2.2 Normy

Používání bezpečnostních komponentů se řídí podle směrnic týkajících se strojních zařízení, aby se zajistila určitá minimální úroveň bezpečnosti strojů a zařízení prodávaných v EU. Při návrhu bezpečnostních opatření postupujeme dle příslušných norem.

Normy týkající se strojní bezpečnosti pro Českou republiku jsou rozděleny to tří skupin:

- Normy typu A (základní bezpečnostní normy) stanovují základní pravidla, zásady konstrukčních principů, terminologie a obecné faktory, které se vztahují na veškerá strojní zařízení.

- Normy typu B (skupinové bezpečnostní normy) řeší určité bezpečnostní hledisko nebo jeden typ bezpečnostního zařízení, který lze použít v rámci širokého rozsahu strojních zařízení.
    - Typu B1 se zabývá konkrétními bezpečnostními faktory.
    - Typu B2 se zabývá konkrétními bezpečnostními prvky.

- Normy typu C (bezpečnostní normy strojních zařízení) kladou detailní bezpečnostní požadavky na určité stroje nebo skupinu strojů.

2.3 Popis normy ČSN EN ISO 13849-1

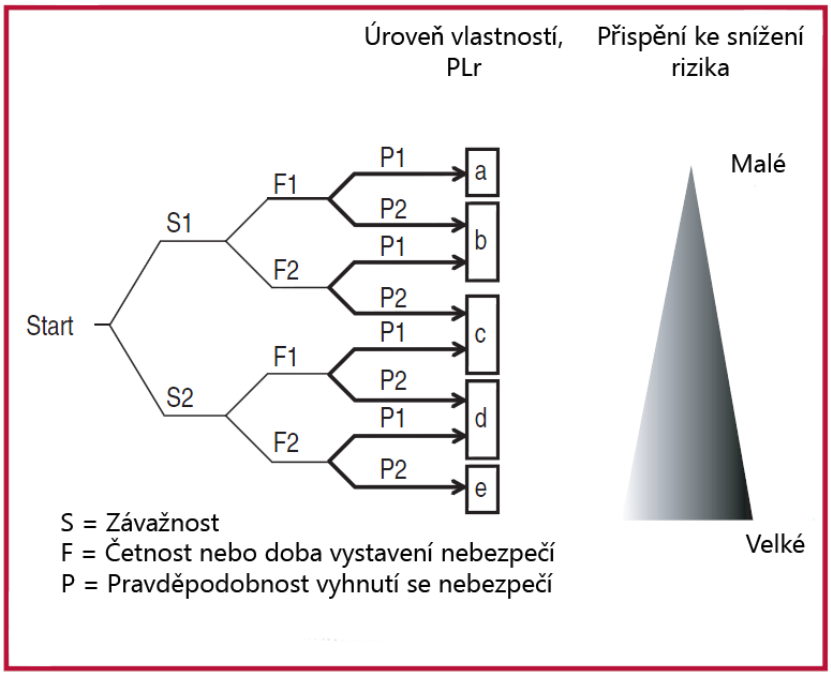
Jednou z nejvýznamnějších norem, která řeší návrh a konstrukci bezpečnostních částí ovládacích systémů je norma ČSN EN ISO 13849-1:2007 *Bezpečnost strojních zařízení. Bezpečnostní části ovládacích systémů. Část 1: Všeobecné zásady pro konstrukci.* Udává požadavky a pokyny pro konstruování a integrace částí ovládacích systémů (SRP/CS), které mohou obsahovat hardware i software. Kromě bezpečnostních funkcí mohou SRP/CS poskytovat také provozní funkce. Norma je platná pro komponenty všech technologii (elektrické, mechanické, hydraulické i pneumatické). Nezabývá se konkrétními bezpečnostními funkcemi a úrovní vlastností pro jednotlivé případy, ale uvádí požadavky na bezpečnostní části ovládacích systémů (SRP/CS), které jsou založeny na bázi programovatelných elektronických systémů.

Norma se zabývá snížením rizika použitím adekvátních ovládacích a bezpečnostních systémů. Pro uplatnění postupů v této normě je potřeba mít zpracovanou analýzu rizik. Norma zavádí pojem „Úroveň vlastností“ neboli PL (Peformance Level). Je definována jako průměrná pravděpodobnost nebezpečné poruchy za hodinu (PFHd). Používá se v pěti úrovních, kdy PL-a je nejnižší a PL-e je nejvyšší. V tabulce 2.1 je uveden vztah mezi hodnotou integrity SIL (definuje norma ČSN EN 61508) a úrovní vlastnosti PL. Mezi další pojmy, které jsou zde uvedeny, patří střední doba od nebezpečného selhání ($MTTF_d$), diagnostické pokrytí (DC) a selhání se společnou příčinou (CCF).

Tabulka 2.1: Vztah mezi PL, SIL a PFH [1]

PL	SIL	PFHd [h^{-1}]
a	-	$\geq 10^{-5}$ do $<10^{-4}$
b	1	$\geq 3x10^{-5}$ do $<10^{-5}$
c	1	$\geq 10^{-6}$ do $<3x10^{-6}$
d	2	$\geq 10^{-7}$ do $<10^{-6}$
e	3	$\geq 10^{-8}$ do $<10^{-7}$

V normě je definován způsob určení požadované úrovně vlastností (PLr) pomocí rozhodovacího grafu (Obrázek 2.1). Pro splnění bezpečnostních podmínek je nutné dokázat, že dosažená hodnota PL je větší nebo rovna požadované hodnotě PLr.

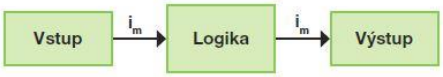
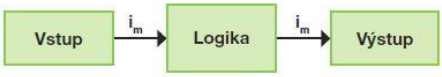
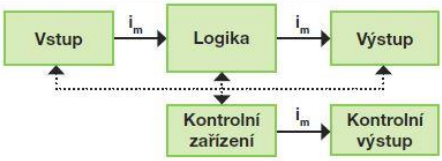
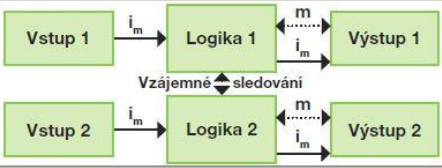
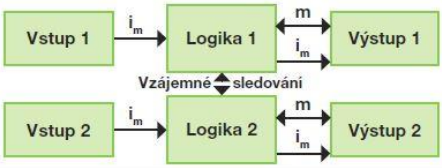


Obrázek 2.1: Graf rizika pro určení požadované úrovně vlastností PL [1]

Při určení závažnosti možného zranění obsluhy klasifikujeme do kategorie S1 běžné úrazy jako lehké zlomeniny, tržné rány, pohmožděniny aj. Závažností S2 jsou ohodnoceny těžká zranění, obvykle s trvalými následky (amputace, rozdrcení, otevřená zlomenina). Četnost F1 charakterizuje minimální dobu vystavení nebezpečí. Parametr F2 má být zvolen tehdy, je-li osoba vystavena nebezpečí často nebo nepřetržitě. Přesnou hranici mezi F1 a F2 nelze specifikovat. Při volbě tohoto parametru je důležité vědět, zda může být nebezpečná situace poznána a za jak dlouho úraz nastane. Mezi další hlediska patří provoz s dozorem nebo bez dozoru, obsluha s odborníky nebo laiky, rychlost s jakou vzniká nebezpečí, možnost vyvarování se nebezpečí aj. Parametr P2 má být zvolen tehdy, není-li žádná možnost vyloučení nebezpečí.

Další důležité téma, kterému se tato norma věnuje, je dělení bezpečnostních funkcí do několika architektur. Při návrhu zařízení si podle hodnocení rizika a výsledné požadované úrovně PLr vybere konstruktér kategorii, podle které bude navrhovat bezpečnostní aplikaci. V tabule 2.2 jsou stručně popsány architektury. V této diplomové práci bude použito zapojení podle kategorie 3 a 4. Zapojení kat. 3 zajišťuje nepřerušovanou bezpečnostní funkci, pokud dojde k jedné poruše. Při použití kat. 4 je z výstupu vedena navíc zpětná vazba, která garantuje bezpečnostní funkci vždy - i v případě jedné nebo více poruch.

Tabulka 2.2: Definované architektury bezpečnostní funkce [2]

Kategorie	Popis	Příklad
Kategorie B	Porucha může vést k selhání bezpečnostní funkce	
Kategorie 1	Porucha může vést k selhání bezpečnostní funkce, ale $MTTF_d$ každého kanálu kategorie 1 je delší než v kategorii B. Selhání bezpečnostní funkce je tedy méně pravděpodobné.	
Kategorie 2	Systémové chování kategorie 2 zajišťuje, že porucha může vést k selhání bezpečnostní funkce mezi jednotlivými kontrolami. Při kontrole bezpečnostní funkce však dojde k detekci selhání.	
Kategorie 3	SRP/CS dle kategorie 3 musí být navržena tak, aby jednotlivá závada v jakékoliv z těchto částí nevedla ke ztrátě bezpečnostní funkce. Kdykoliv je to rozumně možné, musí být detekována jednotlivá závada při nebo před nejbližší vyžadovanou bezpečnostní funkcí.	
Kategorie 4	SRP/CS dle kategorie 4 musí být navržena tak, aby jednotlivá závada v jakékoliv bezpečnostní části nevedla ke ztrátě bezpečnostní funkce a jednotlivá závada byla detekována při nebo před nejbližšími požadovanými bezpečnostními funkcemi, např. bezprostředně při zapnutí nebo na konci provozního cyklu stroje. I když tato detekce není možná, nesmí vést nahromadění nedetekovaných závad ke ztrátě bezpečnostní funkce.	

2.4 Popis normy ČSN EN 61508

Soubor norem ČSN EN 61508 *Funkční bezpečnost elektrických,/elektronických/programovatelných/ elektronických systémů souvisejících s bezpečností* je určen pro konstruktéry strojích zařízení, kteří se podílejí na návrhu a specifikaci elektronického řídicího systému souvisejícího s bezpečnostní (SRECS). Norma se opírá o dvě základní koncepce – životní cyklus bezpečnosti stroje a úroveň integrity SIL. Pracuje s následujícími pojmy:

- Bezpečnost – odstranění nepřijatelného rizika
- Riziko – kombinace pravděpodobnosti poškození a závažnosti tohoto poškození
- Poškození – fyzické zranění nebo poškození zdraví lidí
- Nebezpečí – potenciální zdroj poškození
- Funkční bezpečnost – součást celkové bezpečnosti, na které závisí správné fungování zařízení. Jako příklad je možné uvést oplocení kolem stroje. Zde funkční bezpečností můžeme označit uzamykatelné dveře nikoliv ostatní oplocení. Dveře je možno použít v určitou chvíli jako bezpečný vstup ke stroji.
- Porucha – ukončení bezpečností funkce stroje. Pokud nastane, je nutné zajistit, aby stroj zůstal v definovaném, bezpečném stavu.

- Nebezpečná porucha – porucha, která je schopna uvést stroj do nebezpečného stavu ve kterém jej není možné kontrolovat.
- Odolnost proti vadám – schopnost bezpečnostního přístrojového systému plnit bezpečnostní funkci za přítomnosti vad nebo chyb.

Dále stanovuje postupy a požadavky pro dosažení požadované funkce. Bezpečnostní systémy rozděluje do dvou skupin:

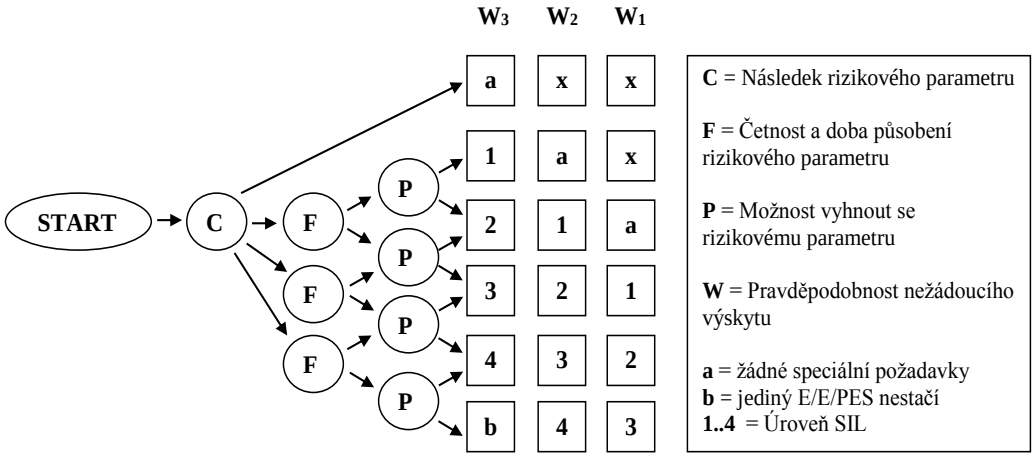
- Režim s nízkým (malým) vyžádáním: četnost vyžádání bezpečnostního systému není větší než jednou ročně.
- Režim s vysokým nebo trvalým vyžádáním: četnost vyžádání bezpečnostního systému je větší než jednou ročně.

Také popisuje jak rozsah rizik, které je potřeba snížit, tak i schopnost kontrolního systému snížit toto riziko z hlediska úrovně integrity neboli SIL (Safety Integrity Level). SIL se dělí do třech skupin, viz tabulka 2.3.

Tabulka 2.3: Vztah SIL a pravděpodobnosti nebezpečí poruchy za hodinu chodu.

SIL	Režim s nízkým vyžádáním [hod^{-1}]	Režim s vysokým vyžádáním [hod^{-1}]
4	$\geq 10^{-5}$ do $<10^{-4}$	$\geq 10^{-9}$ do $<10^{-8}$ porucha 1x za 10 let
3	$\geq 10^{-4}$ do $<10^{-3}$	$\geq 10^{-8}$ do $<10^{-7}$ porucha 1x za 100 let
2	$\geq 10^{-3}$ do $<10^{-2}$	$\geq 10^{-7}$ do $<10^{-6}$ porucha 1x za 1 000 let
1	$\geq 10^{-2}$ do $<10^{-1}$	$\geq 10^{-6}$ do $<10^{-5}$ porucha 1x za 10 000 let

Úroveň integrity SIL se určuje podle rozhodovacího grafu (Obrázek 2.2).



Obrázek 2.2: Rozhodovací graf pro určení úrovně SIL [3]

Parametr W (pravděpodobnost nežádoucího výskytu) se dělí do tří úrovní. W_1 reprezentuje velice malou pravděpodobnost, W_2 střední a W_3 vysokou pravděpodobnost.

Poslední důležitou částí normy je vztah úrovně SIL a podílu bezpečných a nebezpečných poruch (Tabulka 2.4). S bezpečnými poruchami je dopředu počítáno a jsou pro ně nadefinovány bezpečné stavy. S nebezpečnými poruchami není dopředu počítáno nebo je pravděpodobnost jejich vzniku velice malá. V normě jsou definované dva typy poruchových stavů:

- Typ A – jsou dopředu definovány poruchové stavy pro všechny komponenty stroje.
- Typ B – u alespoň jednoho komponentu není definován poruchový stav.

Tabulka 2.4: Souvislost úrovně SIL a odolnosti proti vadám [3]

<table>
<tr><td rowspan="2">Podíl bezpečných poruch</td><td rowspan="2">Typ architektury</td><td colspan="3">Odolnost proti vadám</td></tr>
<tr><td>N=0</td><td>N=1</td><td>N=2</td></tr>
<tr><td rowspan="2"><60%</td><td>Typ A</td><td>SIL 1</td><td>SIL 2</td><td>SIL 3</td></tr>
<tr><td>Typ B</td><td>Nedovolena</td><td>SIL 1</td><td>SIL 2</td></tr>
<tr><td rowspan="2">60%...<90%</td><td>Typ A</td><td>SIL 2</td><td>SIL 3</td><td>SIL 4</td></tr>
<tr><td>Typ B</td><td>SIL 1</td><td>SIL 2</td><td>SIL 3</td></tr>
<tr><td rowspan="2">90%...<99%</td><td>Typ A</td><td>SIL 3</td><td>SIL 4</td><td rowspan="2">SIL 4</td></tr>
<tr><td>Typ B</td><td>SIL 2</td><td>SIL 3</td></tr>
<tr><td rowspan="2">>99%</td><td>Typ A</td><td rowspan="2">SIL 3</td><td rowspan="2">SIL 4</td><td rowspan="2">SIL 4</td></tr>
<tr><td>Typ B</td></tr>
</table>

2.5 Řídicí systém související s bezpečnostní

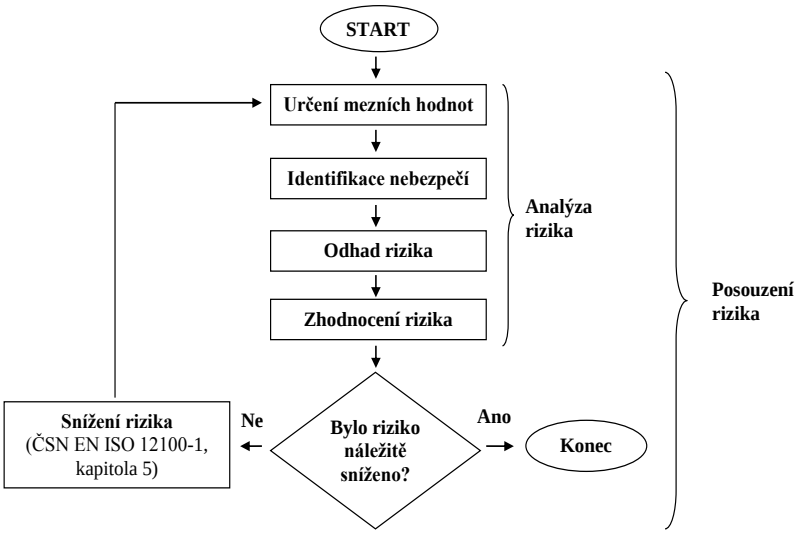
Řídicí systém související s bezpečností (zkratka SRECS, Safety Realted Electrical Control Systems) je část řídicího systému stroje, který zabraňuje výskytu nebezpečných situací. Používá se buď jako samostatný systém, nebo může být integrován do normálního řídicího systému stroje.

Bezpečnostní funkce je část SRECS stroje, která udržuje jeho bezpečný stav. Pokud tato funkce selže, zvyšuje se riziko spojené s užíváním stroje. Při návrhu bezpečnostních funkcí stroje musí byt stanoveny jejich vstupy a úkony. Například aktivace funkce při otevření krytu, přerušení clony nebo zmáčknutí ESTOP. Důsledkem takových to podnětů může být zastavení stroje nebo odpojení napájení.

Bezpečnostní systém musí být navržen takovou úrovní integrity, která je přiměřena riziku stroje.

2.6 Popis normy ČSN EN ISO 14121

Osoby posuzující riziko stroje se řídí normou ČSN EN ISO 14121 *Bezpečnost strojních zařízení – Posouzení rizika – Část 1: zásady*. Tato norma stanovuje všeobecné zásady, které je nutno použit, aby bylo riziko co nejvíce sníženo. Tato norma zahrnuje návod posuzování rizika ve všech fázích životního cyklu stroje. Následující algoritmus zobrazuje řadu kroků, které je nutné při posouzení rizika dodržet.



Obrázek 2.3: Algoritmus postupu při posuzování rizika

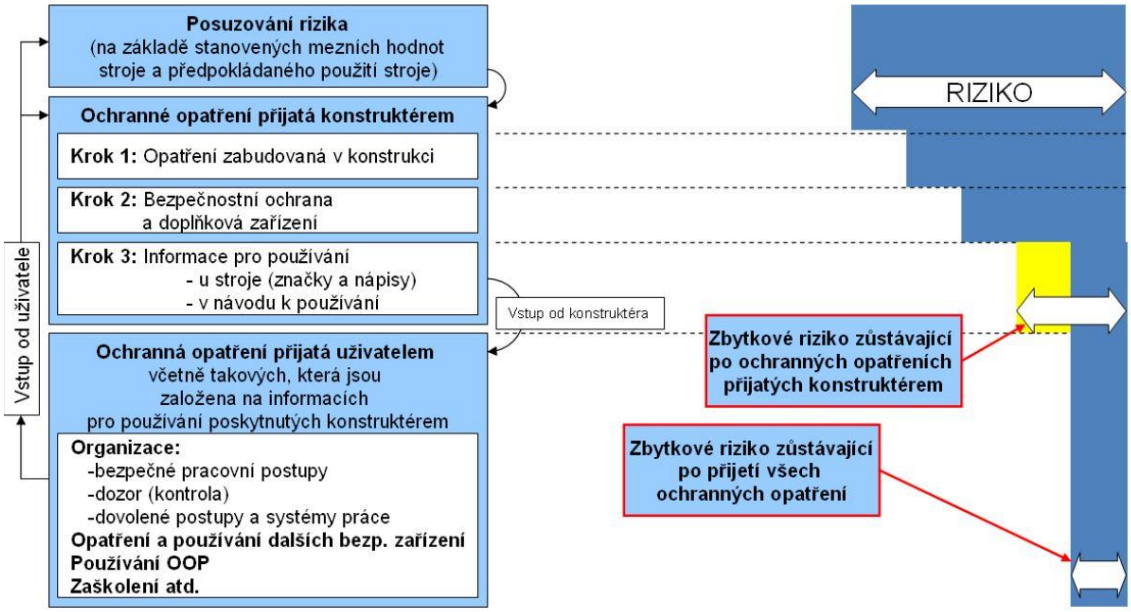
U posuzovaného stroje je nutné určit, v jakých režimech bude používán (spuštění, seřizování, programování, změna nástroje atd.), jaké osoby k němu budou mít přístup a jejich proškolení. Dále je nutné určit rozsah pracovního prostoru stroje a místa nutného kontaktu se strojem. S tímto bodem souvisí i vymezení prostředí, ve kterém bude stroj

pracovat. Je nutné také určit dobu životnosti stroje, úroveň požadované čistoty a doporučit intervaly údržby.

U všech nalezených faktorů je nutné určit jejich závažnost, pravděpodobnost výskytu a možnosti vyvarovat se riziku. Rovněž důležité je definovat dobu a četnost trvání vystavení nebezpečí, účinky nebezpečí, lidský faktor a vhodnost ochranných opatření.

2.7 Popis normy ČSN EN ISO 12100

Cílem normy ČSN EN ISO 12100 *Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – posouzení rizika a snižování rizika* je zprostředkovat konstruktérovi návod ke splnění všech požadavků na bezpečnost stroje. Zásady, které norma popisuje, jsou založeny na zkušenostech z konstrukce, používání, ale i nehod strojů. Proces posouzení a snížení rizika je zde rozdělen do tří krokové metody (Obrázek 2.4).



Obrázek 2.4: Postup snížení rizika [3]

2.8 Postup dosažení bezpečného stroje

Jak již bylo zmíněno v kapitole 2.1, aby bylo možné stroje provozovat, musí splňovat daná bezpečnostní nařízení. Konstruktéři nebo provozovatelé by se měli řídit následujícím postupem kroků, aby dosáhli co možná nejvyšší bezpečnosti stroje.

1. Diskuze nad navrhovaným strojem - provádí tým odborníků, většinou složený z konstruktéra elektro, konstruktéra mechanických částí a technologa.
2. Analýza rizik - dokument, který obsahuje seznam nebezpečných míst stroje, definuje, jak jsou nebezpečná, jak často nebezpečí hrozí a identifikace nebezpečí podle norem.
3. Projekt řešící analýzu risikovosti - vypracovávají konstruktéři elektro a mechanických částí podle dokumentu Analýza rizik. Tento tým vytvoří projekt úpravy stroje tak, aby se snížila nalezená rizika na minimum. Pokud i po aplikaci těchto úprav zbydou nějaká rizika, je třeba na ně upozornit v návodu k použití.
4. Aplikace projektu – podle projektu se na stroji provedou navržené úpravy.
5. Validace – ověření podle norem zda provedené úpravy jsou dostačující pro snížení rizika.
6. Vydání prohlášení o shodě – dokument, kterým ručí provozovatel nebo generální dodavatel, že je stroj sestaven podle platných norem.

2.9 Nástroje urychlující návrh a validaci

Důležitým krokem před uvedením stroje do provozu je jeho validace. Tato práce se zabývá části celkové validace a to ověřením bezpečnosti stroje. U každého stroje se nejprve určí požadovaná úroveň vlastností PLr a následně je nutné ověřit, zda této úrovně stroj dosáhl. Ověření PL lze dokázat pomocí výpočtů uvedených v normě ČSN EN ISO 13849-1. Z důvodů zrychlení, zpřesnění a zjednodušení této části projektu, je možné použít softwarové nástroje. Program *Safety Automation Builder* [4] napomáhá konstruktérovi s volbou bezpečnostních prvků. Výsledný návrh lze poté převést do program *SISTEMA* [5], který vyhodnotí dosaženou úrovně vlastností.

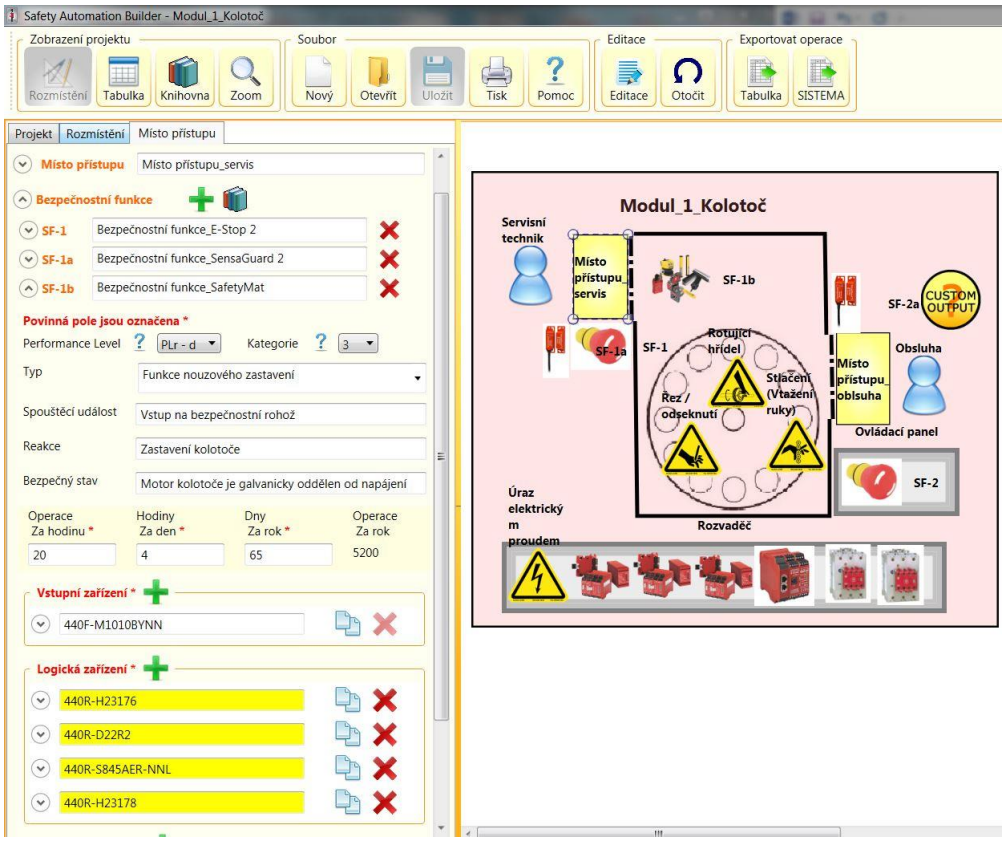
2.9.1 Safety Automation Builder

Safety Automation Builder (SAB) [4] je bezpečnostní nástroj, sloužící pro návrh a dokumentování bezpečnostních systémů. Tento program zjednodušuje a urychluje návrh bezpečnosti stroje a uživatel má jistotu splnění všech bezpečnostních požadavků. Nástroj je produktem firmy Rockwell Automation a je ke stažení zcela zdarma. SAB má velmi jednoduché a intuitivní prostředí, které je popsáno v odstavci *Vytvoření projektu.* Správný návrh zabezpečení a dosažení požadované PLr se na závěr ověří nástrojem SISTEMA.

Vytvoření projektu začíná kliknutím na ikonu *Nový* a vyplněním záložky *Projekt*. Vloží se jméno a popis projektu, pro lepší práci obrázek půdorysu stroje, dále se odpoví na tři otázky a zvolí se *Základní úroveň vlastností (PLr).* V záložce *Rozmístění* se

přetažením zvolené položky do obrázku v pracovním okně vloží pracovní zóna, ovládací panel a rozvaděč, rozmístí se značky nebezpečí nalezených u stroje. Dále se do půdorysu dokreslí navržené pevné a pohyblivé kryty, místa určení k přístupu osob a vloží se osoby. Bezpečnostní funkce a bezpečnostní vybavení stroje se vkládají do prvku *Místo přístupu*. Nejprve se vybere objekt *Místo přístupu* a poté se vypíše levé menu.

Při tvorbě bezpečnostní funkce je nutné zadat její typ, její spouštěcí událost, reakci na ni a bezpečný stav, do kterého se stroj dostane. Požaduje se také určit, jak často je tato funkce aktivována – zadá se počet operací za hodinu, počet hodin za den a počet dní v roce. Dalším krokem je vložení vstupního zařízení (např. E-Stop tlačítko), logického zařízení (např. bezpečnostní relé) a výstupní zařízení (bezpečnostní stykače). Jednotlivé komponenty se dají vybrat v rozbalovacím menu (kliknutím do řádku s typem zařízení) a vybráním správné kategorie a typu, nebo zvolením položky *Pomozte mi vybrat*. Tato volba zjisti pomocí jednoduchých otázek, které zařízení bude nejvhodnější pro Vaši aplikaci. V posledním kroku se zvolí položka z horního menu *Exportovat operace/ SISTEMA*. Na obrázku 2.5 je zobrazen program SAB s otevřenou záložkou *Místo přístupu-servis* a konfigurací funkce *Bezpečnostní funkce_E-Stop 2*. Tato funkce je použita v laboratorní úloze č. 1.



Obrázek 2.5: Pracovní prostředí Safety Automation Builder

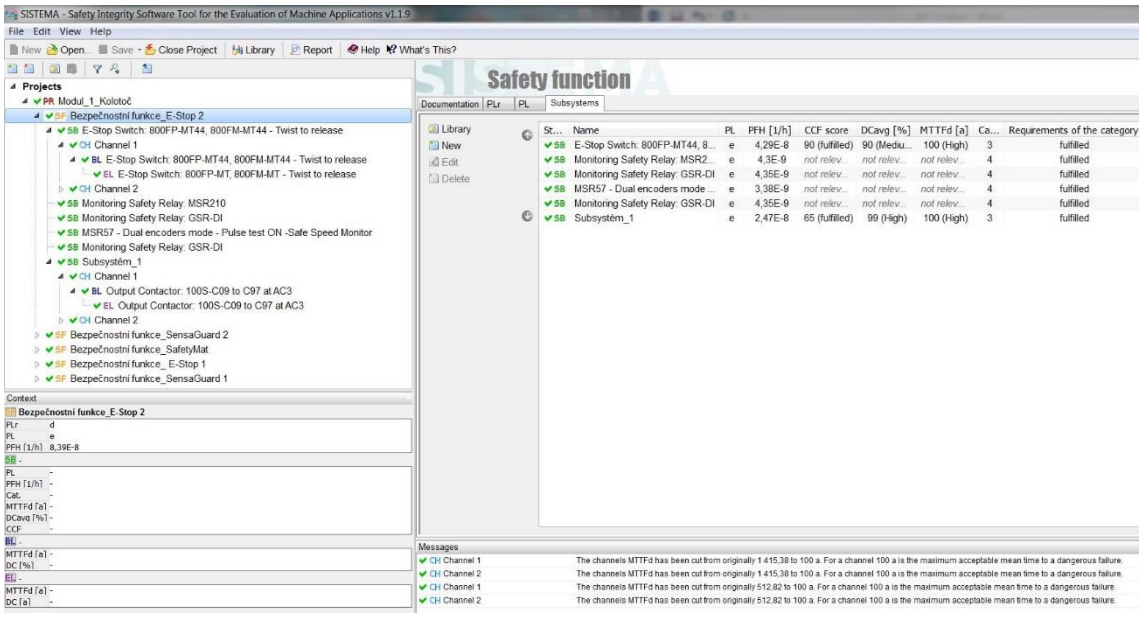
2.9.2 SISTEMA

Softwarový nástroj SISTEMA [5] automatizuje výpočet dosažené úrovně vlastností podle normy EN ISO 13849-1. Tento nástroj je produktem německé organizace IFA. SISTEMA umožnuje uživatelům modelovat strukturu ovládacích prvků souvisejících s bezpečností na základě předepsaných architektur. Výsledkem je ověření, zda návrh dosahuje požadované úrovně PL. Výhodou tohoto programu je možnost použití knihoven s bezpečnostními prvky různých výrobců.

Pomocí tohoto nástroje lze vytvořit projekt s pevně danou strukturou, nebo je možné použít výstup z program SAB. Struktura projektu se dělí do následujících úrovní:

1. PR – Project: je vytvořen pro každý stroj
2. SF – Safety Function: jednotlivé bezpečnostní funkce
3. SB – Subsystem: části bezpečnostní funkce rozdělené podle zvolené architektury
4. CH – Channel: počet kanálů v systému – je určen architekturou
5. BL – Block: charakterizuje fyzické zařízení (vstupní, logické, výstupní)
6. EL – Element: většinou typ použitého elementu např. kontakt

V této diplomové práci byl do nástroje SISTEMA vložen výstup z programu SAB. Celý projekt byl tedy vytvořený a SISTEMA jen ohodnotil kvalitu návrhu. Pracovní okno s jednotlivými bezpečnostními funkcemi laboratorní úlohy č. 1 zobrazuje obrázek 2.6.

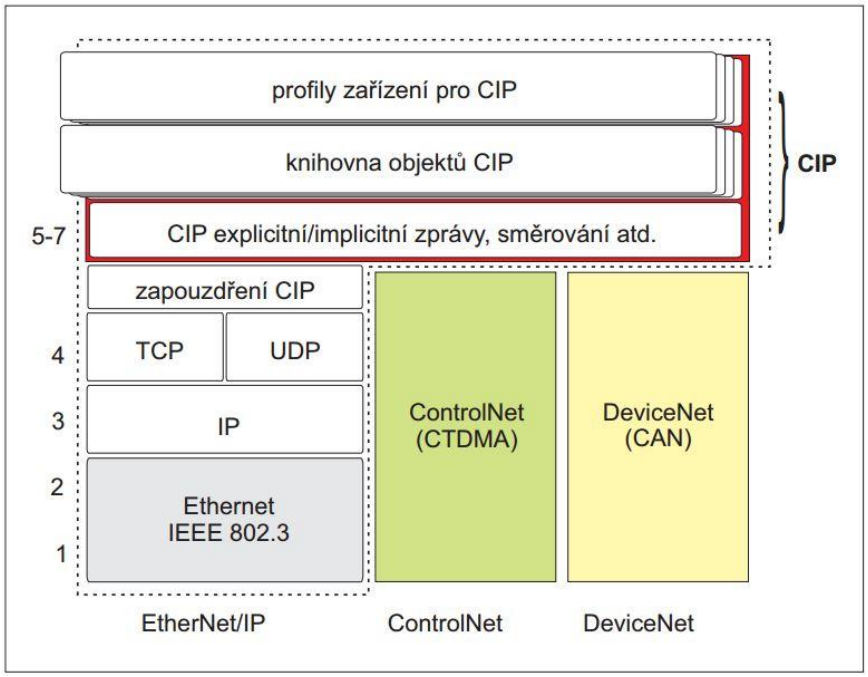


Obrázek 2.6: Pracovní prostředí nástroje SISTEMA

3 COMMON INDUSTRIAL PROTOCOL

Tradiční komunikační sítě používané ve výrobních podnicích jsou navrženy pro jednotlivé aplikace (řízení, přenos informací, bezpečnost aj.). Bohužel, tyto aplikace nejsou schopny pracovat vedle sebe a výrobci byli nuceni zavádět několik různých, mezi sebou nekompatibilních sítí. Cílem výrobců automatizovaných systémů je tedy minimalizovat tuto síťovou rozmanitost a propojit všechna zařízení pomocí jedné sítě.

Common Industrial Protocol (CIP) [6] je všestranný objektově orientovaný protokol průmyslové automatizace publikovaný asociací ODVA (Open DeviceNet Vendors Association) [7]. Zahrnuje sadu zpráv a služeb pro průmyslové aplikace (řídící, bezpečnostní, energetické, synchronizační a pohybové, informační a řídicí sítě). Tento protokol umožnuje uživatelům používat tyto aplikace se sítěmi EtherNet, DeviceNet a ControlNet (Obrázek 3.1). Díky jeho použití mohou tyto sítě mezi sebou komunikovat.

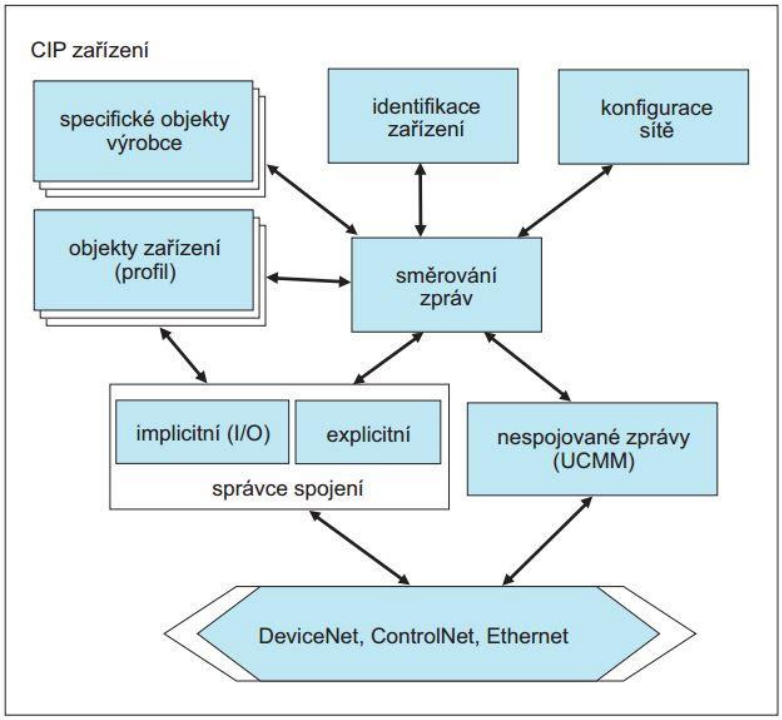


Obrázek 3.1: Komunikační model s využitím protokolu CIP [6]

Objektově orientovaný protokol CIP pracuje s modelem zařízení a využívá komunikaci na principu producent - konzument. Všechna zařízení jsou reprezentována skupinou objektů. Každý objekt má své vlastní atributy (data), služby (příkazy) a funkce (reakce na události). Jsou dány tři skupiny objektů – povinné, aplikační a dané výrobcem. Mezi povinné jsou zařazeny:

- objekt identifikující zařízení
- objekt specifikující předávání zpráv
- objekt pro správu spojení
- objekty s parametry konfigurace komunikační sítě

Jednotlivé typy komunikujících zařízení jsou reprezentovány skupinou aplikačních objektů, které tvoří jejich profil. Na obrázku 3.2 jsou znázorněny vazby mezi objekty.



Obrázek 3.2: Vazby mezi objekty zařízení s rozhraním CIP [6]

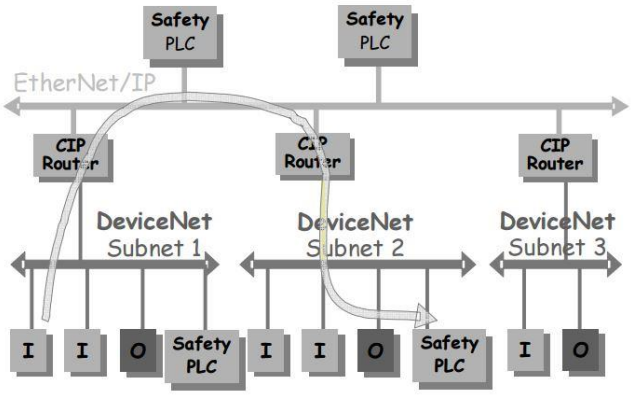
Soupis všech objektů, které jsou pro dané zařízení vytvořeny, je uložen elektronickém dokumentu v tzv. EDS. Tento soubor obsahuje informace potřebné pro konfiguraci sítě.

Společnost ODVA [7] zavedla přístavbu k CIP protokolu pod názvem CIP Safety. Toto rozšíření zajištuje funkční bezpečnost pro CIP sítě a poskytuje uživatelům bezpečnou komunikaci mezi zařízením, řadičem a sítí pro bezpečnostní aplikace.

Dalším rozšířením hlavního protokolu CIP jsou CIP Sync a CIP Motion. CIP Sync umožnuje synchronizaci aplikací v distribuovaných systémech prostřednictvím přesných real-time hodin ve všech zařízení. CIP Syn lze použít pro řízení pohybu pomocí CIP Motion.

3.1 CIP Safety

CIP Safety [8] je bezpečnostní služba postavená na technologii CIP. Tato služba nespoléhá na integritu datového spoje, proto může být použit k propojení jednotlivých zařízení standartní kabel (neredundantní spojení). Toto řešení umožnuje použít standartní datový směrovač i pro bezpečnostní zprávy. Případnou poruchu na vedení vyhodnotí koncové – bezpečnostní - zařízení a použije vhodná opatření. Tato vlastnost protokolu CIP Safety umožnuje propojení mezi bezpečnostními komponenty pomocí odlišných sítí se stále dostatečně rychlou dobou odezvy – viz. obrázek 3.3.



Obrázek 3.3: Znázornění propojení bezpečnostních zařízení pomocí více sítí [8]

Protokol CIP Safety přidává mezi objekty zařízení nový objekt Safety Validator, který zajišťuje integritu bezpečnostních dat. Tento objekt obsahuje čtyři části posílané zprávy – data, časové razítko, úsek časové korekce a časové koordinace. Čas v časové značce, díky které znají konzumenti stáří dat, se určuje použitím požadavku *ping*, kdy se ve zprávě vrátí čas opačného zařízení. Porucha je vyhodnocena tehdy, pokud vyprší čas na přijetí nových dat.

Zařízení mohou být mezi sebou spojena pomocí dvou typů připojení – *Unicast* pro spojení vždy jen dvou zařízení a *Multicast* pro spojení více zařízení. Tyto zařízení mezi sebou komunikují pomocí zprávy v objektu Safety Validator. Zprávy je možné odesílat ve dvou formách – krátké pro Unicast a dlouhé pro Multicast.

Dříve, než může být bezpečnostní komponent používán, je nutné jej nakonfigurovat. Existují dva možné postupy konfigurace – přímo ze zařízení do zařízení nebo přes jiné zařízení. Díky tomu nemusí být konfigurační nástroj přímo připojen k nastavovanému zařízení.

Technologie CIP safety poskytuje čtyři následující ochranná opatření, aby zajistila integritu konfigurace.

Safety Network Number je bezpečnostní síťové číslo, které je přiřazeno k určité bezpečnostní síti. Díky tomuto číslu a vlastní lokální adrese je možné každé zařízení v síti jednoznačně určit.

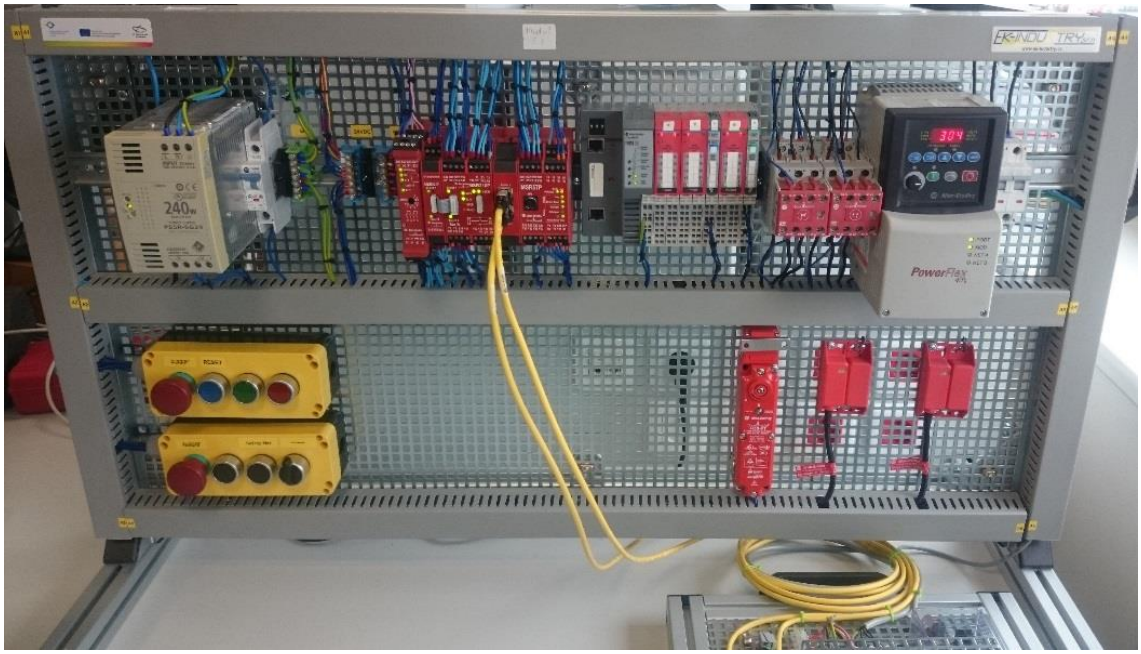
Password Protection je ochrana zařízení volitelným heslem proti změně nastavení chráněného zařízení.

Configuration Ownership. Tento parametr udává, zda bylo zařízení konfigurováno a tím i přiřazeno některému vyššímu bezpečnostnímu zařízení, nebo bylo nastaveno pouze konfiguračním nástrojem.

Configuration Locking umožnuje ověření zařízení před uzamčením a jeho dalším používáním. Verifikace potvrzuje správné nastavení všech bezpečnostní komponentu.

4 DEMONSTRAČNÍ ÚLOHA Č. 1

Ve školí laboratoři je na stolním panelu (Obrázek 4.1) sestavena výuková bezpečnostní laboratorní úloha, která nahrazuje reálný stroj. Navržení a zkonstruování provedla firma EK-Industry, která použila komponenty od firmy Rockwell Automation. Cílem je vytvořit demonstrační laboratorní úlohu zabývající se snížením rizik stroje se zaměřením na pohyb. Postup navržení a realizace této úlohy je popsán v následujících kapitolách.

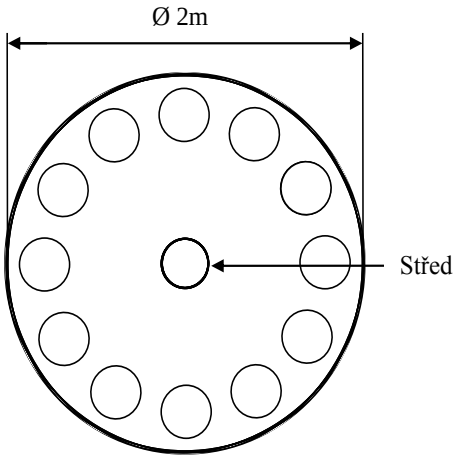


Obrázek 4.1: Panel bezpečnostní laboratorní úlohy č. 1

4.1 Posouzení rizik

Při konstruování nového strojního zařízení je důležité provést posouzení možných rizik. Provádí se podle normy ČSN EN ISO 14121. Posouzením rizika se uvažuje sled logických kroků, které umožnují systematickou analýzu a posouzení rizik. Riziko lze definovat jako kombinaci rozsahu škody a pravděpodobnosti jejího výskytu.

Tato laboratorní úloha je vytvořena jen pro simulaci funkce bezpečnostních prvků. Pro lepší představu celkového stroje a procesu posouzení bezpečnosti, byl navržen virtuální model stroje, který fyzicky představuje panel č. 1 – kolotoč. Na obrázku 4.2 je zobrazen půdorys kolotoče. Je sestaven z kola o průměru dva metry a dvanácti otvorů po obvodu. Jelikož tento stroj je virtuální, je předpokládáno, že je z funkčního hlediska již navržen a další výrobním krokem je zajištění jeho bezpečnosti. V diplomové práci se bude počítat s tím, že tento stroj se nachází v laboratoři jako panel č. 1.



Obrázek 4.2: Virtuální stroj - kolotoč

4.1.1 Určení mezních hodnot

Určení mezních hodnot kolotoče je první fáze při posouzení rizika. Tato činnost je založena na jasném pochopení limitů stroje a jeho funkcí a rozsahu pohybu. Kolotoč se nachází v čisté, klimatizované laboratoři. Bude využíván studenty k výuce programování PLC automatů přibližně 10 hodin týdně během semestru. Dle normy je nutné provádět na tomto zařízení kontrolu bezpečnosti minimálně jednou za rok. Protože máme místo stroje pouze panel se zapojenou úlohou, dostačuje pouze zde kontrolovat funkčnost bezpečnostních (bezpečnostní relé, magnetické snímače, elektronický zámek, E-stop), jistících (jističe a stykače), mechanických (ochranné kryty, motor, enkodéry) a elektrických prvků (např. tlačítka).

Kolotoč – v této úloze je fyzicky pouze motor se dvěma enkodéry – má za úkol pracovat ve dvou režimech, běžný provoz a tzv. „ *režim povolení přístupu“*, ve kterém je kontrolována bezpečná rychlost. Pro účel výuky byla maximální bezpečná rychlost motoru nastavena na 400 ot./min. Kolotoč je řízen frekvenčním měničem PowerFlex40. Obsluha kolotoče jej bude ovládat pouze z ovládacího čelního panelu, kdy bude nastavovat jeho rychlost. Přístup ke stroji má být umožněn pouze v režimu „ *povolení přístupu“*.

4.1.2 Identifikace úloh a nebezpečí

V této kapitole je kladen velký důraz na preciznost. Je nutné definovat všechny předvídatelná nebezpečí a nebezpečné situace. Dle výše zmíněné normy je vhodné vytvořit následující seznam nebezpečí, které je nutno vzít v úvahu při konstruování strojního zařízení.

Nebezpečí:

1. Mechanické nebezpečí
    a. Střih otáčejícím se kolotočem
    b. Pořezání nebo uříznutí končetiny o konstrukci a otočné kolo
    c. Navinutí, vtažení nebo zachycení
2. Elektronické nebezpečí
    a. Zásah nebo smrt elektrickým proudem v rozvaděči
3. Nebezpečí uklouznutí, zakopnutí a pádu

Nebezpečné úlohy:

4. Seřizování a servis
    a. Výměna dílů určených pro otáčení
    b. Výměna a oprava poškozených dílů
    c. Měření otáček stroje

4.1.3 Odhad rizika

U výše identifikovaných nebezpečí je nutné určit, jak velké představují riziko. Čím je toto riziko větší, tím je důležitější jej snížit.

Technická zpráva ISO TR 14121-2 „Posouzení rizik – praktické směrnice a příklady metod“ představuje praktické vodítko a ukazuje různé postupy hodnocení rizik.

Při hodnocení rizika budeme určovat následující faktory:

- Závažnost potenciálního zranění
- Četnost vystavení
- Pravděpodobnost zranění

Závažnost potencionálního zranění je v bodu *1. Mechanické nebezpečí* velké, kdy hrozí v nejhorším případě amputace končetiny a trvalá invalidita. Toto hodnocení se týká i bodu *4. Seřizování a servis*. Bod *2. Elektrické nebezpečí* je v této kategorii možné hodnotit až smrtí.

Četnost vystavení mechanickému nebezpečí je velmi častá, protože se nyní může obsluha dotknout kolotoče kdykoliv. Stejné hodnocení platí i v bodě *4. Seřizování a servis*. Elektrické nebezpečí může nastat pouze při otevření rozvaděče, což se stává velmi zřídka. Četnost uklouznutí je také malá.

Při uvažování pravděpodobnosti výskytu je jasné, že pokud je kolotoč bez oplocení, možnost mechanického nebezpečí je pravděpodobná, při neopatrném personálu i jistá. Pří úkonu seřizování a servisu kolotoče se může stát, že obsluze někdo zapne stroj a nastane nebezpečná situace. Pravděpodobnost tohoto stavu je možná. Pravděpodobnost uklouznutí, zakopnutí a pádu obsluhy je možná.

4.1.4 Opatření pro snížení rizika

Finálním krokem při snižování rizika stroje je navržení ochranných opatření. V normě ČSN EN ISO 12100 jsou definovány typy a postupy použití jednotlivých opatření. Nejprve se riziko sníží opatřením zabudovaným v konstrukci (např. oplocením stroje), poté použití bezpečnostních a doplňkových opatření a jako třetí opatření jsou sepsány pokyny pro užívání stroje.

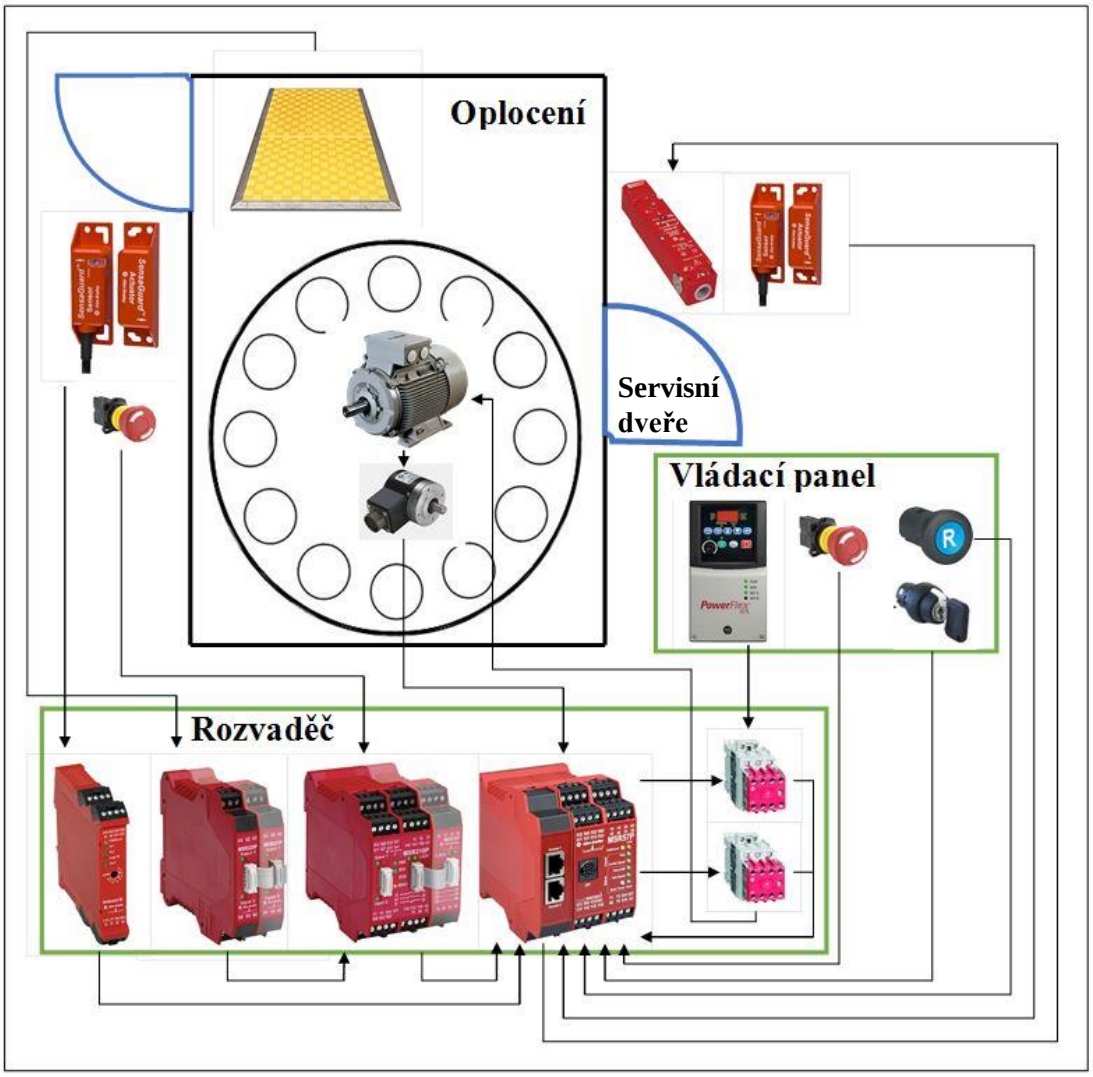
Z pravidla prvním konstrukčním opatřením je oplocení celého stroje. Toto oplocení je nutné pevně ukotvit kolem stroje (např. přišroubovat k podlaze) a mělo by dosahovat minimální výšky 2 m. Aplikací tohoto opatření je riziko sníženo o bod *1. Mechanické nebezpečí*. Z důvodů úkonů obsluhy - *4.* S*eřizování a servis* – je potřeba umožnit obsluze přístup ke stroji. Do oplocení byla namontována dvojice dveří pro snadný přístup. Touto úpravou oplocení bylo umožněno přístupu obsluhy ke stroje i v režimu chodu. Aby se tomu zamezilo, je nutné použít *Bezpečnostní ochranné a doplňkové zařízení.*

Pro opětovné dosaženi minimálního rizika je nutné na dveře připevnit magnetické spínače SensaGuard a na jedny navíc elektronický zámek. Další nebezpečnou situací, která hrozí, je případ, kde jedna osoba bude zavřena vevnitř oplocení a druhá spustí stroj. Této nebezpečné situace se vyvarujeme položením bezpečnostní rohože Safety Mat na podlaze kolem kolotoče uvnitř oplocení. Výše zmíněné bezpečnostní komponenty jsou ovládány logickými zařízeními, které realizují bezpečnostní funkce. Na obrázku 4.3 je zobrazeno blokové zapojení jednotlivých elektrických komponentů na virtuálním stroji – kolotoči.

Bezpečnostní funkce nouzového zastavení

Odpojení energie od zdroje rizika vznikne tehdy, když bezpečnostní systém detekuje stisknutí nouzového tlačítka, nebo rozepnutí magnetického spínače, nebo se aktivuje bezpečnostní rohož. Odpojení energie od zdroje rizika je tvořeno dvěma bezpečnostními redundantními stykači, které způsobí vypnutí přívodu energie do motoru kolotoče.

Požadavkem na bezpečnostní funkci je vypnutí přívodu energie do motoru při stisku minimálně jednoho ze dvou tlačítek bezpečnostní obsluhy. Tuto funkci mohou aktivovat i magnetické spínače (otevření dveří) nebo bezpečnostní nášlapová rohož SafetyMat. Napájení motoru se obnoví až po opuštění obsluhy z ochranného pásma stroje, zavření všech dveří, deaktivací nouzových tlačítek a stisknutí tlačítka reset. Použití navržených opatření nedovolují vstup obsluhy ke stroji v režimu chodu.



Obrázek 4.3: Blokové zapojení virtuálního kolotoče

Bezpečnostní funkce povolení přístupu

U tohoto stroje je požadováno, aby obsluha mohla vykonávat určité úkony. U některých z těchto úkonů musí být kolotoč v pohybu a jeho rychlost musí být udržována v určitém, omezeném rozsahu. K zabezpečení této funkce je nejvhodnější použít modul MSR57P, který disponuje funkcí měření otáček. Před použitím bezpečnostní funkce musí nejprve obsluha snížit rychlost motoru pod bezpečnou hranici, která byla nastavena na 400ot/min. Poté otočit přepínač režimů z pozice *chod* do pozice *povolení přístupu*. V tomto režimu je v relé MSR57P aktivována funkce *safe limit speed*, při které jsou otáčky motoru monitorovány zpětnou vazbou ze dvou enkodérů. Výstupem funkce je odemčení zámku GuardMaster a možnost otevřít servisní dveře. Režim monitorování rychlosti se deaktivuje zavřením servisních dveří, přepnutím stroje do režimu chod a následným zmáčknutím tlačítka reset.

4.2 Ověření bezpečnosti

Následujícím krokem při návrhu zabezpečení stroje je určení požadované úrovně vlastností (Performance Level) a ověření její dosažení. V kapitole 4.1 byly definovány nebezpečí, která obsluze hrozí. Z těchto znalostí se dále určuje požadovaná úroveň vlastností podle rozhodovacího grafu na obrázku 2.1. Zhodnotí se všechny nebezpečí a vybere se to, které má nejhorší výsledek. V této úloze je nejnebezpečnější bod *1. Mechanické nebezpečí*. Jelikož hrozí amputace končetin, byl vybrán parametr *S2*. Osoby jsou tomuto nebezpečí vystaveny neustále, tzn. *F2* a poslední parametr byl zvolen P1, protože osoby vidí, že se kolotoč otáčí a proto je možné se tomuto nebezpečí vyhnout. Požadovaná hodnota je tedy PLr d. K ověření dosažení této úrovně je vhodné použít nástroje SAB a SISTEMA. V programu SAB se vytvoří projekt s navrženými bezpečnostními komponenty. Jejich správný výběr tj. dosažení požadované PLr se ověří v nástroji SISTEMA.

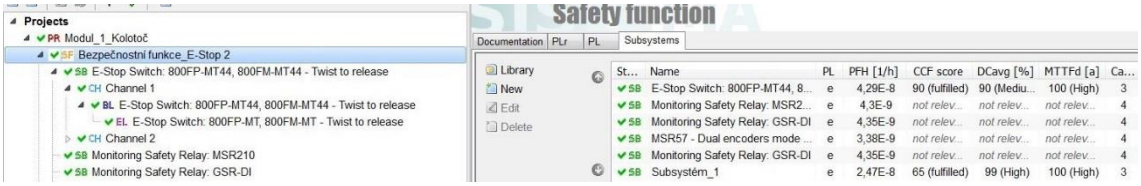
4.2.1 Použití nástroje Safety Automation Builder a SISTEMA

Tento nástroj se používá z důvodů názorného navrhování bezpečnostních funkcí, jednoduchou a správnou volbu bezpečnostních zařízení a následným exportem návrhu do ověřovacího nástroje SISTEMA.

Projekt byl vytvořen podle návodu v kapitole 2.9.1. Byl pojmenován *Panel_1_Kolotoč*, úroveň vlastností byla nastavena na PLr-d a byl vložen půdorys kolotoče. Hlavní částí projektu jsou následující funkce:

Funkce nouzového zastavení se aktivuje zmáčknutím E-Stop tlačítka 2. Po zastavení kolotoče zůstává kolotoč v bezpečném stavu a motor je galvanicky oddělen od napájení. Aktivace funkce byla nastavena na 20 operací za hodinu, 4 hodiny denně a 65 dní v roce. Tyto hodnoty odpovídají používání laboratorní úlohy studenty během roku. Do dalších kolonek je nutné vložit vstupní zařízení tj. E-Stop tlačítko 2, jako logická zařízení byla navržena čtyři bezpečnostní relé (GSR_DI, MSR220P, MSR210P a MSR57P), kterými disponuje panel č. 1. Výstupním zařízením jsou dva redundantní stykače 100S-C. V projektu byly vytvořeny další dvě identické funkce, které se budou lišit jen popisy událostí a vstupní zařízení (v první funkci aktivuje bezpečnostní funkci spínač SensaGuard, v druhé rohož SafetyMat).

Stejné funkce, ale pouze dvě, se vloží i do objektu *Místo přístupu_obsluha* . Počet operací se ponechá sejný. Vstupní zařízení bude pro první funkci nouzového zastavení E-Stop tlačítko 1 a pro duhou magnetický spínač SensaGuard. V poslední kroku se zvolí položka z horního menu *Exportovat operace/ SISTEMA.* Tento nástroj se automaticky otevře s exportovaným projektem (Obrázek 4.4). Jednotlivé funkce jsou zde označeny zeleně, což znamená ověření dosažené úrovně. V pravém okně *Subsystems* jsou vypsány detaily zvolené bezpečnostní funkce. Report z tohoto nástroje nalezneme na přiloženém CD.



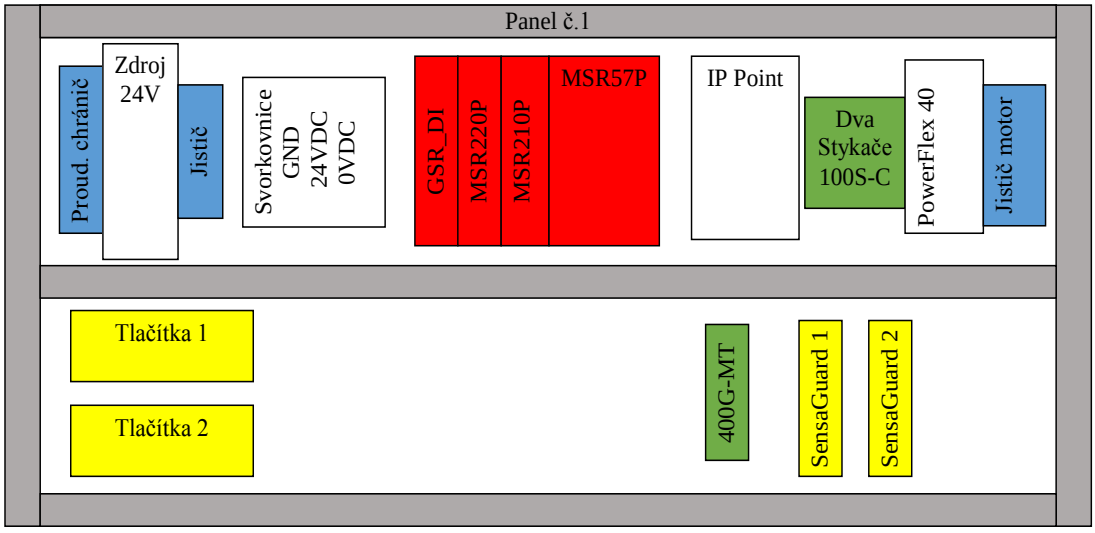
Obrázek 4.4: Projekt Panel_1_Kolotoč v nástroji SISTEMA

4.3 Realizace bezpečnostní úlohy

Tato část laboratorní úlohy je dalším logickým krokem k dosažení bezpečného stroje. Zabývá se úpravou elektroinstalace laboratorního panelu č. 1, který fyzicky představuje virtuální stroj – kolotoč. Dosavadní zapojení od firmy EK-Industry nebylo vhodné pro tuto úlohu, a proto bylo nutné provést jeho úpravy. Použití a zapojení jednotlivých komponentů je popsáno v následujících odstavcích.

4.3.1 Panel č. 1

Hlavní částí úlohy je laboratorní panel postavený na stole v laboratoři. Na panelu jsou umístěny komponenty, jejichž soupise je v tabulce 4.1. Blokové rozmístění zařízení na panelu je zobrazeno na obrázku 4.5. Panel je napájen 230V přes eurozásuvku na zadní straně. Vedle ní je umístěn hlavní vypínač. Rozvod 230V je dále jištěn pojistkou a proudovým chráničem (modře), ze kterého je napájen zdroj PS5R-SG24 a frekvenční měnič PowerFlex40, který řídí motor představující kolotoč. Ostatní součásti jsou napájeny zdrojem 24VDC, ke kterému je přes jistič (modře) propojena svorkovnice 24VDC pro kladný pól a 0VDC pro nulový pól.



Obrázek 4.5: Blokové schéma laboratorního panelu č. 1

Bezpečnostní komponenty jsou zde barevně rozděleny do tří skupin. Žlutě jsou označeny vstupy bezpečnostních funkcí, červeně logické zařízení a zeleně výstupy funkcí. Celý bezpečnostní systém je zapojen podle architektury *kategorie 3* - norma ČSN EN ISO 13849.

Mezi navržené vstupní zařízení patří dvě E-Stop tlačítka, dva bezkontaktní spínače SensaGuard, elektronický zámek GuardMaster 400G-MT, bezpečnostní rohož Safety Mats, která je simulována tlačítkem, modré resetovací tlačítko a přepínač funkce povolení přístupu.

Hlavní logickou jednotkou je modul MSR57P, který řídí všechny bezpečnostní funkce stroje. Jelikož nedisponuje potřebným počtem vstupů, byly pro rozšíření použity další moduly a to relé MSR210P a k němu rozšiřující MSR220P. Tyto tři logické jednotky umí pracovat pouze s mechanickými kontakty bezpečnostních prvků a rohoží Safety Mat. Aby bylo možné připojit i bezkontaktní spínače SensaGuard, které mají výstup ovládán tranzistory, bylo nutné použít dvouvstupové bezpečnostní relé GSR DI s kontaktovým výstupem. Bezpečný stav ve stop režimu je zajištěn odpojením napájení motoru pomocí dvou redundantních stykačů. Imaginární stroj kolotoč zde představuje třífázový motor 2IK6A-SW2 od firmy Oriental motor se dvěma enkodéry.

Tabulka 4.1: Seznam komponentů laboratorního panelu č. 1

Panel č. 1	**Popis**
Zdroj PS5R-SG24	24VDC / 10A
PowerFlex40	frekvenční měnič
Logické jednotky	
GSR DI	GuardMaster bezpečnostní relé, 2 dvoukanálové vstupy, 1 dvoukanálový N.O. výstup
MSR220P	Monitorující bezpečnostní relé, 2 tříkanálové vstupy
MSR210P	Monitorující bezpečnostní relé, 2 tříkanálové vstupy, 1 dvoukanálový N.O. výstup
MSR57P	GuardMaster bezpečnostní relé pro aplikace s pohybem
100S_C Safety Contactors	Guard master bezpečnostní stykač, 9A, 24V DC, 2 N.O a 2 N.C. kontakty
440G-MT	Guard master bezpečnostní elektronický zámek, 24V DC, 3 N.C. a 1 N.O. kontakty
440N-Z21SS2AN9	Senza Guard bezkontaktní magnetický spínač
Panel s tlačítky	
E-Stop	2 N.C. kontakty
Modré reset	1 N.O. kontakt
Černé Safety Mat	2 N.C. kontakty
Přepínač	2 N.C. kontakty
Panel s motorem a enkodéry	
2IK6A-SW2	Motor 3 fáze, 230VAC / 60Hz / 0.079A ,výrobce: Oriental motor
844A-Z305C 1024	Optický inkrementální enkodér, 5V DC, rozlišení 1024 ppr
DC zdroj 2x5VDC 1A	DC/DC zdroj z 24VDC na 2x5VDC, maximální proud I=1A, pro napájení enkodérů

4.3.2 Panel s motorem a enkodéry

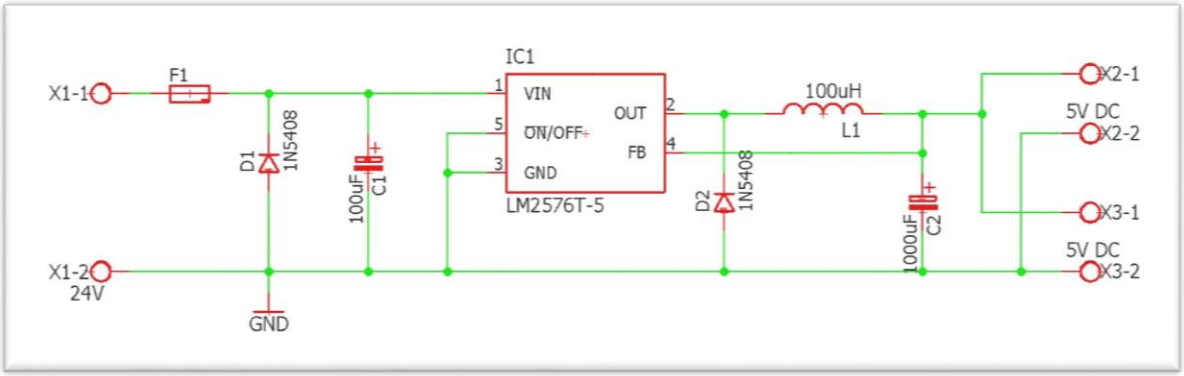
Součástí této laboratorní úlohy je kromě hlavního panelu i druhý (menší) přenosný panel, na kterém je umístěn třífázový motor s dvěma enkodéry a DC/DC zdroj pro napájení enkodérů.

Třífázový motor 2IK6A-SW2 [9] od firmy Oriental motor je zapojen do hvězdy. Při napájení 230V/ 60Hz má motor 1500 ot./min s maximální příkonem 0.079A. Jelikož slouží pouze jako simulační motor výsledného stroje a pohání pouze dva enkodéry, tento výkon plně dostačuje. Otáčky motoru snímají dva enkodéry **844A-Z305C 1024** [10] od firmy Allen-Bradley a jsou připojeny k hřídeli motoru v poměru otáček 1:1. Poskytují rozlišením 1024 pulzů za otáčku, výstupy A+, A-, B+, B- . Tyto enkodéry je nutné napájet napětí 5VDC s minimálním proudem 120mA. Jelikož laboratorní panel neobsahoval vhodný zdroj, bylo nutné jej navrhnout a sestavit.

Spínaný DC/DC zdroj je napájen napětím 24VDC a dodává výstupní napětí 2x5VDC. Byl navrhnut podle doporučeného zapojení od výrobce řídícího integrovaného obvodu LM257T-5 [11] . Vstupní napětí tohoto obvodu je 7VDC až 40VDC, na výstupu poskytuje 5VDC s maximální zátěží 3A. V tabulce 4.2 jsou vypsány použité součástky spínacího zdroje, schéma zapojení zobrazuje obrázek 4.6.

Tabulka 4.2: Seznam součástek spínaného 5VDC zdroje

Název	Parametr	Popis
F1	1,6A	Pojistka skleněná
D1	1N5822	Dioda
D2	1N5408	Dioda
C1	100µF/50V	Elektrolytický kondenzátor
C2	1000µF/10V	Elektrolytický kondenzátor
IC1	LM2576	Regulátor spínaného napětí
L1	100µH	Cívka
X1,X2,X3	ARK210/2EX	Dvoupólová svorkovnice



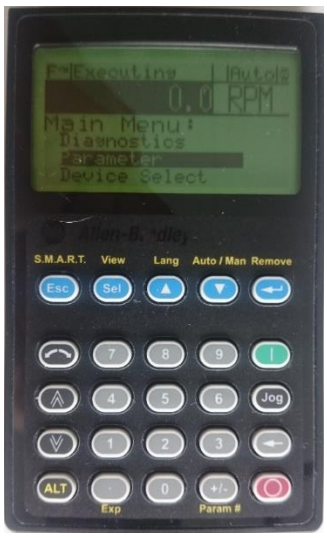
Obrázek 4.6: Schéma spínaného DC/DC zdroje 2x5V 1A

4.3.3 Popis bezpečnostních modulů

Každá bezpečnostní funkce je tvořena bezpečnostními vstupy, logickou jednotkou a bezpečnostními výstupy. Jako logickou jednotku můžeme použít bezpečnostní PLC (pro složitější aplikace) nebo bezpečnostní relé. V této laboratorní úloze byly zvoleny 4 typy bezpečnostních relé pro připojení všech vstupů a výstupů.

MSR57P [12] je bezpečnostní monitorovací modul určený pro řešení aplikací s pohybem, které vyžadují obsluhu během provozu. Relé disponuje dvěma vstupy pro enkodéry, pomocí kterých monitoruje rychlost motoru. Dále umožnuje dvoukanálové připojení bezpečnostních prvků (např. E-Stop tlačítko), přepínač režimů stroje a monitorování zámku dveří. Tyto bezpečnostní okruhy jsou pulzně testovány, aby bylo možné detekovat jejich přerušení nebo zkrat. Tato událost má za následek aktivaci relé. Výstupy modulu slouží pro ovládání elektromagnetického zámku dveří, spínání stykačů nebo ovládání bezpečnostního frekvenčního měniče s funkcí Safe Torque-off. Výslednou funkci je nutné naprogramovat nastavením skupiny parametrů, které jsou v relé předefinovány. Pro splnění bezpečnostní úrovně PLr e a SIL3 je nutné zapojit oba enkodéry.

Naprogramování modulu MSR57P je možné provádět pomocí dvou nástrojů a to programu DriveExplorer nebo DriveTools. Programy se naistalují do PC, které se následně pomocí převodníku spojí s MSR57P. Další možností je použití programátoru 20-HIM-A3 [13] zobrazeném na obrázku 4.7.



Obrázek 4.7: Programátor 20-HIM-A3

Programátor nabízí stejné možnost nastavení a podporu funkcí jako aplikace do PC, pouze jejich ovládání není tak přehledné. Po připojení HIM programátoru k modulu MSR57P se provede automatická synchronizace, po níž je možno diagnostikovat chyby a chybové hlášení, nastavovat seznam parametrů nebo přehrát firmware bezpečnostního modulu. Jednoduchým sloupcovým menu se prochází pomocí modrých šipek nahoru a

dolů, vnoření nebo změna údaje se provádí entrem (modré tlačítko vpravo), tlačítkem ESC se vrací zpět. Celý seznam parametrů se vyvolá zvolením žlutého ALT a tlačítkem +/- (žlutě Param #). Veškeré parametry a jejich vlastnosti jsou popsány v příručce k relé MSR57P.

Modul **MSR210P** [14] má dva tříkanálové bezpečnostní vstupy s funkcí pulzního testování. K těmto vstupům lze připojit pouze kontaktové komponenty tj. tlačítka, kontakty zámků a dveří a rohože Safety Mat. Resetovací funkce lze nastavit pomocí propojení svorek Y40, Y41 a Y42. Dalšími vlastnosti jsou monitoring externího zařízení (EDM) a oznámení stavu modulu PLC automatu. Výstup zahrnuje dva N.O. a jeden N.C. kontakty.

MSR220P [15] je vstupní rozšiřující modul pro bezpečnostní relé MSR210P. Disponuje dvěma tříkanálovými vstupy s funkcí pulzního testování bezpečnostních okruhů.

Obrázek 4.8: Modul MSR57P , MSR220P, MSR 210P, GSR DI 440R-D22R2 [16]

Všechny výše vyjmenované bezpečnostní relé (Obrázek 4.8) umí pracovat pouze s mechanickými kontakty komponentů. Protože v aplikaci jsou použity i dva magnetické spínače SensaGuard, bylo nutné vložit bezpečnostní relé, které umí s těmito snímači pracovat. **GuardMaster Safety Relays (GSR) DI** [17] kat. č. 440R-D22R nabízí dva dvoukanálové bezpečnostní vstupy a dva elektromechanické výstupy. Podporuje připojení jak klasických kontaktů, tak i OSSD výstupy snímačů (optické závory, magnetické spínače). Na čelní straně je umístěn otočný přepínač, pomocí kterého lze nastavit logickou funkci mezi vstupy a typ restartu.

4.3.4 Popis ostatních bezpečnostních prvků

Mezi výstupní komponenty bezpečnostní funkce patří elektronický zámek **440G-MT** [18]. Ten je ovládán 24V DC cívkou s funkcí *power to release* a je vybaven kontakty, které monitorují její polohu (3 N.C. a 1 N.O.). Jelikož zámek neumožňuje monitorování polohy jeho západky, je nutné vedle něj nainstalovat alespoň jeden snímač polohy západky (nebo součásti k ní připevněné, např. dveří). K tomuto úkolu zde slouží dva magnetické snímače **SensaGuard** [19] kat. č. 440N-Z21SS2H-AS. Disponují dvoukanálovým výstupem OSSD. Mohou být použity k zabezpečení až dvou dveří.

Aby bylo možné zajistit bezpečný stav stroje při aktivaci bezpečnostní funkce, tj. úplné zastavení motoru, je nutné jej odpojit od napájení. Z tohoto důvodu jsou v obvodu zapojeny dva redundantní bezpečnostní stykače **100S-C**. Tyto stykače jsou vybaveny dvěma N.C. a dvěma N.O. kontakty pro sledování jeho stavu (Obrázek 4.9).

Obrázek 4.9: GuardMaster 400G-MT, SensaGuard 400N, Stykač 100S-C

4.3.5 Popis zapojení bezpečnostních komponentů

Pro dosažen požadované úrovně vlastností je nutné použít jako zdroj napětí vstupních zařízení speciální bezpečností výstupy relé. Z tohoto důvodu jsou výstupy testovacích pulzů relé MSR57P (svorky S11 a S21) vedeny odděleně přes E-Stop 1 tlačítko a přes výstup relé MSR210P (svorku 13->14 a 23->24) do vstupních svorek S12 a S22 relé MSR57P. Na svorky S11 a S21 je dále připojen přepínač pro povolení režimu přístupu (SLS) ze kterého signál směřuje na vstupní svorky S52 a S62. Třetí bezpečnostní okruh je zapojen ze svorek S11 a S21 přes výstupní svorky relé GSR_DI (13->14 a 23->24) do vstupů relé MSR57P (svorky S32 a S42). Čtvrtý bezpečnostní okruh je veden ze svorek S11 a S21 přes kontakty magnetického zámku 400G-MT (kontrola polohy zámku) do vstupních svorek X32 a X42. K relé je dále připojeno resetovací tlačítko mezi svorkami Y1 a S34 a monitorování kontaktů bezpečnostní stykačů 100S-C okruhem z Y1 do Y2. Mezi výstupní svorky S1 a S2 je připojena cívka zámku 400G-MT. Hlavní výstupní funkcí relé je ovládat stykače 100S-C výstupními svorkami 14 a 24. Poslední připojené zařízení jsou dva enkodéry motoru žlutými kabely do zásuvek RJ-45 na přední straně relé.

Relé GSR_DI bylo do konfigurace vloženo pro připojení magnetických senzorů SensaGuard. Tyto senzory mají výstup typu OSSD se kterým umí pracovat pouze

zmíněné relé. Na vstupní svorky S12 a S22 je připojen senzor SensaGuard 1, na svorky S32 a S42 senzor SensaGuard 2. Automatický restart je nastaven propojením svorek S34 na napájecí napětí +24VDC.

Relé MSR210P disponuje dvěma tříkanálovými vstupy. Pro správnou funkci je nutné použít všechny vstupy. Pokud některé přebývají, je nutné je proklemovat s příslušnými výstupními svorkami. V této aplikaci jsou výstupy testovacích pulzů (svorky S11 a S21) vedeny přes tlačítko E-Stop 2 do vstupních svorek S12 - proklemováno s S42 a svorek S22 – proklemováno s S52. Dále je ještě vložena klema mezi svorky S11, S32 a A62. Automatický restart je nastaven propojením svorek Y31, Y40 a Y41.

K relé MSR210P je plochým kabelem připojeno rozšiřující vstupní relé MSR220P. Ze zdrojových svorek S41 a S52 relé MSR210P sloužící pro připojení rohože SafetyMat je veden okruh přes černé tlačítko SafetyMat do vstupních svorek S12 a S22 relé MSR220P. Zbylé vstupy tohoto relé jsou proklemovány se svorkou S41 relé MSR210P.

Výše popsané zapojení zejména kontaktních vstupů umožnuje detekovat rozpojení vodiče, zkrat na 24V nebo GND a nebo mezi jednotlivými kanály. Pro správnou funkci je ještě nutné nastavit relé MSR57P a GSR_DI. Přesné zapojení všech komponentů je zakresleno v elektrickém schématu (Příloha 1).

4.4 Konfigurace zařízení

Poslední fází před zpuštěním a otestování funkční bezpečnosti stroje je nastavení parametrů programovatelných relé a to GSR_DI a MSR57P.

K nastavení relé GSR_DI je nutné dodržet jednoduchý postup podle manuálu, předem je však nutné zvolit si požadovanou funkci. Na přední straně relé se nachází otočný deseti polohový přepínač, sloužící pro nastavení zvolené funkce. Po relé je požadováno automatický restart a funkci násobení mezi vstupy. Následujícími kroky slouží pro nastavení funkce a verifikaci:

1. Při odpojeném napájení se otočným přepínačem zvolí poloha 0.
2. Zapne se napájení, kontrolka PWR/Fault červeně bliká.
3. Otočným přepínačem se zvolí funkce 6 (IN1 AND IN2) OR L12, kontrolka vstupu 6x bliká s menší pauzou.
4. V posledním kroku se relé odpojí od napájení a po chvíli znovu připojí.
5. Nyní je v relé uložena zvolená funkce IN1 AND IN2.

Konfigurace relé MSR57P je už poněkud složitější. Při jeho nastavení je nutné si nejprve definovat funkce, které má relé vykonávat, dále těmto úkonům přizpůsobit jeho elektrické zapojení a následně nastavit jeho parametry. Pro tuto bezpečnostní úlohu bylo relé nastaveno jako *Singel Unit Systém*, bezpečnostní funkce byla zvolena *Master, Safe Limited Speed with Doot Monitoring*, dále byly zvoleny dva enkodéry s TTL (inkrementální) výstupem a rozlišením 1024 pulzů na otáčku, kontrola jejich napájení 5V a poměrem 1:1. Pro demonstraci funkce povolení přístupu (SLS) byl bezpečný stav motoru nastaven na 400 ot./min a méně. Po požadavku přístupu musí být do 2s otáčky

nižší než 100 ot./min, jinak relé vyhlásí chybu. Poslední funkcí relé je odemčení zámku a kontrola zavřených dveří. Celý seznam parametrů a jejich nastavení nalezneme v tabulce 4.3.

Tabulka 4.3: Nastavení parametrů MSR57P

Parametr	Popis	Hodnota		Parametr	Popis	Hodnota
1	Password	1		43	Direction Tol	0
5	Lock State	Lock		44	Safe Stop Input	1
6	Operating Mode	Run		45	Safe Stop Type	0
7	Reset Defaults	0		46	Stop mon Delay	0
10	Signature ID	----		47	Max Stop Time	0
13	New Password	0		48	Standstill Speed	0,1
17	Password Commnad	0		49	StandStill Pos	10
18	Security Code	256		50	Decel Ref Speed	0
19	Vendor Password	0		51	Stop Decel Tol	0
20	Cascade Config	0		52	Lim Speed Input	1
21	Safetu Mode	4		53	LimSpd Mon Delay	0
22	Reset Type	1		54	Enable SW Input	0
23	Reset Loop	0		55	Safe Speed Limit	400
24	OverSpd Response	0		56	Speed Hysteresis	0
25	Language Code	0		57	Door Out Type	0
26	Max Display Spd	1800		58	DM Input	1
27	Fbk Mode	1		59	Lock Mon Enable	1
28	Fbk 1 Type	1		60	Lock Mon Input	1
29	Fbk 1 Units	0		61	Max Speed Enable	0
30	Fbk 1 Polarity	0		62	Safe Max Enable	0
31	Fbk 1 Resolution	1024		63	Max Spd Stop Typ	0
32	Fbk 1 Volt Mon	5		64	Max Accel Enable	0
33	Fbk 1 Speed	0		65	Safe Accel Limit	0
34	Fbk 2 Units	0		66	Max Acc Stop Type	0
35	Fbk 2 Polarity	0		67	Fault Status	0
36	Fbk 2 Resolution	1024		68	Guard Satus	0
37	Fbk 2 Volt Mon	5		69	IO Diag Satus	0
38	Fbk 2 Speed	0		70	Config Flt Code	0
39	Fbkj Speed Ratio	1		71	MP Out Mode	1
40	Fbk Speed Tol	4		72	SS Out Mode	1
41	Sbk Pos Tol	1		73	SLS Out Mode	0
42	Direction Mon	0		74	Door Out Mode	0

Nastavení parametrů pomocí programátoru HIM se provádí podle následujících kroků:

1. Uživatel zadá heslo (parametr P1, od výroby nastaveno na 0).
2. Stav relé nastaví na Unlock (P5 = 0), rozbliká se dioda Lock.
3. Změní režim relé na Program (P6 = 0).
4. Změní všechny potřebné parametry podle tabulky 4.3.
5. Pokud je to nutné, změní heslo (P13) a uloží ho (P17 = 1).
6. Změní heslo na nové (P1).
7. Přepne relé do režimu Run (P6 = 1).
8. Uzamkne nastavení (P5 = 0).
9. Provede restart napájení (Dioda Lock svítí = relé uzamčeno).

5 DEMONSTRAČNÍ ÚLOHA Č. 2

Druhá výuková bezpečnostní laboratorní úloha je obdobně jako první sestavena na stolním panelu (Obrázek 5.1) ve školní laboratoři. Panel navrhla a zkonstruovala firma EK-Industry, která použila komponenty od firmy Rockwell Automation. Cílem je vytvořit demonstrační laboratorní úlohu zabývající se snížením rizik stroje. Koncept celé úlohy je zaměřen na použití CIP Safety technologie. Postup navržení a realizace této úlohy je popsán v následujících kapitolách.

Obrázek 5.1: Bezpečnostní laboratorní úloha č.2

5.1 Posouzení rizik

Posouzení rizik se provede stejným postupem, jako u demonstrační úlohy č. 1.

Laboratorní úloha č. 2 simuluje bezpečnostní opatření kolem stroje. Jelikož úloha neobsahuje fyzický stroj, pro účely této úlohy bylo použito robotické rameno jako virtuální stroj (Obrázek 5.2). Tento stroj byl do výroby dodán jeho výrobcem a je na provozovateli, aby zajistil jeho bezpečný provoz. Prvním krokem při posouzení rizik robotického ramene je určení jeho mezních hodnot.

Obrázek 5.2: Virtuální stroj – robotické rameno

5.1.1 Určení mezních hodnot

Určení mezních hodnot je první fáze při posouzení rizika. Je nutné definovat pohybový rozsah stroje, režimy a prostředí, ve kterém bude pracovat a pracovní dobu. Robotické rameno měří v nejvyšším bodě 2,5m a pohybuje se v okruhu 2 m kolem své základny. Stroj má pracovat ve dvou režimech – pracovním a servisním. Volba režimu je ovládána obsluhou. Při servisním režimu musí být zajištěn bezpečný stav stroje (musí být zastaven popřípadě odpojen od energie).

V této úloze bude předpokládáno, že se stroj nachází ve školní laboratoři. Na úloze budou pracovat studenti přibližně 10 hodin týdně během semestru. Dle normy je nutné provádět na zařízení kontrolu bezpečnosti minimálně jednou za rok. Protože máme místo stroje pouze panel se bezpečnostními komponenty, je nutné kontrolovat funkčnost bezpečnostních (bezpečnostní relé magnetické snímače, zámek, E-stop), jistících (jističe a stykače), mechanických (ochranné kryty) a elektrických prvků (např. tlačítka).

5.1.2 Identifikace úloh a nebezpečí

Je nutné definovat všechny předvídatelné nebezpeční a nebezpečné situace. Normou ČSN EN ISO12100 je požadováno vytvořit následující seznam nebezpečí, které je nutno vzít v úvahu při konstruování strojního zařízení.

Nebezpečí:

1. Mechanické nebezpečí
    a. Stlačení ramenem
    b. Navinutí otáčející se částí ramene
    c. Vtažení nebo zachycení při pohybu ramene
    d. Naražení a střih končetin
2. Elektronické nebezpečí
    a. Zásah nebo smrt elektrickým proudem v rozvaděči
    b. Zásah nebo smrt elektrickým proudem při dotyku kovové části stroje

3. Nebezpečí hluku
    a. Hluk při pohybu ramene
    b. Hluk z frekvenčního měniče
4. Nebezpečí uklouznutí, zakopnutí a pádu

Nebezpečné úlohy:

5. Seřizování a servis
    a. Seřizování a čištění stroje
    b. Výměna a oprava poškozených dílů

5.1.3 Odhad rizika

U výše identifikovaných nebezpečí je nutné určit, jak velké představují riziko.

Technická zpráva ISO TR 14121-2 „Posouzení rizik – praktické směrnice a příklady metod“ představuje praktické vodítko a ukazuje různé postupy hodnocení rizik.

Při vyčíslení rizika budeme určovat následující faktory:

- Závažnost potenciálního zranění
- Četnost vystavení
- Pravděpodobnost zranění

Závažnost potencionálního zranění je v bodu *1. Mechanické nebezpečí* velké, kdy hrozí v nejhorším případě trvalá invalidita nebo i smrt. Toto hodnocení se týká i bodu *5. Seřizování a servis*. Bod *2. Elektrické nebezpečí* je v této kategorii možné hodnotit až smrtí.

Četnost vystavení mechanickému nebezpečí je velmi častá, protože se nyní může obsluha přiblížit k ramenu kdykoliv. Stejné hodnocení platí i v bodě *5. Seřizování a servis*. Elektrické nebezpečí může nastat při otevření rozvaděče, nebo při poruše stroje a spojením konstrukce s fázi. Tento stav může nastat velmi zřídka. Četnost uklouznutí je také malá.

Stroj se dokáže pohybovat velkou rychlostí, a proto je pravděpodobnost výskytu mechanického nebezpečí jistá. Pravděpodobnost úrazu elektrickým proudem není příliš pravděpodobná a vystavení nebezpečí hluku lze ohodnotit jako jisté. Jelikož je stroj umístěn v laboratoři, obsluha má pravděpodobnost uklouznutí, zakopnutí a pádu možnou.

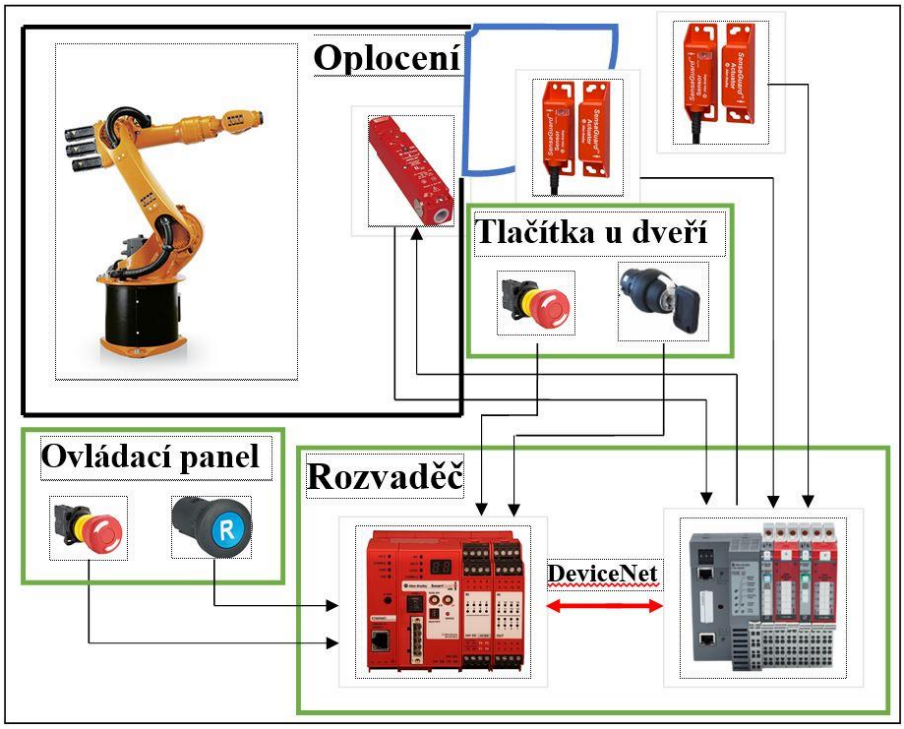
5.1.4 Opatření pro snížení rizika

Finálním krokem při snižování rizika stroje je navržení ochranných opatření. V normě ČSN EN ISO 12100 je definován typ a postup použití jednotlivých opatření.

Nejjednodušším a nejúčinnějším opatřením je oplocení celého stroje. Toto oplocení je nutné pevně ukotvit kolem stroje (např. přišroubovat k podlaze) a mělo by dosahovat minimální výšky 2m. Aplikací tohoto opatření je riziko sníženo o bod *1. Mechanické nebezpečí*. Z důvodů úkonů obsluhy - *4.* S*eřizování a servis* - je nutné umožnit obsluze

přístup ke stroji. Do oplocení byly namontovány dveře pro snadný přístup. Touto úpravou oplocení bylo umožněno přístupu obsluhy do stroje i v režimu chodu. Aby se tomu zamezilo, je nutné použít *Bezpečnostní ochranné a doplňkové zařízení.*

Pro opětovné dosaženi minimálního rizika je nutné monitorovat stav dveří (otevření a zavření). K tomuto úkolu je vhodné použít magnetické spínače SensaGuard. Z důvodů větší bezpečnosti se na dveře naistaluje ještě elektronický zámek. Výše zmíněné bezpečnostní komponenty jsou součástí bezpečnostních funkcí. Na obrázku 5.3 je zobrazeno blokové zapojení jednotlivých elektrických komponentů kolem virtuálního robotického ramene.



Obrázek 5.3: Blokové zapojení bezpečnostních komponentů robotického ramene

Bezpečnostní funkce nouzového zastavení

Tato funkce se aktivuje poté, co logické zařízení detekuje stisknutí nouzového tlačítka, nebo rozepne magnetický spínač. Výstupem této funkce by mělo být zastavení stroje, nebo ideálně odpojení zdroje rizika od energie. Jelikož uvedení ramene do bezpečného stavu není úkolem této úlohy, je zde stav stroje indikován kontrolkami a to zelená pro stav chodu a červená pro stav stop (bezpečný stav). Výstupem této funkce je tedy hlášení řídicímu systému robotického ramene o aktivaci bezpečnostní funkce a příkaz k jeho zastavení. Pokud je stroj ve stop režimu (svítí, nebo bliká červená kontrolka) je odemčen elektronický zámek a obsluha může vejít ke stroji. Do režimu chodu se stroj vrátí po zavření dveří, deaktivaci E-Stop tlačítek a stisknutím modrého tlačítka reset.

Funkce servis

Tato funkce není úplně bezpečnostní, ale při jejím zvolením je nutné provést bezpečnostní opatření, než je umožněn vstup osob do oplocení. Přepnutí přepínače z režimu chodu do režimu servis je vyvolán požadavek na zastavení robotického ramene. Tato funkce je použita z důvodu šetrnosti ke stroji, kdy se nejprve počká, až se dokončí pracovní operace a až poté se umožní vstup osob do oplocení (odemčení zámku). Pro znázornění této situace je po aktivaci funkce servis vloženo časové zpoždění před odemčením zámku (v tomto čase by se měl stroj zastavit). Pro vrácení do režimu chodu je nutné zavřít dveře, přepnout přepínač do režimu chod a poté zmáčknout resetovací tlačítko.

5.2 Ověření bezpečnosti

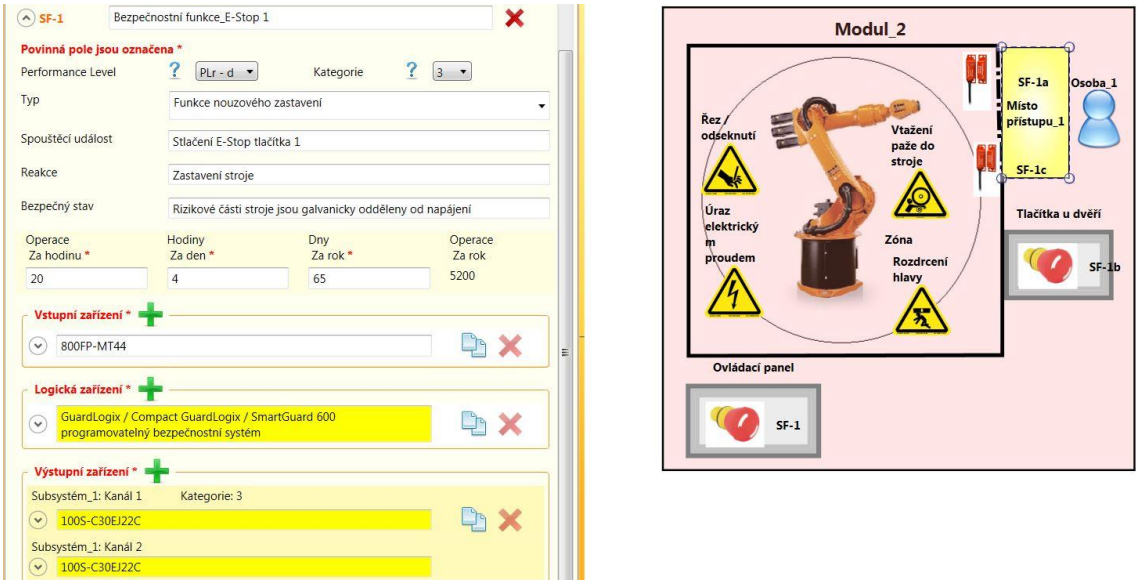
Ověření bezpečnosti se konstruktér ujišťuje, že byl stroj navrhnut podle příslušných bezpečnostních norem. Nejprve je nutné definovat požadovanou úroveň vlastností podle grafu na obrázku 2.1. V kapitole 5.1. byly definovány nebezpečí, které je nutné zhodnotit. Jako nejvíce rizikové bylo označeno *Mechanické nebezpečí*. Důsledek těchto zranění byl klasifikován až smrtí proto byl zvolen parametr *S2*. Obsluha je tomuto nebezpečí vystavena neustále tzn. F2. Všechny mechanické nebezpečí jsou pozorovatelné (na rozdíl od elektrických) a z tohoto důvodu volíme parametr P1. Požadovaná hodnota je tedy PLr d. K ověření dosažené úrovně použijeme nástroje SAB a SISTEMA.

5.2.1 Použití nástroje Safety Automation Builder a SISTEMA

Projekt byl vytvořen podle návodu v kapitole 2.9.1. Byl pojmenováno *Panel_2*, úroveň vlastností nastavena na PLr-d a byl vložen obrázek robotického ramene. V projektu byly vytvořeny následující funkce:

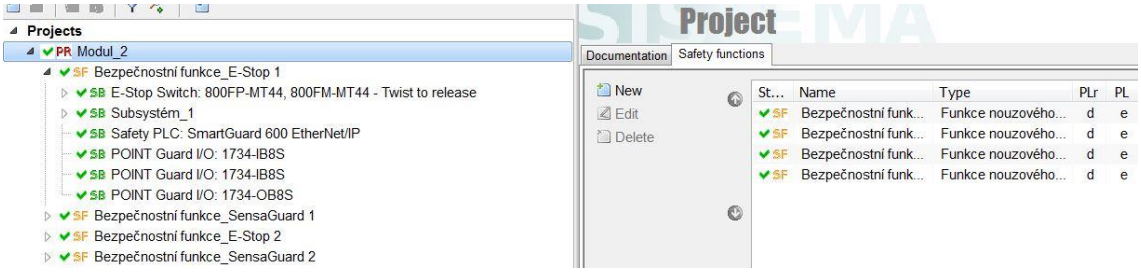
Bezpečnostní funkce_E-Stop 1 je funkce typu nouzového zastavení. Čestnost použití je natavena na 20 operací za hodinu, 4 hodiny za den a 65 dnů za rok což odpovídá práci studentů na úloze během semestru. Vstupní zařízení je tlačítko E-Stop 1, jako logické zařízení byl navržen PLC automat SmartGuard 600 se dvěma vstupními bezpečnostními moduly IB8S a jedním výstupním modulem OB8S. Jako výstupní zařízení byly zvoleny dva redundantní stykače 100S-C. Osazení stykačů je nutné pro dosažení požadované úrovně bezpečnosti, ale jejich použití není úkolem laboratorní úlohy. Totožná funkce byla vytvořena i pro druhé E-Stop tlačítko.

Dále byly vytvořeny dvě bezpečnostní funkce nouzového zastavení iniciovány bezpečnostním krytem. U obou funkcí byl vybrán snímač SensaGuard jako vstupní zařízení, logické a výstupní zařízení zůstalo stejné, jako v předešlých funkcích. Pracovní okno a nastavení funkce E-Stop 1 je zobrazeno na obrázku 5.4. Posledním krokem k ověření je zvolení exportu operace do SISTEMA.



Obrázek 5.4: Příklad nastavení bezpečnostní funkce E-Stop 1 v nástroji SAB

Nástroj SISTEMA podává konstruktérovi zpětnou vazbu o kvalitě jeho návrhu a zda dosáhl nebo nedosáhl požadované PLr. Obrázek 5.5 zobrazuje výsledné hodnocení navržených funkcí. Požadovaná PLr byla d a tento návrh dosahuje až na úroveň e. Zelené značky znamenají správnost návrhu. Výpis programu je zobrazen na přiloženém CD.



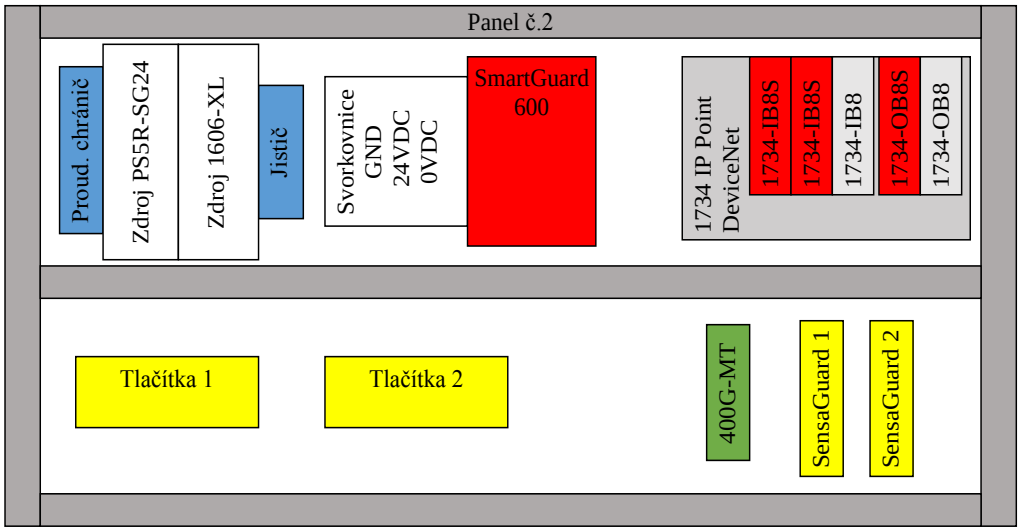
Obrázek 5.5: Ověření dosažení úrovně vlastností v nástroji SISTEMA

5.3 Realizace bezpečnostní úlohy

Tato část laboratorní úlohu se zabývá úpravou elektroinstalace laboratorního panelu č. 2, který fyzicky představuje virtuální stroj. Dosavadní zapojení od firmy EK-Industry bylo nutné zkontrolovat a v některých případech provést změny. Použití a zapojení jednotlivých komponentů je popsáno níže.

5.3.1 Panel č. 2

Laboratorní panel č. 2 obsahuje bezpečnostní instrumentaci, jejíž soupis je v tabulce 5.1. Blokové rozmístění těchto komponentů je zobrazeno na obrázku 5.6. Panel je napájen 230V přes eurozásuvku na zadní straně panelu. Vedle ní je ještě umístěn hlavní vypínač. Rozvod 230V je dále jištěn pojistkou a proudovým chráničem (modře), ze kterého je napájeny zdroje PS5R-SG24 a 1606-XL. Všechny komponenty jsou napájeny zdrojem PS5R-SG24, ke kterému je přes jistič (modře) připojena svorkovnice 24VDC pro kladný pól a 0VDC pro záporný pól. Zdroj 1606-Xl slouží pouze k napájení sítě DeviceNet.



Obrázek 5.6: Blokové schéma laboratorního panelu č.2

Bezpečnostní komponenty jsou zde barevně rozděleny do tří skupin. Žlutě jsou označené vstupy bezpečnostních funkcí, červeně logické zařízení a zeleně výstupy funkcí. Celý bezpečnostní systém je zapojen podle architektury *kategorie 3* normy ČSN EN ISO 13849. Logickou jednotkou je zde bezpečnostní PLC SmartGuard 600, které realizuje všechny bezpečnostní funkce stroje. K tomuto PLC je přes síť DeviceNet připojen modul POINT Guard I/O obsahující bezpečnostní karty. Vstupními zařízeními jsou dva bezkontaktní spínače SensaGuard, dvě E-Stop tlačítka, modré resetovací tlačítko a přepínač pro změnu režimů stroje. Výstupním zařízením je pouze elektronický zámek GuardMaster. Jak již bylo řečeno v kapitole návrhu bezpečnostní funkce, panel fyzicky neobsahuje dva bezpečnostní stykače pro odpojení napájení přívodu energie. Jejich zapojení není úkolem této úlohy, nicméně jejich použití je pro dosažení úrovně PL nutné. Dále bude počítáno s tím, že virtuální stroj je připojen přes dva stykače 100S-C, které jsou ovládané SmartGuard 600. Jejich stav je indikován zelenou a červenou kontrolkou.

Tabulka 5.1: Seznam komponentů laboratorního panelu č.2

Panel č.2	**Popis**
Zdroj PS5R-SG24	24VDC / 10A
Zdroj AB 1606-XL	24VDC / 8A
SmartGuard 600	Bezpečností PLC
Vzdálený modul IO karet	
1734_AENT	DeviceNet I/O adaptér
1734-IB8S	24VDC bezpečnostní vstupní karta
1734-IB8S	24VDC bezpečnostní vstupní karta
1734-IB8	24VDC vstupní karta
1734-OB8S	24VDC bezpečnostní výstupní karta
1734-OB8	24VDC výstupní karta
440G-MT	Guard master bezpečnostní elektronický zámek, 24V DC, 3 N.C. a 1 N.O. kontakty
440N-Z21SS2AN9	Senza Guard bezkontaktní magnetický spínač
Panel s tlačítky	
E-Stop	2 N.C. kontakty
Modré reset	1 N.O. kontakt
Přepínač módu	2 N.C. kontakty
Červená kontrolka	24VDC
Zelená kontrolka	24VDC

5.3.2 Popis bezpečnostního PLC SmarGuard 600

Bezpečnostní PLC SmartGuard 600 [20] (dále jen SG 600) je určené pro náročnější aplikace než bezpečnostní relé. PLC disponuje šestnácti digitálními vstupy, osmi digitálními výstupy, čtyřmi pulzními testovacími výstupy (slouží jako zdroj vstupů) a USB port. Dále je vybaven síťovým rozhraním DeviceNet a EtherNet/IP s podporou komunikace CIP Safety. SG 600 je certifikované pro použití v bezpečnostních aplikací až do úrovně intergrity (SIL) 3 a úrovně vlastností (PL) e.

Obrázek 5.7: Bezpečnostní PLC SmartGuard 600

Bezpečnostní vstupy podporují následující funkce:

1. Diagnostika – pomocí zdroje pulzů SG 600 sleduje poruchy připojených zařízení
2. On a Off zpoždění – nastavení časového filtru 0-126ms pomáhá snížit vliv klepání a chvění.
3. Dvoukanálový režim – lze nastavit mezi dvěma zvolenými vstupy, nastavení je nutné použít dle použité bezpečnostní kategorie

Bezpečnostní výstupy podporují následující funkce:

1. Diagnostika – pomocí zdroje pulzů SG 600 sleduje poruchy připojených zařízení
2. Rozpoznání přetížení – výstup je odpojen při průtoku velkého proudu
3. Dvoukanálový režim – lze natavit mezi dvěma zvolenými výstupy, při zjištění chyby jsou oba výstupy nastaveny do bezpečného stavu

Pulsní testovací výstupy se obvykle používají s bezpečnostními vstupy. Mohou byt nastaveny jako standartní zdroj. Umí poznat přetížení, na které reagují odpojením výstupu.

PLC může pracovat samostatně, nebo působit na síti DeviceNet jako master nebo slave zařízení nebo zároveň plnit obě funkce. Může také komunikovat současně se sítěmi DeviceNet i EtherNet/IP a posílat mezi nimi zprávy.

SmartGuard 600 lze programovat po síti DeviceNet nebo EtherNet/IP nebo také připojením přes USB. Konfigurovat toto zařízení lze v nástroji RSNetWorx, minimální verze 8.0. Řídící program se tvoří v Logic editoru v prostředí RSNetWorx. Při programování se používají základní logické operace jako AND a OR, funkční bloky (např. E-Stop) a binární vstupy a výstupy.

5.3.3 Popis POINT Guard I/O

POINT Guard I/O je modul zprostředkovávající komunikaci mezi sítovým rozhraním DeviceNet a I/O kartami. Tento modul je rozšiřující slot pro PLC sestavy GuardLogix nebo pro SmartGuard 600. POINT I/O komunikuje pomocí protokolu CIP Safety přes síť DeviceNet s řídícím procesorem. Je tedy vhodný pro bezpečnostní aplikace až do SIL3 a PLe.

Základní částí celého modulu je POINT I/O DeviceNet Communication Interface Module [21]. Slouží jako napájení základny pro I/O karty a také jako port pro připojení komunikace. V této aplikaci byla zvolena osmimístná základna, ve které jsou zapojeny dvě vstupní bezpečnostní karty 1734-IB8S (každá zabere 2 místa), jedna standartní vstupní karta 1734-IB8, jedna bezpečnostní výstupní karta 1734-OB8S a jedna výstupní karta 1734-OB8. Nebezpečnostní karty (IB8 a OB8) nejsou na panelu používány, a proto nebudou dále zmiňovány. Jednotlivé karty komunikují po síti DeviceNet (každá karta má svou adresu). Jejich nastavení se jako u SmartGuard 600 provádí v nástroji RSNetWorx.

5.3.4 Popis 1734-IB8S

Digitální vstupní bezpečnostní karta 1734-IB8S [22] disponuje 8 bezpečnostními vstupy, čtyřmi zemnícími svorkami a čtyřmi pulzními testovacími výstupy. Karta umožnuje připojit bezpečnostní zařízení jako E-Stop tlačítko, spínače dveří a světelné závory. Vstupy mohou být nastavený jako jednokanálové (při použití bezpečnostních senzorů) nebo dvoukanálové. Jako zdroj lze použít pulzní testovací výstupy. V dvoukanálovém zapojen je vyhodnocován soulad mezi dvěma vstupními signály. V obou těchto případech zapojení dosahuje úroveň bezpečnosti kategorie PLe a SIL3.

5.3.5 Popis 1734-OB8S

Digitální **výstupní** bezpečnostní karta 1734-OB8S [22] disponuje 8 bezpečnostními výstupy, a 8 zemnícími svorkami. Karta umožnuje připojit bezpečnostní zařízení jako jsou elektronické zámky nebo bezpečnostní stykače. Pokud je výstup nastaven jako jednokanálový s funkcí pulzního testování, zapojení dosahuje PLd a SIL 2. V dvoukanálovém režimu zajišťuje redundantní kontrolu výstupu pomocí pulzního testování a dosahuje PLe a SIL3.

5.3.6 Popis ostatních bezpečnostních prvků

Mezi výstupní komponenty bezpečnostní funkce patří elektronický zámek **440G-MT** [18]. Tento obsahuje ovládací 24V DC cívku s funkcí *power to release* a kontakty, které monitorují její polohu (3 N.C. a 1 N.O.). Jelikož zámek neumožňuje monitorování polohy jeho západky, je nutné vedle něj nainstalovat alespoň jeden snímač polohy západky (nebo součásti k ní připevněné, například dveří). K tomuto úkolu zde slouží dva magnetické snímače **SensaGuard** [19] kat. č. 440N-Z21SS2H-AS. Disponují dvoukanálovým výstupem OSSD. Mohou být použity k zabezpečení až dvou dveří.

5.3.7 Popis zapojení

Pro dosažen požadované úrovně vlastností je nutné použít jako zdroj napětí vstupních zařízení speciální bezpečnostní výstupy PLC. Z tohoto důvodu je tlačítko E-Stop 1 napájeno z testovacích výstupů SG 600 (T0 a T1) a jeho výstupní signál je připojen ke vstupní svorkám I0 a I1. Druhý bezpečnostní okruh je zapojen z testovacích výstupů T2 a T3 přes kontakty E-Stop 2 tlačítka do vstupů I2 a I3. Ze stejných zdrojových svorek je připojen i přepínač režimů (SLS) a jeho signál snímají vstupy I4 a I5. K PLC SG 600 je připojeno i tlačítko Reset mezi svorky T1 a I15.

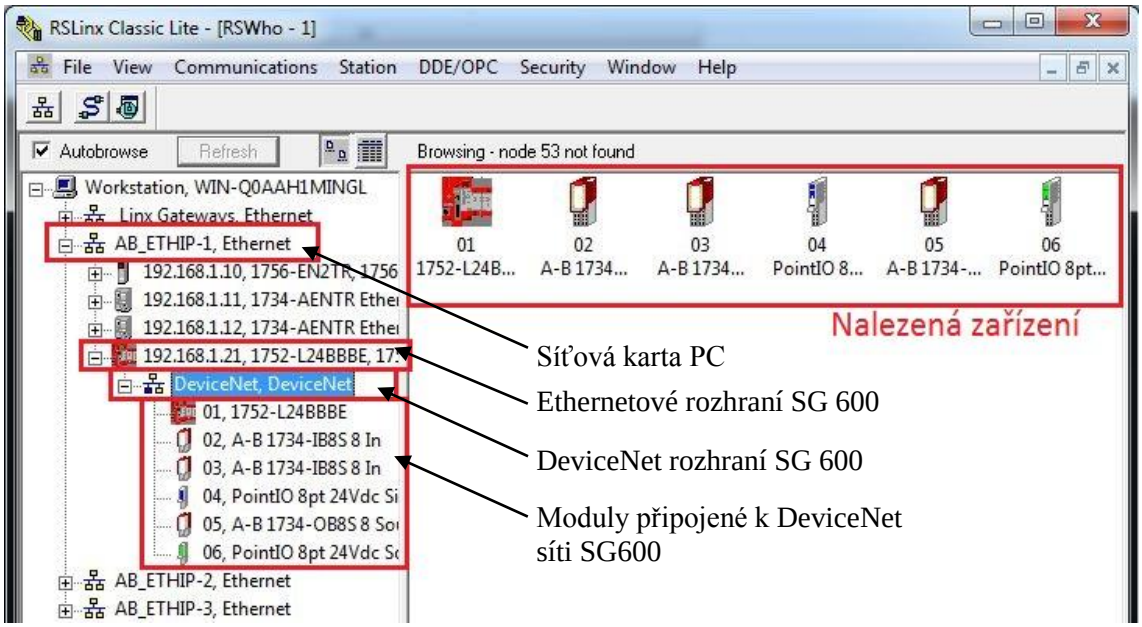
Výstupy magnetických snímačů SensaGuard jsou připojeny do bezpečnostní karty IB8S_1. Zdrojem signálového okruhu snímače SensaGuard_1 jsou svorky T0 a T1 karty IB8S_1. Výstupy snímače jsou připojeny na svorky I0 a I1. Vstup druhého snímače SensaGuad_2 je připojen na svorky T2 a T3 a výstup směřuje do svorek I2 a I3. Do druhé karty IB8S_2 jsou připojeny kontakty zámku 400G-MT, které monitorují polohu západky. Okruh je veden z testovacích výstupu T0 a T1 přes kontakty zámku do vstupů I0 a I1 karty IB8S_2. Do vstupů této karty jsou ještě připojeny 4 tlačítka a to zelené do

I4, červené do I5, a dvě černé do I6 a I7. Tyto tlačítka nejsou v této úloze používána. Výstupní kartou IB8S je ovládána cívka zámku 400G-MT a tři barevné kontrolky. Cívka zámku je připojena mezi svorky 0O a COM 0. Modrá kontrolka je připojena na výstup O4, zelená na O5 a červená na O6. Druhé kontakty kontrolek jsou připojeny na zem. Přesné zapojení všech komponentů je zaznamenáno v elektrickém schématu v Příloha 2.

5.4 Konfigurace zařízení

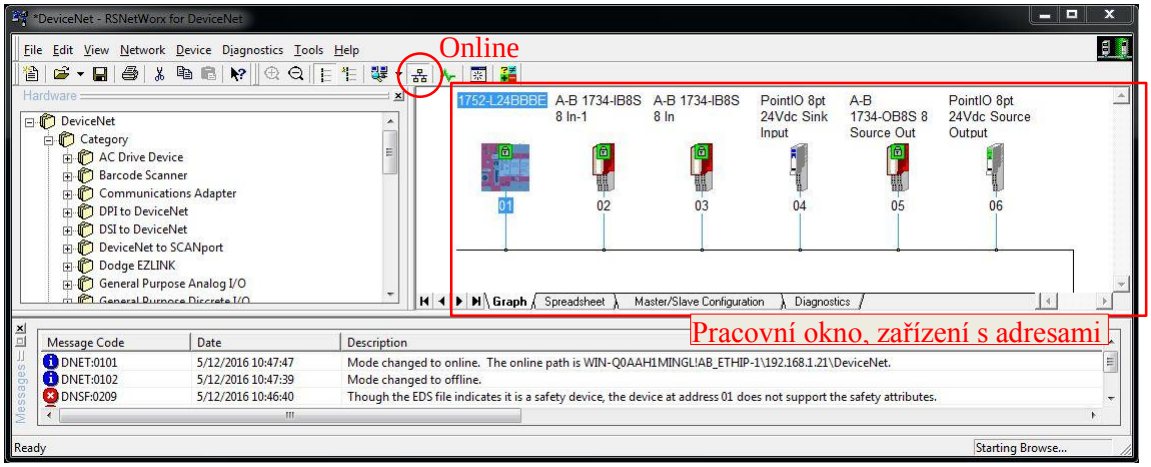
Konfigurace zařízení se skládá z několika kroků. Nejprve je nutné nastavit komunikaci jednotlivých zařízení po síti DeviceNet, poté jim nastavit parametry a následně vytvořit logické funkce řídícího PLC SG 600. Konfigurace zařízení se provádí pomocí nástroje *RSLinx Classic, RSNetWorx a BOOTP/DHCP*.

RSLinx Classic [24] je komunikační program od firmy Rockwell Automation. Program zprostředkovává komunikaci mezi PC a sítovými zařízeními od firmy Rockwell Automation. Tento program používají ke komunikaci se zařízeními všechny nástroje od firmy Rockwell Automation (např. RSLogix5000 a FactoryTalk view studio). Požadovaná verze je 2.55 a novější. V RSLinx je nutné nejprve nastavit komunikaci se síťovou kartou PC. Po zpuštění programu se zvolí záložka *Communication/Configure Drivers.*. V rolovacím menu se vybere EtherNet/IP Driver, klikne na *Add New*.. a přidá se síťová karta, ke které je připojeno PLC. Nastavená komunikace je potom vidět v pracovním okně programu (Obrázek 5.8).



Obrázek 5.8: Pracovní prostředí RSLinx Classic

RSNetWorx [25] je softwarový nástroj od firmy Rockwell Automation. Slouží pro konfigurací sítových zařízení. V této úloze bude použit program pro sít DeviceNet. Umožnuje vytvářet různé topologie sítě DeviceNet a spravovat jednotlivá zařízení. Pracovní okno je zobrazeno na obrázku 5.9.



Obrázek 5.9: Pracovní prostředí RSNetWorx for DeviceNe

5.4.1 BOOTP/DHCP

Jak již bylo popsáno v kapitole 5.3.7 Popis zapojení, k síti DeviceNet je připojeno PLC SG 600 a POINT I/O s pěti moduly. Moduly jsou zařízení komunikující po síti.

První zařízení, které je nutné konfigurovat je PLC SmartGuard 600. Nastavení je možné provést před USB port (pomalá a zdlouhavá metoda), nebo přes některé síťové rozhraní (DeviceNet nebo EtherNet/IP). Nejvýhodnější je použít EtherNet/IP.

Nastavení komunikace mezi SG 600 a PC

U tohoto nastavení se naskytují dvě možnosti. Pokud již bylo někdy SG 600 připojeno před EtherNet/IP a má nastavenou statickou adresu, můžeme jej najít v programu RSLinx.

Pokud SG 600 není nalezeno nástrojem RSLinx, nemá přidělenou IP adresu. Přidělení se provádí nástrojem BOOTP/DHCP. Po otevření nalezne zařízení připojená na sít EtherNet/IP. Vybereme MAC adresu, která nemá přidělenou IP adresu (je to MAC adresa SG 600) a přidělíme jí adresu 192.168.0.21 (pro tuto laboratorní úlohu). Poté otevřeme RSLinx, po rozkliknutí zvoleného ethernetového připojení je vidět SG 600 s nadefinovanou IP adresou (Obrázek 5.8). Nyní je nutné nastavit tuto adresu jako statickou. Po kliknutí pravým na SG600 (v RSLinx je zobrazena jeho IP adresa) vybereme *Module Configuration/ Port Configuration* a zvolí se statické nastavení sítě (IP adresu můžeme změnit, nebo ponechat stejnou).

5.4.2 Nastavení sítě DeviceNet

V této laboratorní úloze je na sít DeviceNet připojeno celkem 6 zařízení (SG 600 a 5 I/O modulů). Každé zařízení musí mít vlastní DeviceNet adresu. Pokud již byly adresy přiděleny, můžeme moduly vidět v RSLinx jako zařízení připojené ke SG 600. Pokud zařízení (I/O moduly) nemají přiřazené adresy, nebo je chceme změnit, použijeme nástroj RSNetWorx for DeviceNet, kde adresy změníme.

Nastavení DeviceNet adres

U SG 600 se jeho adresa nastavuje na čelním panelu pomocí DIP přepínače. Při změně adresy je nutné, aby PLC bylo odpojeno od napájení. V této úloze mu byla nastavena adresa 01.

V případě, že jednotlivé I/O moduly nemají přidělené adresy (nevidíme je v RSLinx), mají všechny od výroby adresu 63. Změna se provede následujícími kroky:

1. Na síť připojíme jen jedno nové zařízení (v první kroku tedy jen IB8S-1).
2. V RSNetWorx klikneme na *online* a vybereme ethernetové spojení s SG 600.
3. RSNetWorx zobrazí nalezené zařízení v pracovním okně (vidíme SG 600 s adresou 01 a kartu IB8S-1 s adresou 63).
4. Změníme její adresu kliknutím na *Tools/Node Commissioning..* Zvolíme *Browse…* vybereme příslušnou ethernetovou síť, a zvolíme DeviceNet modul SG 600.
5. V okně *Node Commissioning* změníme adresu na 02 a klikneme na *Apply*.
6. Přepneme se do režimu *offline* a pak do *online,* konfigurované zařízení nalezneme s novou adresou.
7. V dalším kroku připojíme druhou I/O kartu IB8S a přiřadíme jí adresu 03
8. Podle kroků *2.až 6.* nastavíme adresy všem zařízením na síti DeviceNet.

Výsledná topologie sítě je zobrazena na obrázku 5.9.

Všem zařízením je nutné přidělit *Safety Network Number*. Toto číslo generuje master PLC a musí se nakopírovat do všech přidružených zařízení v síti. Vložení stejného čísla do zařízení zabezpečí síti její jedinečnost, což vyžaduje zabezpečení CIP Safety. V programu RSNetWorx se přepneme do režimu *Online,* poté dvakrát klikneme na SG 600 a v záložce *Safety* klikneme na *Safety Network Number* a na tlačítko *Copy.* Poté dvakrát klikneme na každé zařízení v síti, otevře se okno *Safety Network Number Mismatch* kde je již nové *Software Safety Network Number* vloženo, stačí kliknout na *Download*. Tímto krokem jsme spojili všechna zařízení do jedné sítě přidružené SG 600.

5.4.3 Konfigurace bezpečnostních modulů řady POINT I/O

Bezpečnostní moduly řady POINT I/O komunikují pomocí protokolu CIP Safety. Tato komunikace vyžaduje nastavit vlastnosti vstupů, výstupů a zdrojových pulzních svorek jednotlivých zařízení. Tento úkon se provádí v nástroji *RSNetWorx.* Nejprve se přejde do režimu *Online,* v pracovním okně se zobrazí připojená zařízení na síti DeviceNet. Pro každý bezpečnostní modul se musí provést nastavení kliknutím pravým tlačítkem na vybraný modul a volbou *Properties….* V dotazovacím okně se zvolí *Upload* nastavení. Následně se otevře okno a zvolí se záložka *Safety Configuration.* Zde se nastaví vstupy a výstupy bezpečnostního výstupního modulu OB8S podle tabulky 5.2. Na závěr se klikne na *Apply*.

Tabulka 5.2: Nastavení modulu 1734-OB8S

Modul 4, Adresa 05	
Parameter	Current Value
Output Points 00/01	
output 00/01 Operation Type	Single
Output 00 Mode	Safety
Output 01 Mode	Not Used
Output Points 04/05	
output 04/05 Operation Type	Single
Output 04 Mode	Safety
Output 05 Mode	Safety
Output Points 06/07	
output 06/07 Operation Type	Single
Output 06 Mode	Safety
Output 07 Mode	Not Used

Stejným postupem se nastaví i první vstupní modul 1734-IB8S-1 podle tabulky 5.3 a druhý vstupní modul 1734-IB8S-2 podle tabulky 5.4.

Tabulka 5.3: Nastavení modulu 1734-IB8S-1

Modul 1, Adresa 02	
Parameter	Current Value
Input Points 00/01	
Input 00/01 Operation Type	Single
Input 00/01 Operation Discrepancy	0x10ms
Input 00 Mode	Safety
Input 00 Test Source	None
Input 00 Off -> On Delay Time	0 ms
Input 00 On -> Off Delay Time	0 ms
Input 01 Mode	Safety
Input 01 Test Source	None
Input 01 Off -> On Delay Time	0 ms
Input 01 On -> Off Delay Time	0 ms
Input Points 02/03	
Input 00/01 Operation Type	Single
Input 00/01 Operation Discrepancy	0x10ms
Input 00 Mode	Safety
Input 00 Test Source	None
Input 00 Off -> On Delay Time	0 ms
Input 00 On -> Off Delay Time	0 ms
Input 01 Mode	Safety
Input 01 Test Source	None
Input 01 Off -> On Delay Time	0 ms
Input 01 On -> Off Delay Time	0 ms
Test Output Points	
Test Output 00 Mode	Power Supply
Test Output 01 Mode	Power Supply
Test Output 02 Mode	Power Supply
Test Output 03 Mode	Power Supply

Tabulka 5.4: Nastavení modulu 1734-IB8S-2

Modul 2, Adresa 03	
Parameter	Current Value
Input Points 00/01	
Input 00/01 Operation Type	Dual-channel Equivaletn
Input 00/01 Operation Discrepancy	0x10ms
Input 00 Mode	Safety Pulse Test
Input 00 Test Source	Test Outout 0
Input 00 Off -> On Delay Time	0 ms
Input 00 On -> Off Delay Time	0 ms
Input 01 Mode	Safety Pulse Test
Input 01 Test Source	Test Outout 1
Input 01 Off -> On Delay Time	0 ms
Input 01 On -> Off Delay Time	0 ms
Input Points 04/05	
Input 04/05 Operation Type	Single
Input 04/05 Operation Discrepancy	0x10ms
Input 04 Mode	Standard
Input 04 Test Source	None
Input 04 Off -> On Delay Time	0 ms
Input 04 On -> Off Delay Time	0 ms
Input 05 Mode	Standard
Input 05 Test Source	None
Input 05 Off -> On Delay Time	0 ms
Input 05 On -> Off Delay Time	0 ms
Input Points 06/07	
Input 06/07 Operation Type	Single
Input 06/07 Operation Discrepancy	0x10ms
Input 06 Mode	Standard
Input 06 Test Source	None
Input 06 Off -> On Delay Time	0 ms
Input 06 On -> Off Delay Time	0 ms
Input 07 Mode	Standard
Input 07 Test Source	None
Input 07 Off -> On Delay Time	0 ms
Input 07 On -> Off Delay Time	0 ms
Test Output Points	
Test Output 00 Mode	Pulse Test
Test Output 01 Mode	Pulse Test

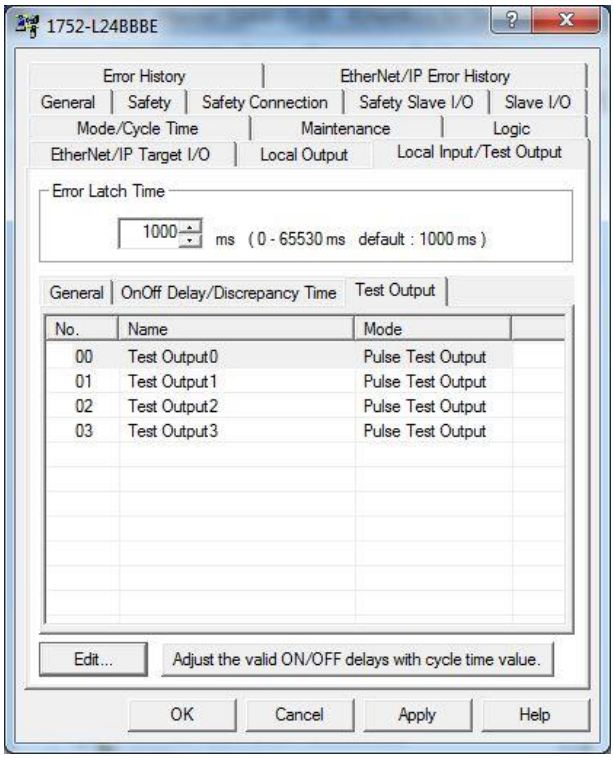
5.4.4 Konfigurace bezpečnostního PLC SG 600

Toto zařízení disponuje šestnácti binárními vstupy, osmi výstupy a čtyřmi testovacími zdrojovými svorkami. Vlastnosti těchto portů je nutné nastavit ve vlastnostech SG 600. V programu RSNetWorx zapneme režim *Online*, dvojitým kliknutím na SG 600 otevřeme vlastnosti a zvolíme *Upload*. Otevřeme záložku *Local Input/Test Output* / *General*. Zde pojmenujeme a nastavíme vstupní svorky pro připojení E-Stop tlačítek a resetu podle tabulky 5.5.

Tabulka 5.5: Nastavení lokálních vstupů SG 600

Local Input/Test Output			
No.	Name	Mode	Test Source
00	E-Stop 1.1	Test pulse from test oout	Test Output0
01	E-Stop 1.2	Test pulse from test oout	Test Output1
02	E-Stop 2.1	Test pulse from test oout	Test Output2
03	E-Stop 2.2	Test pulse from test oout	Test Output3
04	Servis 1.1	Test pulse from test oout	Test Output2
05	Servis 1.2	Test pulse from test oout	Test Output3
15	Reset	Used as safety input	

Zdrojovým signálem pro E-Stop tlačítka jsou pulzní testovací výstupy SG 600, které je nutné nastavit v záložce *Local Input/Test Output* / *Test Output* podle obrázku 5.10.



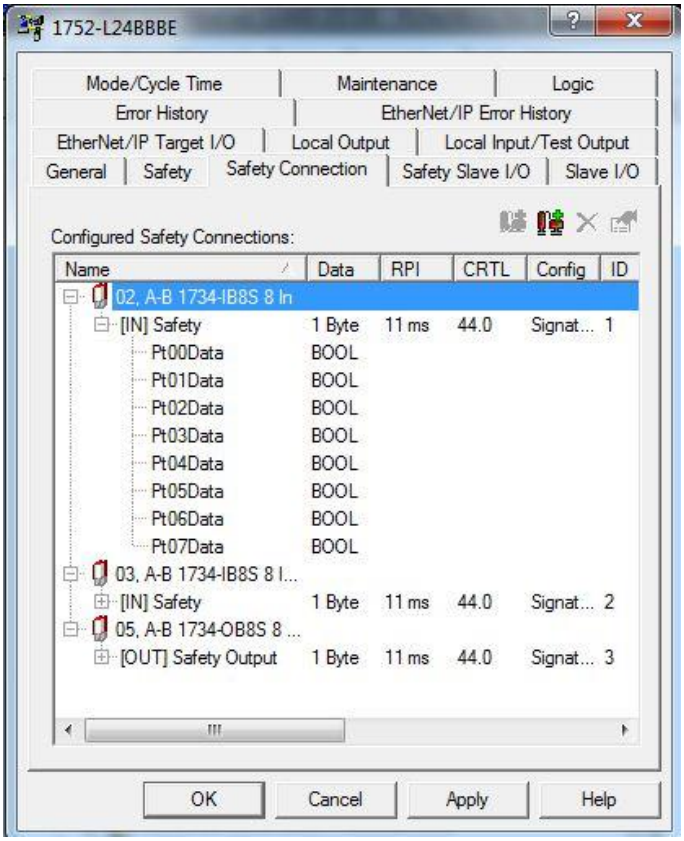
Obrázek 5.10: Nastavení testovacích výstupů SG 600

Nastavení komunikace mezi bezpečnostními moduly a SG 600

SG 600 pracuje jako master zařízení na vytvořené síti DeviceNet. K tomuto PLC je možné přiřadit bezpečnostní slave zařízení, které může master používá jako vlastní vstupy. Konfigurace se provádí ve vlastnostech SG 600 v záložce *Safety Connection.* Kliknutím na *přidat bezpečnostní spojení* a nastavením podle tanulky 5.6 se vytvoří proměnné, které představují porty bezpečnostních modulů. Výsledné nastavení zobrazuje obrázek 5.11.

Tabulka 5.6: Nastavení komunikace I/O modulů a SG 600

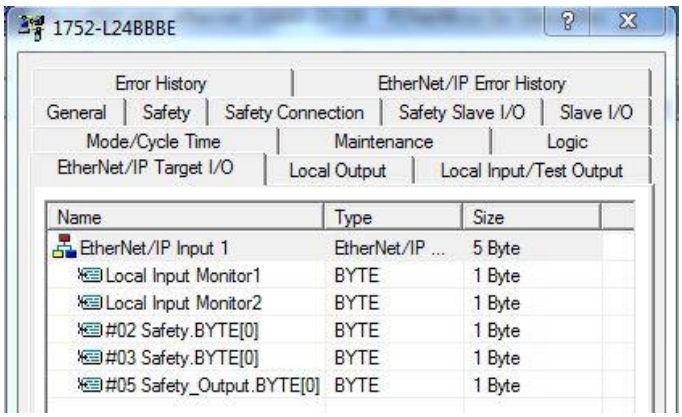
Name			RPI
02,A-B 1734-IB8S 8 In	Connecrion Name	[IN] Safety +C	11ms
	Connecrion Type	Milticast	
	Configuration	Configuration singnature must match	
03,A-B 1734-IB8S 8 In-1	Connecrion Name	[IN] Safety	11ms
	Connecrion Type	Milticast	
	Configuration	Configuration singnature must match	
05,A-B 1734-OB8S 8 Source Out	Connecrion Name	[OUT] Safety Output	11ms
	Connecrion Type	Milticast	
	Configuration	Configuration singnature must match	



Obrázek 5.11: Nastavení komunikace mezi SG 600 a bezpečnostními moduly

Nastavení ethernetové komunikace

Požadavkem na tuto laboratorní úlohu je vytvoření její vizualizace v PC. Pro tento účel je nutné nastavit komunikaci SG 600 a jiného PLC, přes které bude vizualizace spuštěna. Ethernetová komunikace na straně SG 600 se nastavuje v jeho vlastnostech v záložce *EtherNet/IP Targe I/O*. Zde se klikne na *New* a otevře se okno *Edit EtherNet/IP Targe I/O.* V otevřeném okně se zaškrtne položka *Targe Input* a poté se vyberou všechny lokální vstupy zařízení (*Local I/O Monitor* a zaškrtnout *Input [bit0-15]*). Dále se přidají všechny tři bezpečnostní moduly do tabulky *Rounting I/O* (klikne se na *New* a vybere se celý byte jedné karty, pak *OK*). Výsledné nastavení je zobrazeno na obrázku 5.12.

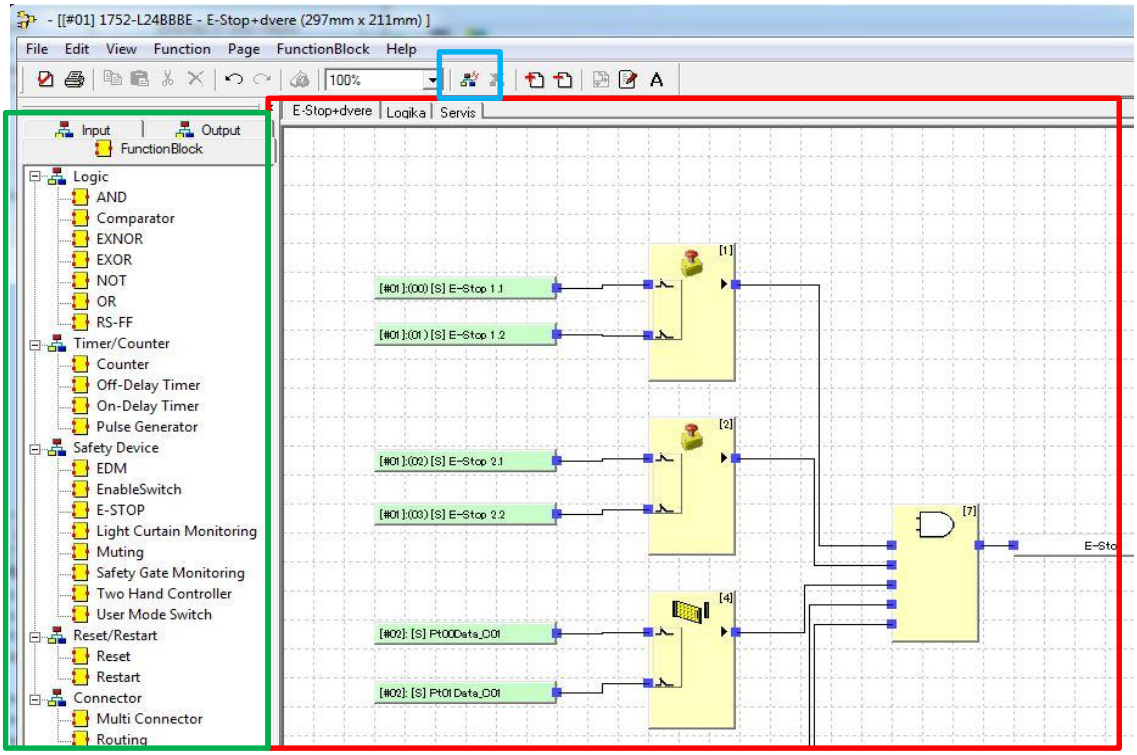


Obrázek 5.12: Nastavení ethernetové komunikace u SG 600

5.4.5 Programové vybavení SG 600

SmarGuard 600 je jednoduché bezpečnostní PLC, které je ovládáno vlastním programem. Tento ovládací software programátor vytváří ve speciální grafickém editoru *Logic*, určeném pro toto PLC. Jednotlivé vstupy a výstupy jsou zde reprezentovány jako zdroje a spotřebiče. Výsledná logika se tvoří vkládáním logických operací například AND a OR do pracovní plochy. Editor obsahuje i funkční bloky pro ovládání speciální funkcí např. E-Stop tlačítka.

Editor nalezneme ve vlastnostech SG 600 v záložce *Logic*. Po kliknutí na *Edit* se otevře editor (Obrázek 5.13). Skládá se z pracovního okna (červeně) do kterého se vkládají vstupy, výstupy a funkce z levého menu (zeleně). Výslednou funkci je možné po nahrání do PLC sledovat přepnutím do režimu *monitoring* (modře). Po ukončení editace logické funkce (zavřením okna) se program nahraje do PLC kliknutím na tlačítko *Apply*.



Obrázek 5.13: Programovací rozhraní *Logic*

Popis programu

Řídicí program SG 600 realizuje navržené funkce v kapitole 5.1.4. Naprogramovaná logika je rozdělena do tří částí (oken). První okno se jmenuje *E-Stop+dveře* a je zde naprogramována bezpečnostní funkce E-Stop tlačítek a magnetických snímačů. Byly použity dva funkční bloky *Emergency Stop Pushbutton Monitoring*, které zpracovávají signál z E-Stop tlačítek a dva funkční bloky *Safety Gate Monitoring*, ke kterým byly připojeny snímače SensaGuard. Výstupem tohoto zapojení je proměnná *E-Stop*. Funkce je zapojena na obrázku 5.13.

V druhém okně *Logika* je vytvořena logická funkce realizující bezpečnostní požadavky aplikace. Je zde použit funkční blok *Restart* zpracovávající signál z resetovacího tlačítka a soustava logických funkcí. Program pracuje tak, že monitoruje stav proměnné *E-Stop*, *Servis* a tlačítka *reset*. Při zmáčknutí E-Stop nebo rozpojení snímače SensaGuard se vyvolá požadavek na zastavení stroje. Jelikož zde není fyzický stroj, je předpokládáno, že se stroj ihned zastaví (indikováno blikáním nebo svícením červené kontrolky). Blikající červená kontrolka značí zmáčknuté E-Stop tlačítko nebo rozpojený snímač SensaGuard. V tomto stavu se odemkne zámek 400G-MT a je možné vejít do oplocení k robotickému ramenu. Před navrácením do stavu chod je nutné zavřít dveře a deaktivovat tlačítka E-Stop. Následně se rozsvítí modré tlačítko reset indikující možnost jeho zmáčknutí. Po resetu se rozsvítí zelená kontrolka indikující režim chod.

Ve třetím okně *Servis* je vytvořena funkce servis, které má za úkol šetrně zastavit robotické rameno s doběhem pracovního úkonu a poté odemknout zámek. Vstupem funkce je přepínač režimů, jehož signál zpracovává funkční blok *Enable Switch*

Monitoring. Funkce vyvolá požadavek na zastavení stroje a počká, až se stroj zastaví a poté odemkne zámek. V této úloze je čekání napevno nastaveno na 2 s z demonstračních důvodů. Zpět do režimu chodu se stroj zapne tlačítkem *reset*. Všechny tři části programu jsou zobrazena v příloze 3.

Export programu je umístěn na přiloženém CD (Sindelek_CIPSafety_Logika.led).

5.4.6 Změna módu SG 600 a validace nastavení sítě

Při nastavování parametrů je SG 600 v režimu *Normal Mode – Idle*. Po nastavení všech parametrů a vytvoření řídícího programu je nutné SG 600 přepnout do režimu automatického zpuštění po připojení napájení. Nastavení se provede ve vlastnostech PLC v záložce *Mode/Cycle Time.* Zde se zvolí bod *Automatic Execution Mode* a klikne se na *Apply*. Po nahrání nastavení do PLC je nutné se k němu znovu připojit (volba režimu *Online*) a ve stejné záložce dole kliknout na tlačítko *Change Mode.*. a zvolit mód *Execute*. Nyní je relé v režimu RUN a bezpečnostní funkce je aktivní.

Validace sítě DeviceNet

Validace slouží k ověření správného nastavení všech komponentů a následnému zamknutí proti změnám. Pokud se uzamčení neprovede, SG 600 nebude po resetu napájení v režimu RUN. Ověření nastavení se provádí v programu RSNetWorx. Zde se přepneme do režimu *online* a zvolíme záložku *Network/ Safety Device Verification Wizard.* Zobrazí se okno, ve kterém vybereme všechna zařízení pro ověření, dále dostaneme report z ověření, poté si vybereme zařízení, která chceme zamknout (zamkneme všechny nabízené) a posledním krokem se zařízení uzamknout.

Výsledkem validace je důkaz správného nastavení všech komponentů na síti a uzamčení jejich nastavení proti změně.

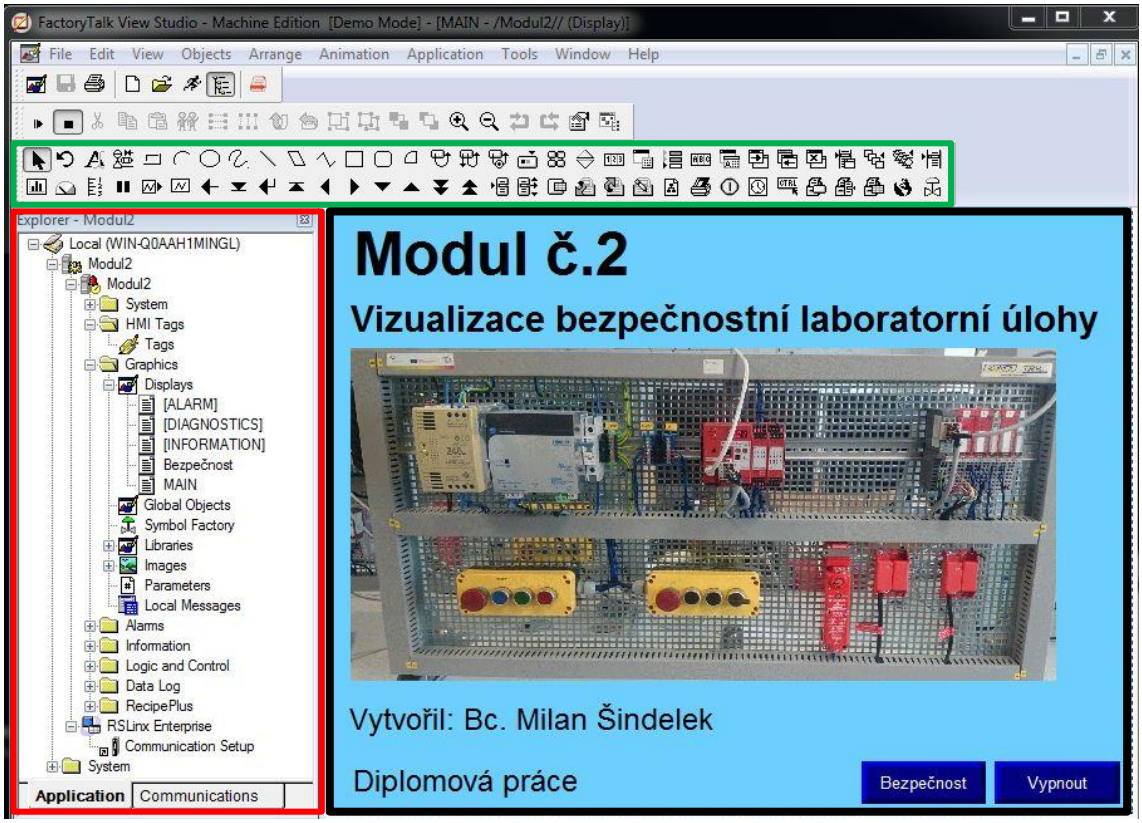
V příloze na CD je uložena záloha projektu sítě z programu RSNetWorx (Sindelek_CIPSafety_DeviceNet.dnt). Soubor obsahuje veškerá nastavení všech komponentů na síti.

5.5 Vizualizace

Vizualizace je grafické uživatelské prostředí, které umožnuje operátorovi monitorovat a ovládat rozsáhlé strojí zařízení z jednoho místa pomocí dotykového panelu nebo PC. Jedná se tedy o počítačový program, který co nejvěrohodněji simuluje všechny důležité dění na stroji. Díky tomu obsluha vidí, jak stroj pracuje z jednoho místa (třeba i z kanceláře) a nemusí u něj být přítomna.

5.5.1 FactoryTalk View Studion ME

Nástroj FactoryTalk View Studio ME [26] je program od firmy Rockwell Automation určený k vytváření vizualizace. Je to grafický editor, který navíc umožnuje vkládání jednoduchých funkcí a tagů. Hlavní okno (Obrázek 5.14) se skládá z několik základních částí. V horní oblasti (zeleně) jsou programátorovi k dispozici nejrůznější objekty, které může vložit do vizualizační obrazovky. Vlevo (červeně) se nachází panel se strukturou projekt a jeho nastavením. Pracovní plocha je označena černě. Zde se ve vyhrazeném prostoru vytváří výsledný vzhled a funkce vizualizace.

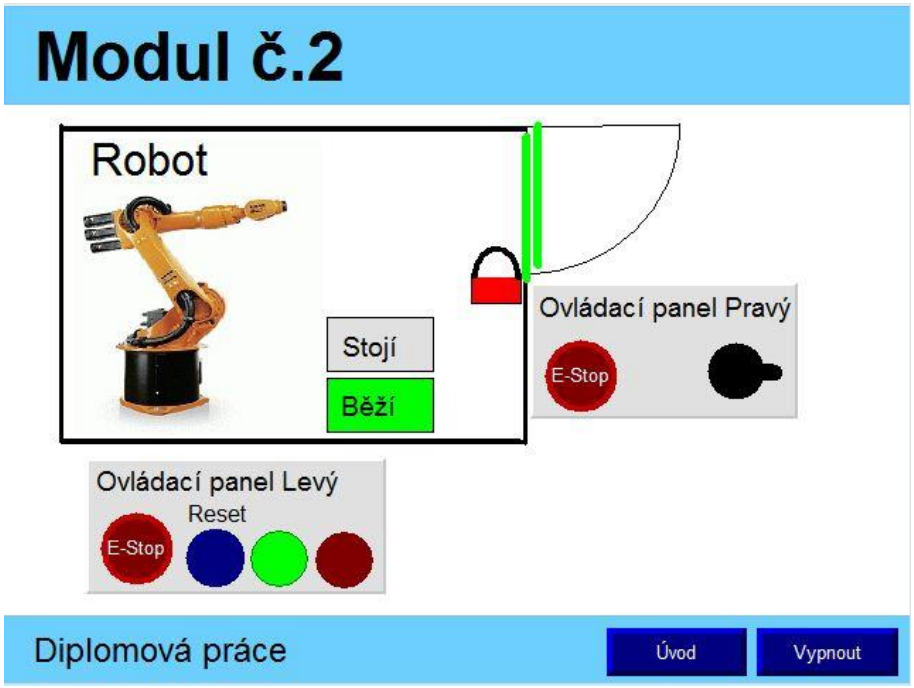


Obrázek 5.14: Hlavní okno FactoryTalk View Studio ME

5.5.2 Tvorba vizualizace

V programu FactoryTalk View Studio ME byl vytvořen projekt s rozlišením obrazovky 640x480 bodů. V záložce *Graphics/Displays* byly vytvořeny dvě okna. Obrazovka *MAIN* je úvodní obrazovkou vizualizace a má dvě ovládací tlačítka a to *Vypnout* pro ukončení vizualizace a *Bezpečnost* pro otevření okna s vizualizací bezpečnosti stroje. Úvodní obrazovka je na obrázku 5.14.

Monitorování bezpečnostních funkcí stroje zobrazuje obrazovka *Bezpečnost* (Obrázek 5.15). Byly zde vytvořeny dvě tlačítka – *Vypnout* pro ukončení a *Úvod*, pomocí kterého se zobrazí úvodní obrazovka. Dále zde byl umístěn obrázek virtuálního stroje – robotického ramene a k němu náležící indikace jeho stavu (Stojí nebo běží). Kolem celého ramene je umístěno oplocení (černě) a jedny dveře se dvěma senzory jejich polohy (zeleně). U dveří je také zobrazen stav zámku. Ve vizualizaci jsou vytvořeny dva ovládací panely, které jsou umístěny i na panelu č. 2. Ve vizualizaci jsou fyzická tlačítka nahrazena kontrolkami, které zobrazují stav tlačítek na panelu. V projektu byly ještě jednotlivým objektům přiřazeny animace, které jsou popsány dále.



Obrázek 5.15: Obrazovka vizualizace *Bezpečnost*

5.5.3 Nastavení komunikace

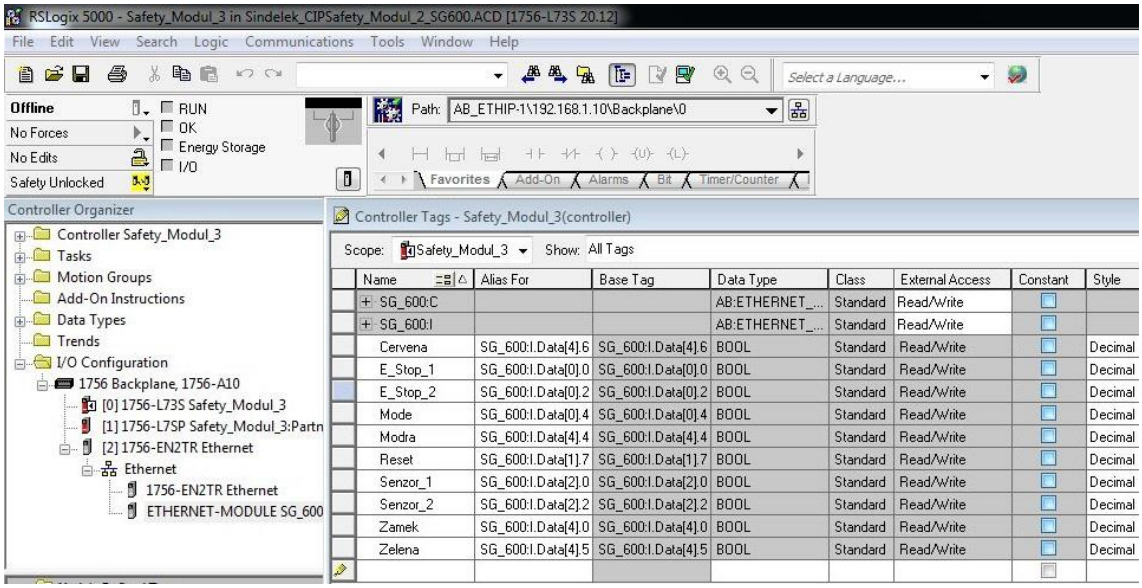
Podstatnou částí projektu ve vizualizaci je nastavení spojení mezi sledovaným PLC automatem a projektem ve FactoryTalk View Studio. Přímou komunikaci bohužel nelze zprostředkovat, a proto bylo nutné použít PLC ControlLogix 1756 jako přenašeč informací. Blokové schéma komunikace je zobrazeno na obrázku 5.16.

Obrázek 5.16: Blokové schéma komunikace mezi vizualizací a SG 600

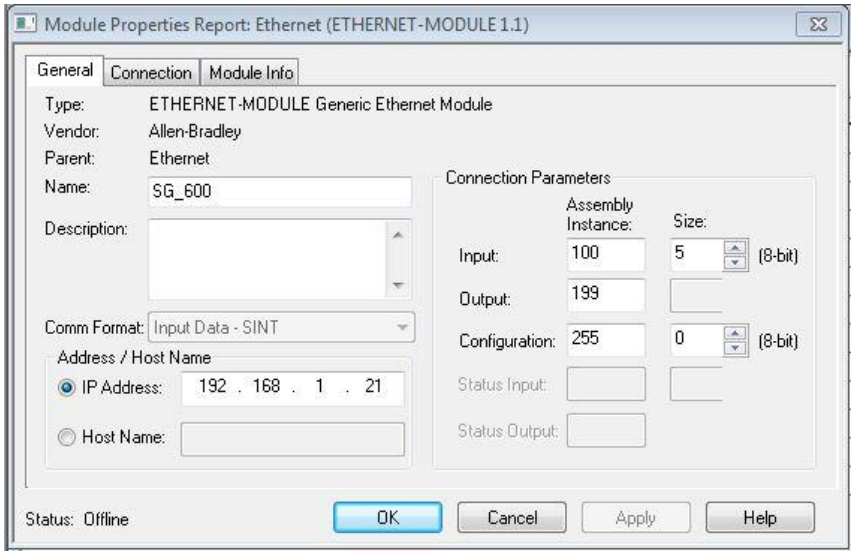
V první kroku byla vytvořena komunikace mezi SG 600 a ControlLogix 1756. Nastavení sítě na straně SG 600 již bylo provedeno v kapitole 5.4.4. Zbývá vytvořit základní programové vybavení PLC ControlLogix 1756.

Komunikace mezi PLC ControlLogix 1756 a PLC SG 600

Ve vývojovém prostředí RSLogix5000 (Obrázek 5.17) byl vytvořen projekt s procesorovou jednotkou 1756-L73S. Poté bylo nutné doplnit hardwarovou konfiguraci PLC sestavy. Ta je zobrazena v levém sloupci hlavního okna v záložce *I/O configuration.* Nejprve se přidá ethernetový modu PLC sestavy kliknutím na *1756 Backplane, 1756-A10* a volbou *New Module...* Ze seznamu byl vybrán ethernetový modul *1756-EN2TR* a byla mu nastavena IP adresa 192.168.1.10. V dalším kroku bylo nutné přidat spojení mezi ethernetovým modulem sestavy ControlLogix a PLC SG 600. Tento úkon se provede kliknutím na modul *1756-EN2TR* a volbou *New Module....* Ze seznamu byl vybrán modul *ETHERNET-MODULES*, který bylo nutné nastavit podle obrázku 5.18.



Obrázek 5.17: Hlavní okno RSLogix 5000

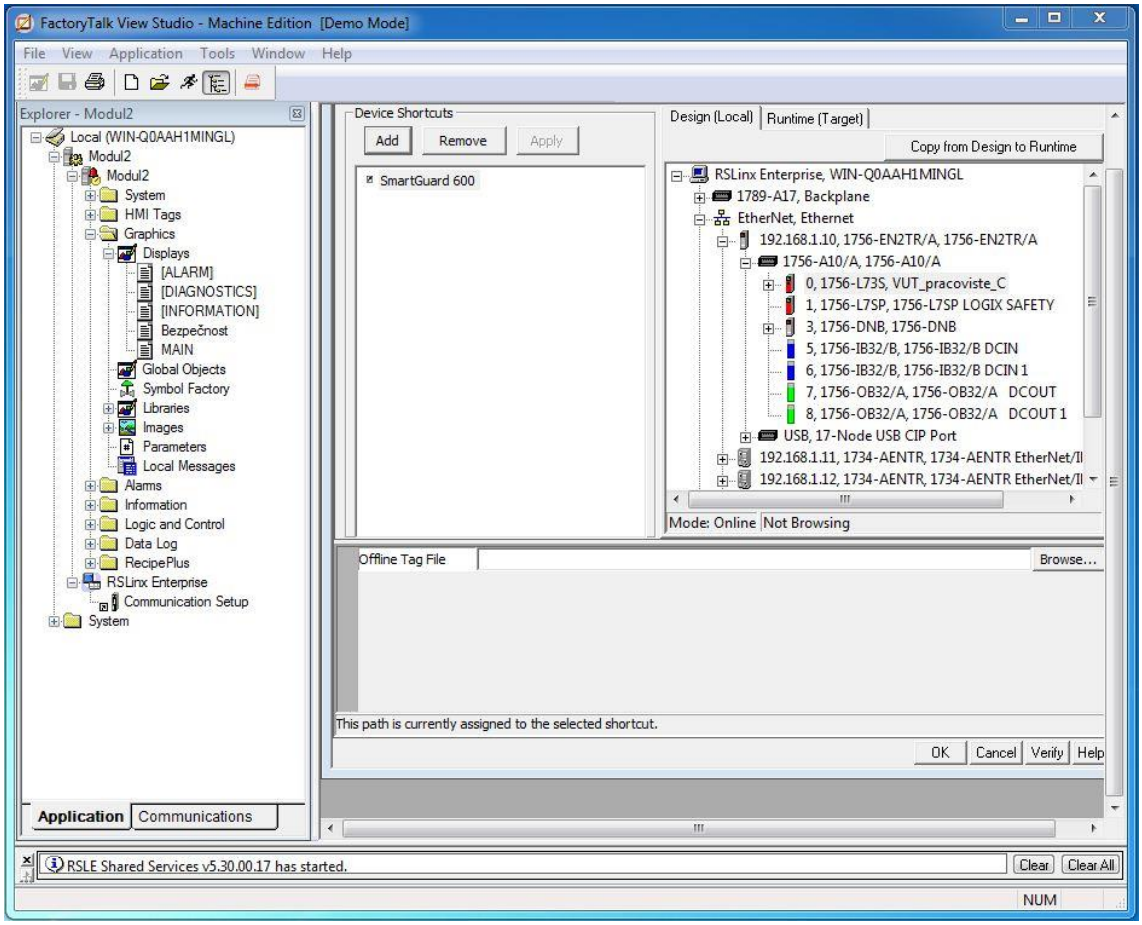


Obrázek 5.18: Nastavení ethernetového modulu pro SG 600

V této fázi je již nastavena komunikace mezi ControlLogix 1756 a PLC SG 600. V tabulce Controller Tags (Obrázek 5.17) jsou vidět dvě datové struktury (SG_600:C a SG 600:I), které obsahují přijímaná data z SG 600. Dále jsou v tabulce vytvořeny lokální bitové proměnné, kterým jsou přiřazeny aliasy z datové struktury SG 600:I. Vytvoření těchto proměnných nebylo nutné, ale ulehčuje to výslednou práci s daty. Posledním krokem v nástroji RSLogix 5000 je download projektu do PLC automatu ControlLogix 1756 a přepnutí do režimu RUN. Report projektu programu pro PLC ControlLogix 1756 je součástí přiloženého CD.

Komunikace mezi vizualizací a PLC ControlLogix 1756

Tento odstavec popisuje postup nastavení komunikačního propojení mezi tagy v PLC ControlLogix 1756 a vizualizací. Nastavení se provádí na straně vizualizace, u které se nastaví cesta k proměnným v PLC. V programu FactoryTalk View Studio v levém menu *Explorer* je záložka *RSLinx Enterprise / Communicarion Setup*. Dvojitým kliknutím na ni se otevře okno (Obrázek 5.19) s nastavením cesty ze síťové karty PC k PLC automatu. Nejprve bylo přidáno nové zařízení kliknutím na políčko *Add* a pojmenováním SmartGuard 600. Poté se v záložce *Desing (Local)* zvolila cesta k PLC. V předposledním kroku bylo vybrána položka *0,1756-L73S, VUT_pracoviste_C* a zvolí se *Copy from Desing to Runtime*. Posledním krokem je kliknutí na políčko *Verify* a poté OK.

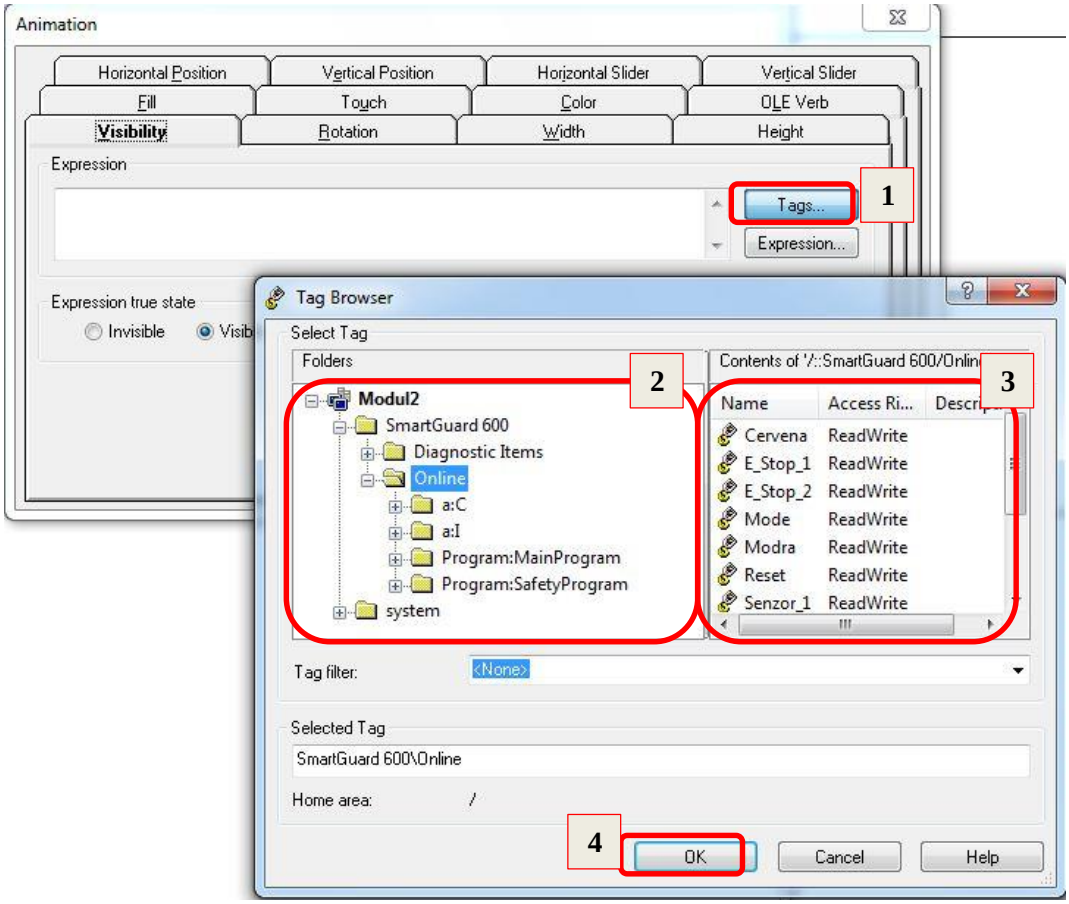


Obrázek 5.19: Nastavení komunikační cesty mezi vizualizací a ControlLogix 1756

K tagům se poté přistupuje přidáním animace k zvolenému prvku ve vizualizaci (kliknutím pravým tlačítkem na prvek a zvolení *Animation*). Otevře se okno *Animation*, kde se u zvolené animace klikne na *Tags*, nastaví se cesta k online tagům, následně se vybere ovládací proměnná a potvrdí se *OK*. Okna s nastavení jsou zobrazena na obrázku 5.20. Seznam použitých tagů ve vizualizaci je v tabulce 5.7.

Tabulka 5.7: Seznam tagů použitých ve vizualizaci

Name	Alias	Comment
E_Stop_1	SG_600:I.Data[0].0	E-Stop tlačítko 1
E_Stop_2	SG_600:I.Data[0].2	E-Stop tlačítko 2
Senzor_1	SG_600:I.Data[2].0	Magnetický senzor SensaGuard 1
Senzor_2	SG_600:I.Data[2].2	Magnetický senzor SensaGuard 2
Mode	SG_600:I.Data[0].4	Pčepínač módů běh a servis
Reset	SG_600:I.Data[1].7	Resetovací modré tlačítko
Zamek	SG_600:I.Data[4].0	Elektronický zámek 400G-MT
Modra	SG_600:I.Data[4].4	Modrá kontrolka
Zelena	SG_600:I.Data[4].5	Zelená kontrolka
Cervena	SG_600:I.Data[4].6	Červená kontrolka



Obrázek 5.20: Přiřazení tagu k animaci prvku vizualizace

6 ZÁVĚR

Diplomová práce je zaměřena na posouzení a snížení rizika stroje. Hlavní úkolem bylo návrh a realizace dvou demonstračních bezpečnostních laboratorních úloh s použitím CIP Safety technologii. K realizaci dvou úloh byly použity dva panely, vyrobené firmou EK-Industry. Pro osazení panelů bylo použito bezpečnostních komponentů od firmy Rockwell Automation. Panely demonstrují pouze bezpečnostní část stroje.

Diplomovou prací jsou řešeny dvě bezpečnostní laboratorní úlohy. Každá úloha je tvořena kapitolou popisující panel s bezpečnostní instrumentací, kapitolou posouzení rizik a ověření dosažené úrovně bezpečnosti. Dále je zde uveden popis návrhu a realizace bezpečnostních funkcí, konfigurace zařízení a vizualizace procesu.

První část této práce popisuje normy, kterými je nutné se řídit při návrhu zabezpečení stroje. Použití těchto norem nařizuje legislativa České republiky.

V druhé kapitole jsou popsány nástroje Safety Automation Builder a SISTEMA, které konstruktérům usnadňují návrh bezpečnostních prvků stroje a jejich použití garantuje správnost návrhu dle norem.

Použité bezpečnostní komponenty komunikují pomocí bezpečnostního protokolu CIP Safety po síti DeviceNet. Třetí kapitola popisuje základní princip protokolu CIP a jeho bezpečnostní nástavbu CIP Safety.

První demonstrační úloha je zaměřena na aplikaci s pohybem. Jelikož neobsahuje reálný stroj, ale pouze třífázový motor se dvěma enkodéry, který jej simuluje a nahrazuje navržený virtuální stroj (kolotoč). Na tomto stroji bylo dle normy ČSN EN ISO 14121 provedeno posouzení rizika a dle normy ČSN EN ISO 13849-1 stanovena požadovaná úroveň vlastností (PLr) d. Nalezená rizika byla minimalizována postupem dle normy ČSN EN ISO 12100. Kolem kolotoče byl instalováno ochranné oplocení, na dveře byl nainstalován elektronický zámek 400G-MT a snímače SensaGuard, na podlahu kolem kolotoče byla položena bezpečnostní rohož SafetyMat. Bezpečný (klidový) stav stroje je zajištěn odpojením motoru od energie dvěma redundantními stykači 100S-C. Klidový stav motoru je monitorován dvěma enkodéry a bezpečnostním relé MSR57P.

Návrh těchto bezpečnostních opatření a ověření dosažené PL bylo provedeno nástroji Safety Automation Builder a SISTEMA s žádaným výsledkem PLd. Navržené bezpečnostní funkce byly realizovány a odzkoušeny na laboratorním panelu č. 1.

Druhá demonstrační úloha je zaměřena na použití bezpečnostních komponentů komunikujících pomocí protokolu CIP Safety po síti DeviceNet. Bezpečnostní vybavení bylo navrženo k zabezpečení virtuálního robotického ramene. Jako v demonstrační úloze č. 1, i zde bylo provedeno posouzení rizik robotického ramene. Po určení mezních hodnot, identifikaci úloh a nebezpečí a odhadu rizika byla stanovena minimální PLr úrovně d. Z důvodů snížení rizika byly navrženy následující bezpečnostní opatření: Oplocení kolem celého stroje do výšky 2 m, použití magnetických senzorů SensaGuard a elektronického zámku 400G-MT na přístupové dveře a použití dvou E-Stop tlačítek. K návrhu těchto

opatření bylo provedeno v nástroji Safety Automation Builder a zhodnocení dosažené bezpečnostní úrovně s výsledkem d bylo provedeno nástrojem SISTEMA. Navržené bezpečnostní funkce slouží k zabezpečení stroje pouze v režimu chod, pro režim servis by robotické rameno muselo být odpojitelné od energie např. pomocí dvou stykačů 100S-C. Toto zabezpečení ale nebylo úkolem práce a proto je stav stroje simulován kontrolkami zelenou (chod) a červenou (stop).

K ovládání bezpečnostních funkcí je použit PLC automat SmarGuard 600 se vzdálenou bezpečnostní I/O periferii se kterou komunikuje přes sít DeviceNet. Použití těchto bezpečnostních komponentů umožnuje vytvoření vizualizace laboratorní úlohy.

V poslední části této laboratorní práce byla vytvořena vizualizace druhé laboratorní úlohy. Úkolem bylo monitorování bezpečnostních funkcí probíhajících na stroji (na panelu č. 2). Vizualizace se skládá ze dvou oken. Obrazovka *MAIN* je úvodní obrazovkou vizualizace a má dvě ovládací tlačítka a to *Vypnout* pro ukončení vizualizace a *Bezpečnost* pro otevření okna s vizualizací bezpečnosti stroje. Monitorování bezpečnostních funkcí stroje zobrazuje obrazovka *Bezpečnost,* do které byl vložen půdorys stroje s navrženými bezpečnostními částmi. Stavy tlačítek jsou zde indikovány příslušnými kontrolkami a stav zámku a dveří je graficky rozlišen. Dále bylo vytvořeno propojení PLC SG 600 před síť EtherNet s vizualizaci v PC pomocí automatu ControlLogix 1756. Vizualizace názorně zobrazuje dění na panelu č. 2.

Po dohodě s vedoucím práce nebyla druhá vizualizace realizována, protože použité logické zařízení v první laboratorní úloze neumožnuje přímé monitorování bezpečnostních funkcí.

Výsledkem diplomové práce jsou dvě realizované a plně funkční demonstrační úlohy. V první představuje požadavky na zabezpečení pohybujících se součástí, druhá úloha demonstruje použití bezpečnostního PLC SG 600, bezpečnostních I/O modulů POINT Guard a komunikace pomocí protokolu CIP Safety po síti DeviceNet. K druhé úloze byla vytvořena i vizualizace zobrazující reálné dění na panelu č. 2.

Literatura

[1] Safebook 4. *Rockwell Automation* [online]. 2011 [cit. 2015-11-02]. Dostupné z: http://marketing.rockwellautomation.com/safety/cs/safebook4_Form

[2] *Bezpečnostní příručka pro strojní zařízení*. 1. Praha: Schneider Electronic cz, 2010.

[3] STIBOR, Karel. *Bezpečnost v moderním průmyslu* [online]. Brno: VUT v Brně, 2010. 35 s. [cit. 2015-11-02], Dostupné z: http://www.crr.vutbr.cz/system/files/brozura_07_1010.pdf

[4] Safety Automation Builder. Rockwell Automation, Inc. *Rockwell Automation* [online]. 2015 [cit. 2016-04-12]. Dostupné z: http://www.marketing.rockwellautomation.com/safety-solutions/cs/MachineSafety/ToolsAndDownloads/Safety_Automation_Builder/

[5] SISTEMA. Rockwell Automation, Inc. *Rockwell Automation* [online]. 2015 [cit. 2016-04-12]. Dostupné z: http://www.marketing.rockwellautomation.com/safety-solutions/cs/MachineSafety/ToolsAndDownloads/sistema_download

[6] ZEZULKA, František a Ondřej HYNČICA *Průmyslový Ethernet IX: EtherNet/IP, EtherCAT*. *AUTOMA* [online]. 2008, č. 10 [cit. 2016-05-1]. Dostupné z : http://www.odbornecasopisy.cz/res/pdf/37910.pdf

[7] About ODVA. *ODVA* [online]. 2015 [cit. 2016-05-1]. Dostupné z: https://www.odva.org/About-ODVA

[8] CIP Safety: Safety networking for today and beyond. *ODVA* [online]. 2010 [cit. 2016-05-1]. Dostupné z: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00110R2_DeviceNet_Safety_White_Paper.pdf

[9] *Motor 2IK6A-SW2m* [online]. India: Oriental motor, 2016 [cit. 2016-04-30]. Dostupné z: http://www.orientalmotor.co.in/products/ac/list/detail/?product_name=2IK6A-SW2M&brand_tbl_code=AC&series_code=802&type_code=

[10] *Encoders Bulletin 844A* [online].Allen-Bradley, 2014 [cit. 2016-04-30]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/ca/c116-ca506_-en-p.pdf

[11] *LM2576* [online]. Texas: Texas Instruments, 1999 [cit. 2016-04-30]. Dostupné z: http://www.ti.com/lit/ds/symlink/lm2576.pdf

[12] MSR57P. *Rockwell Automation* , [online]. [cit. 2016-05-1]. Dostupné z : http://50.18.122.28/en/3377539/5866177/5985760/4444281/4444297/7833407/7833409/2e19e308b0cb950bd50bf86b20ee2a70/Safety.pdf

[13] PowerFlex 7-Class Options. Rockwell Automation, Inc. *Rockwell Automation* [online]. 2015 [cit.2016-05-08]. Dostupné z: http://www.ab.com/en/epub/catalogs/36265/1323285/9613107/Accessories.html

[14] MSR210P. *Rockwell Automation* , [online]. [cit. 2016-05-08]. Dostupné z : http://50.18.122.28/en/3377539/5866177/5985760/4444281/4444307/4444662/b633e53f8870d6a96248e65ebedcc911/Safety.pdf

[15] MSR220P. *Rockwell Automation* [online]. Germany: Rockwell Automation, 2011 [cit. 2016-05-08]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/in/440r-in067_-mu-p.pdf

[16] *Logic* [online]. The USA: Rockwell Automation, 2016 [cit. 2016-04-30]. Dostupné z: http://www.ab.com/en/epub/catalogs/3377539/5866177/5985760/Logic.html

[17] *Guardmaster® Safety Relays (GSR) DI* [online]. the U.S.A.: Rockwell Automation, 2016 [cit. 2016-04-30]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/440r-um013_-en-p.pdf

[18] *440G-MT* [online]. The USA: Rockwell Automation, 2015 [cit. 2016-04-30]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/in/440g-in001_-en-p.pdf

[19] *SensaGuard Non-contact Interlock Switches* [online]. The USA: Rockwell Automation, 2016 [cit. 2016-04-30]. Dostupné z: http://ab.rockwellautomation.com/Sensors-Switches/Safety-Interlock-Switches/SensaGuard-Non-Contact-Interlock-Switches

[20] SmartGuard 600. *Rockwell Automation* , [online]. [cit. 2016-05-09]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1752-um001_-en-p.pdf

[21] POINT I/O DeviceNet Communication Interface Module. *Rockwell Automation* , [online]. [cit. 2016-05-09]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1734-in057_-en-e.pdf

[22] POINT Guard I/O Safety Modules. *Rockwell Automation* [online]. 2015 [cit. 2016-05-11]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1734-um013_-en-p.pdf

[23] Plastikářský průmysl. *Kuka* [online]. 2016 [cit.2016-05-10]. Dostupné z: http://www.kuka-robotics.com/czech_republic/cs/solutions/branches/plastics/start.htm?WBCMODE=PresentationUnpublished

[24] RSLinx® Classic Getting Results Guide. *Rockwell Automation* [online]. 2015 [cit. 2016-05-11]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/gr/linx-gr001_-en-e.pdf

[25] RSNetWorx for DeviceNet. *Rockwell Automation* [online]. 2015 [cit. 2016-05-11]. Dostupné z: http://literature.rockwellautomation.com/idc/groups/literature/documents/gr/dnet-gr001_-en-e.pdf

[26] FACTORYTALK VIEW ME. *Rockwell Automation* [online]. 2016 [cit. 2016-05-12]. Dostupné z: http://www.rockwellautomation.com/rockwellsoftware/products/factorytalk-view-me.page

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

SRP/CS – bezpečnostní část ovládacích systémů (Safety Related Part of Control Systém)

DC – diagnostické pokrytí (Diagnostic Coverage)

MTTFd – střední doba mezi dvěma nebezpečnými poruchami (Mean Time To Failure)

PFHd – pravděpodobnost nebezpečného selhání za hodinu (Probability of Dangerous Failure per Hour)

PL – úroveň vlastností (Performance Level)

PLC – programovatelný logický automat (Programmable Logic Controller)

N.C. – rozepínatelný kontakt (Normally Closed)

N.O. – spínací kontakt (Normally Open)

OSSD – signál výstupního výstupního prvku (Output Signal Switching Devices)

EDS – elektronický popis zařízení (Electronic Device Sheet)

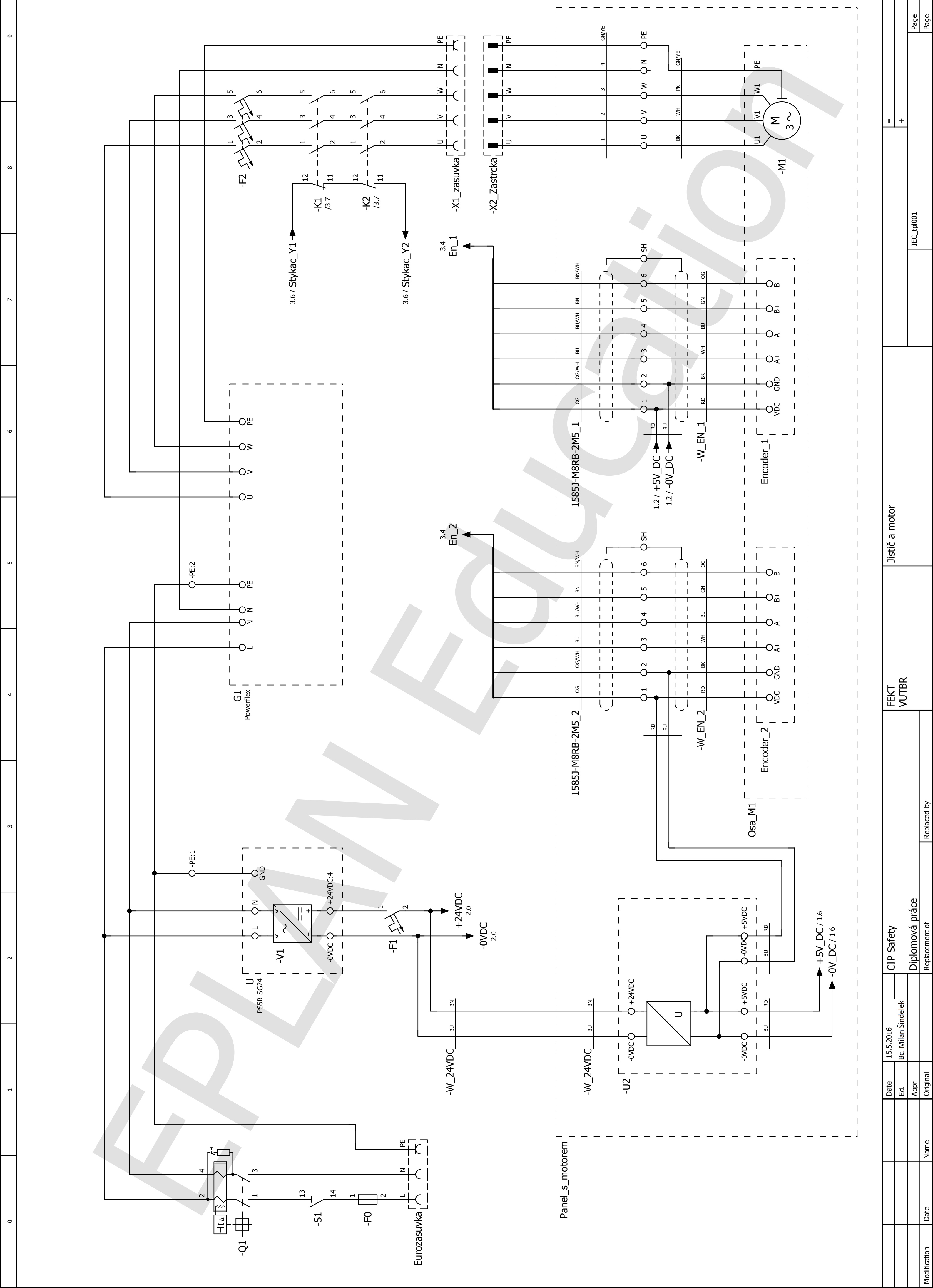
I/O – vstupně /výstupní (Input/Output)

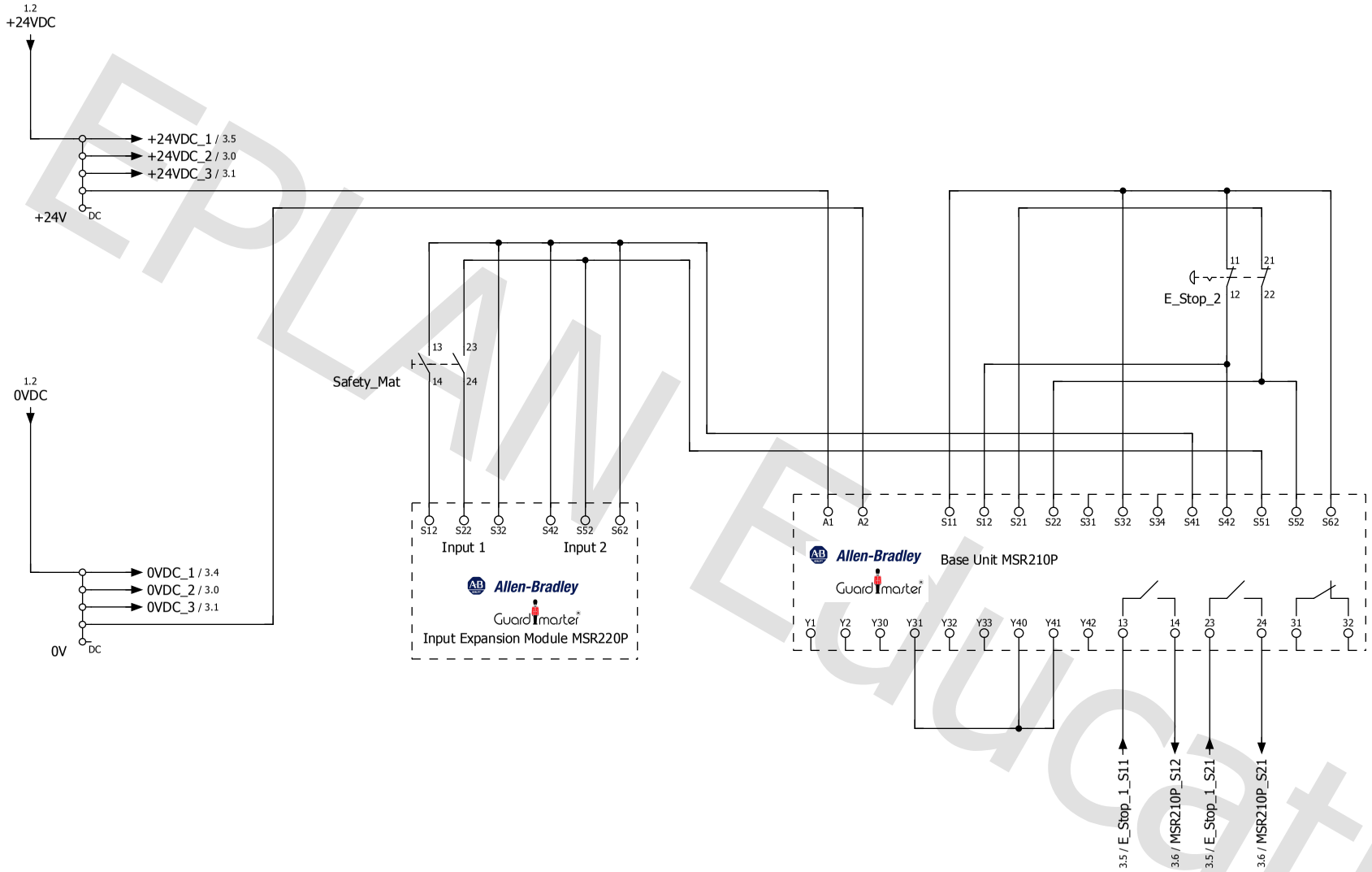
CIP – běžný průmyslový protokol (Common Industrial Protocol)

SG 600 – SmartGuard 600

SEZNAM PŘÍLOH

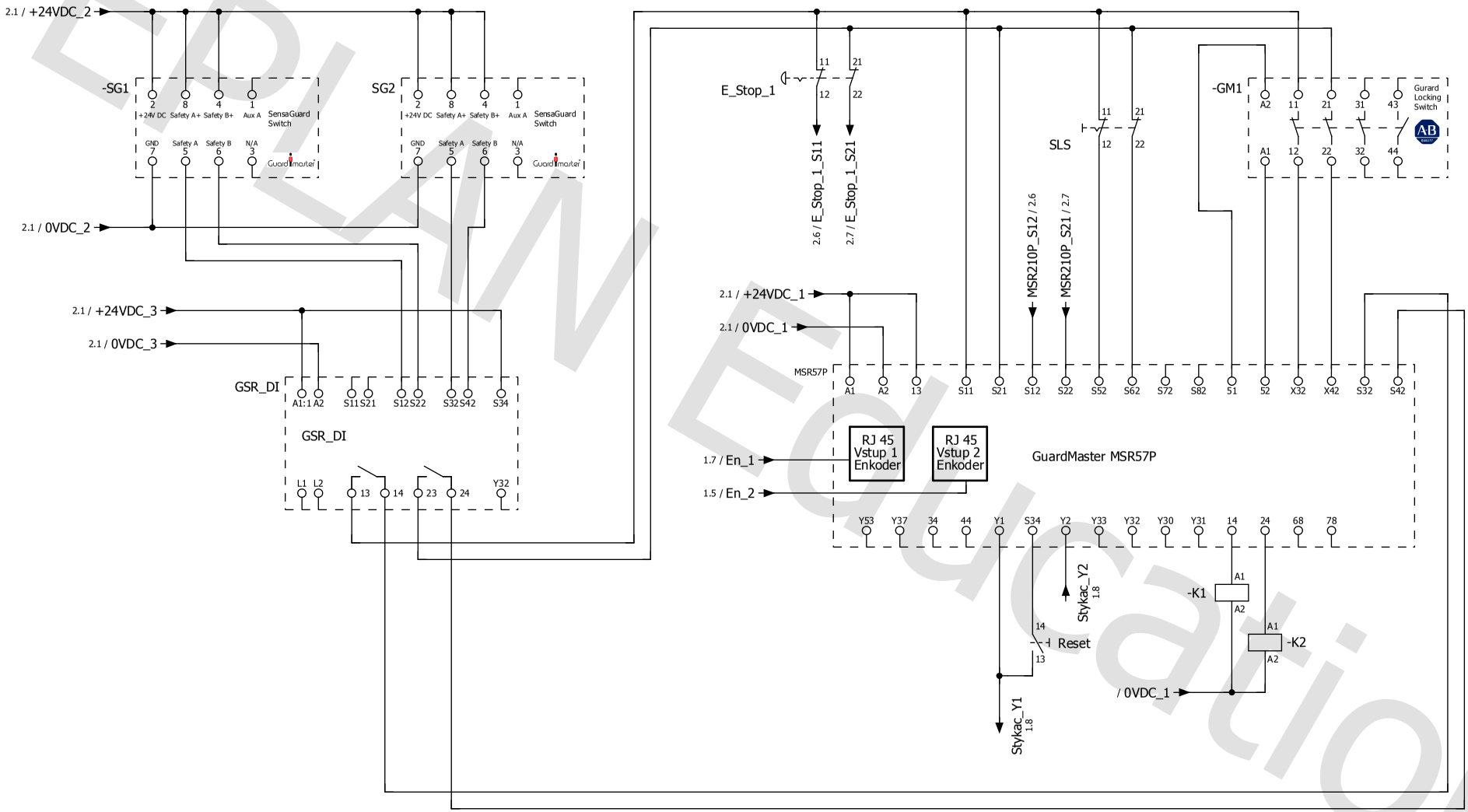
Příloha 1: Schéma zapojení elektroinstalace panelu č. 1





1 3

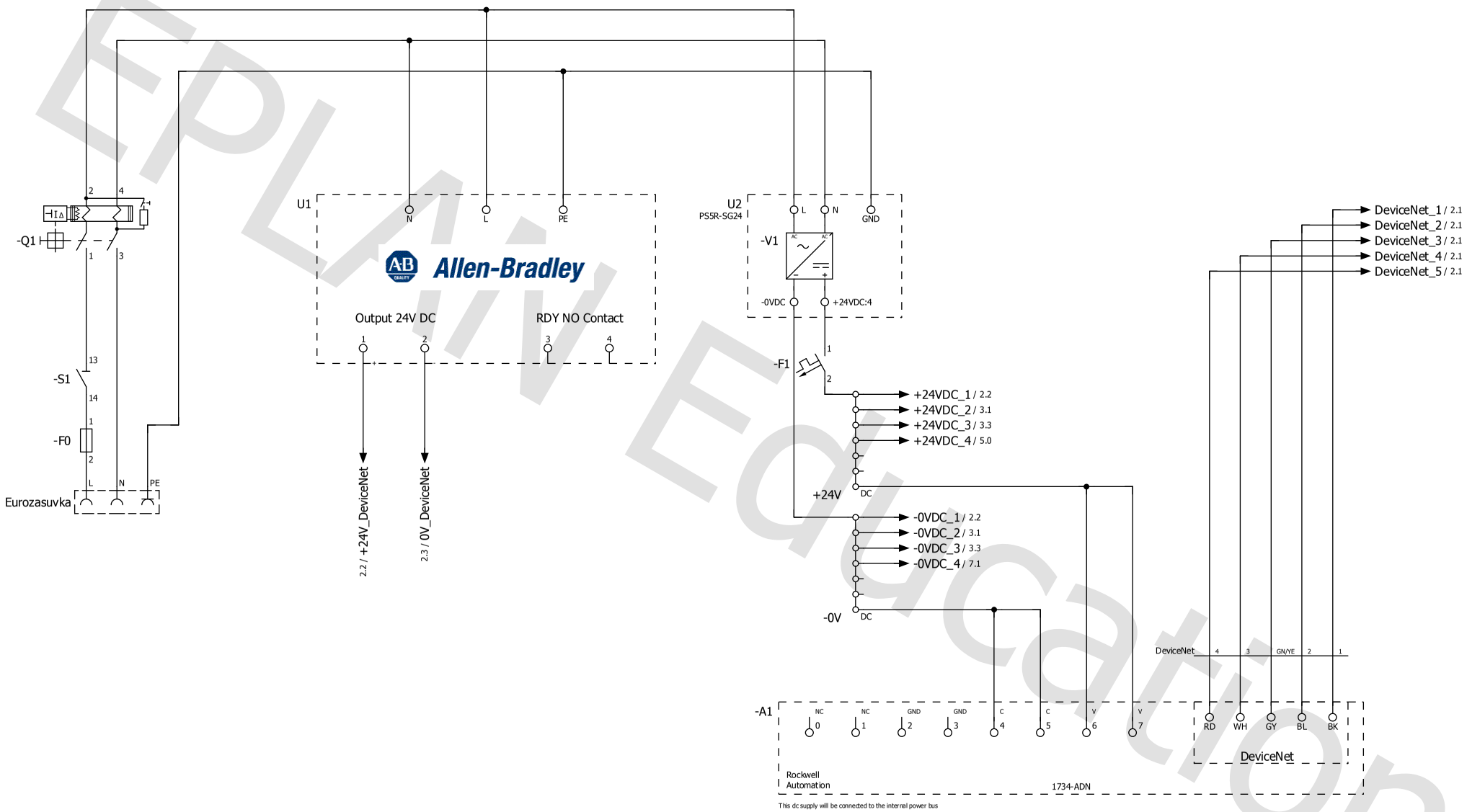
			Date	14.5.2016	CIP Safety	FEKT VUTBR	Logika MSR200	=	
			Ed.	Bc. Milan Šindelek				+	
			Appr		Diplomová práce			IEC_tpl001	Page 2
Modification	Date	Name	Original		Replacement of	Replaced by			Page 3



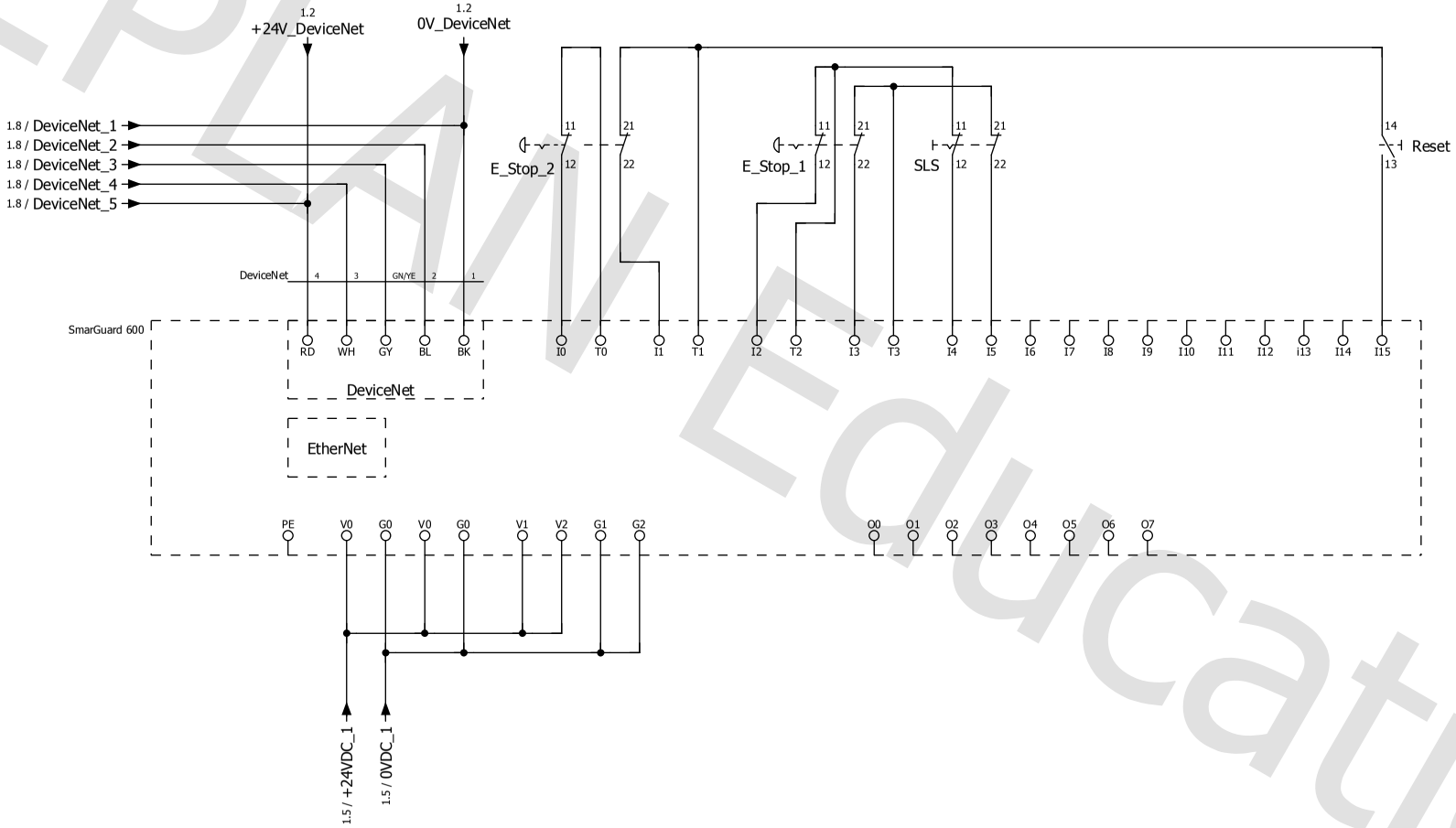
2

			Date	14.5.2016	CIP Safety	FEKT VUTBR	Logika MSR57P		=
			Ed.	Bc. Milan Šindelek					+
			Appr		Diplomová práce			IEC_tpl001	Page 3
Modification	Date	Name	Original		Replacement of	Replaced by			Page 3

Příloha 2: Schéma zapojení elektroinstalace panelu č. 2

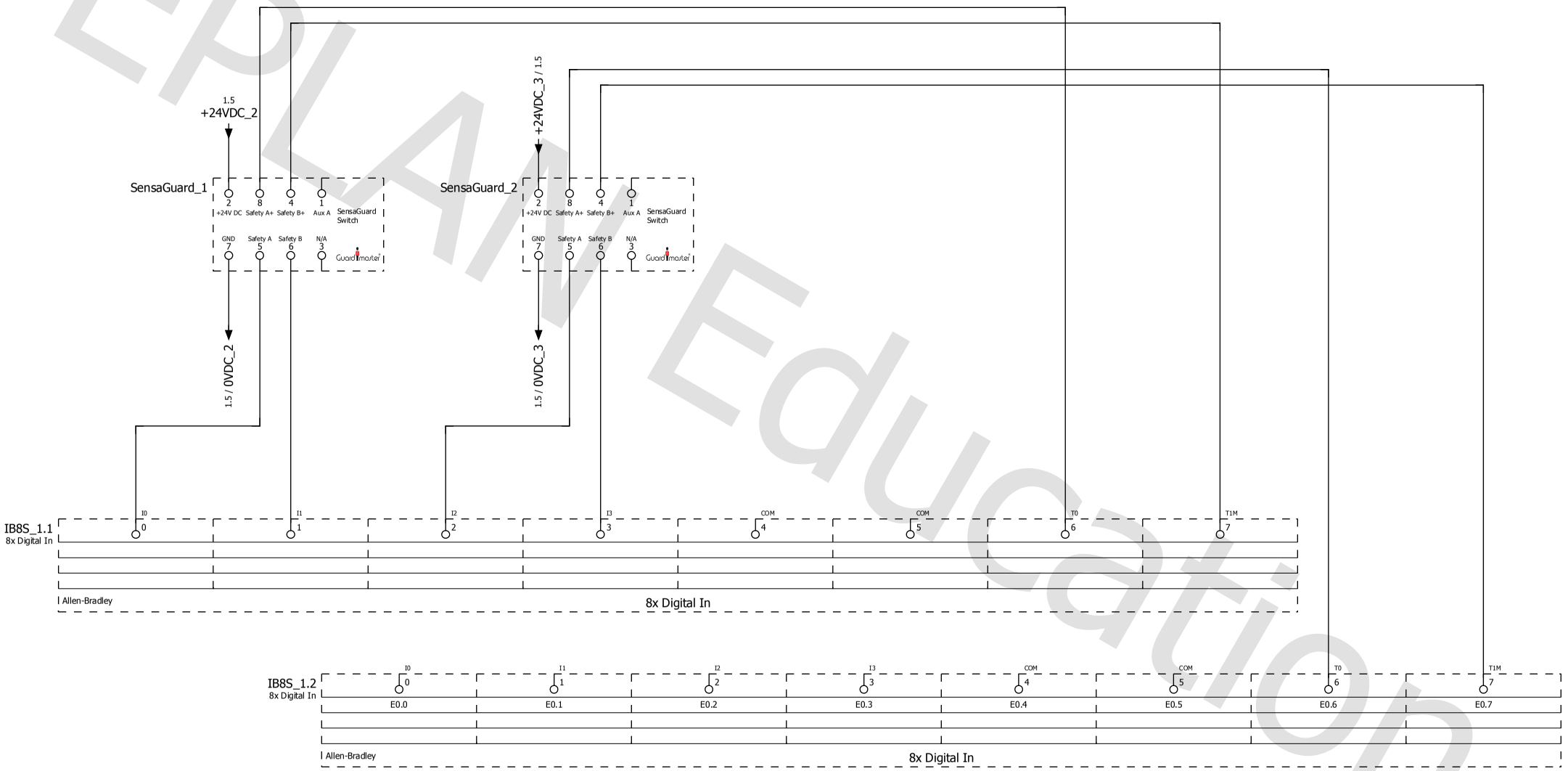


			Date	15.5.2016	Modul č. 2	FEKT VUTBR	Jistič		=
			Ed.	Bc. Milan Šindelek					+
			Appr		Diplomová práce - CIP Safety				
Modification	Date	Name	Original		Replacement of	Replaced by			Page 1 / Page 7



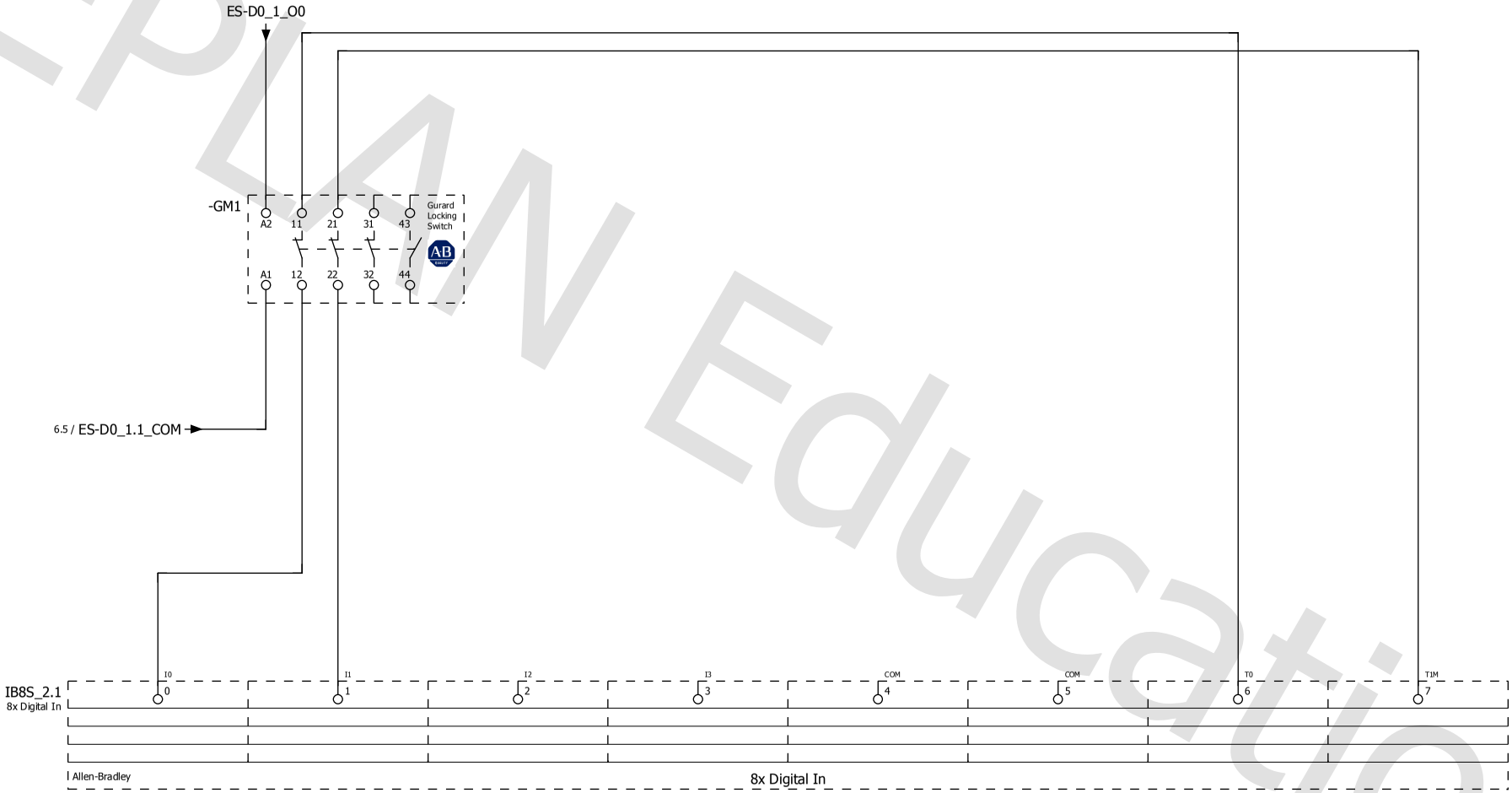
1 3

			Date	15.5.2016	Modul č. 2	FEKT VUTBR	Logika SmarGuard 600		=
			Ed.	Bc. Milan Šindelek					+
			Appr		Diplomová práce - CIP Safety				Page 2
Modification	Date	Name	Original		Replacement of	Replaced by			Page 7



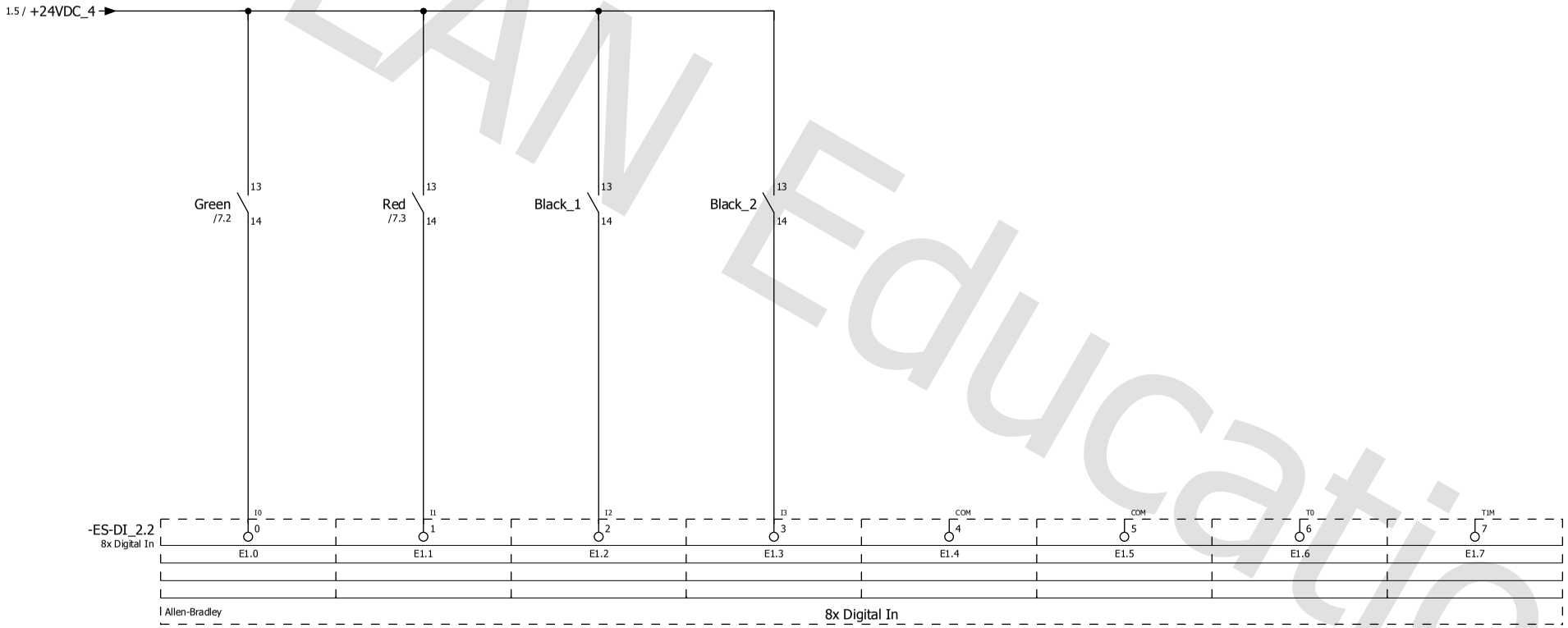
2 4

			Date	15.5.2016	Modul č. 2	FEKT VUTBR	IB8S_1		=
			Ed.	Bc. Milan Šindelek					+
			Appr		Diplomová práce - CIP Safety				Page 3
Modification	Date	Name	Original		Replacement of	Replaced by			Page 7



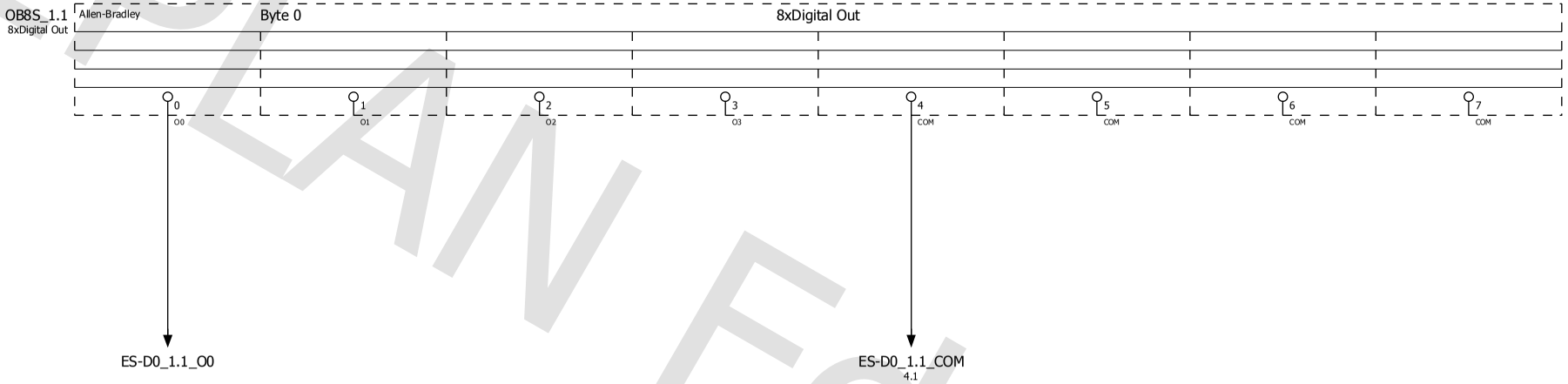
3 5

			Date	14.5.2016	Modul č. 2		FEKT VUTBR	IB8S_2.1		=
			Ed.	Bc. Milan Šindelek						+
			Appr		Diplomová práce - CIP Safety					Page 4
Modification	Date	Name	Original		Replacement of	Replaced by				Page 7

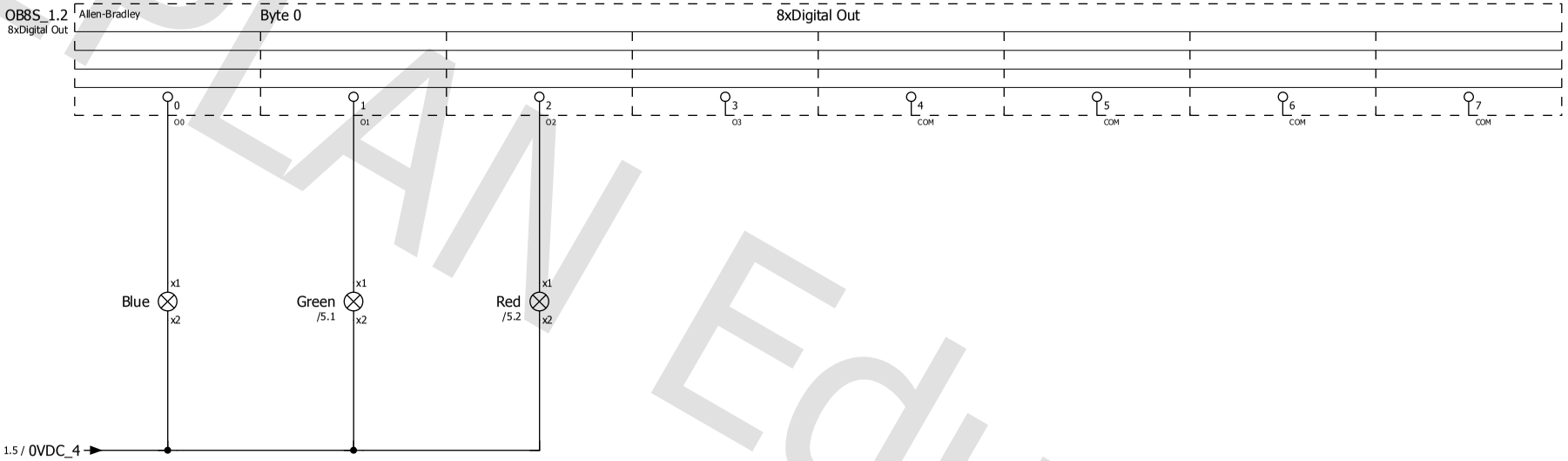


4 6

			Date	15.5.2016	Modul č. 2	FEKT VUTBR	IB8S_2.2		=	
			Ed.	Bc. Milan Šindelek					+	
			Appr		Diplomová práce - CIP Safety					Page 5
Modification	Date	Name	Original		Replacement of	Replaced by				Page 7

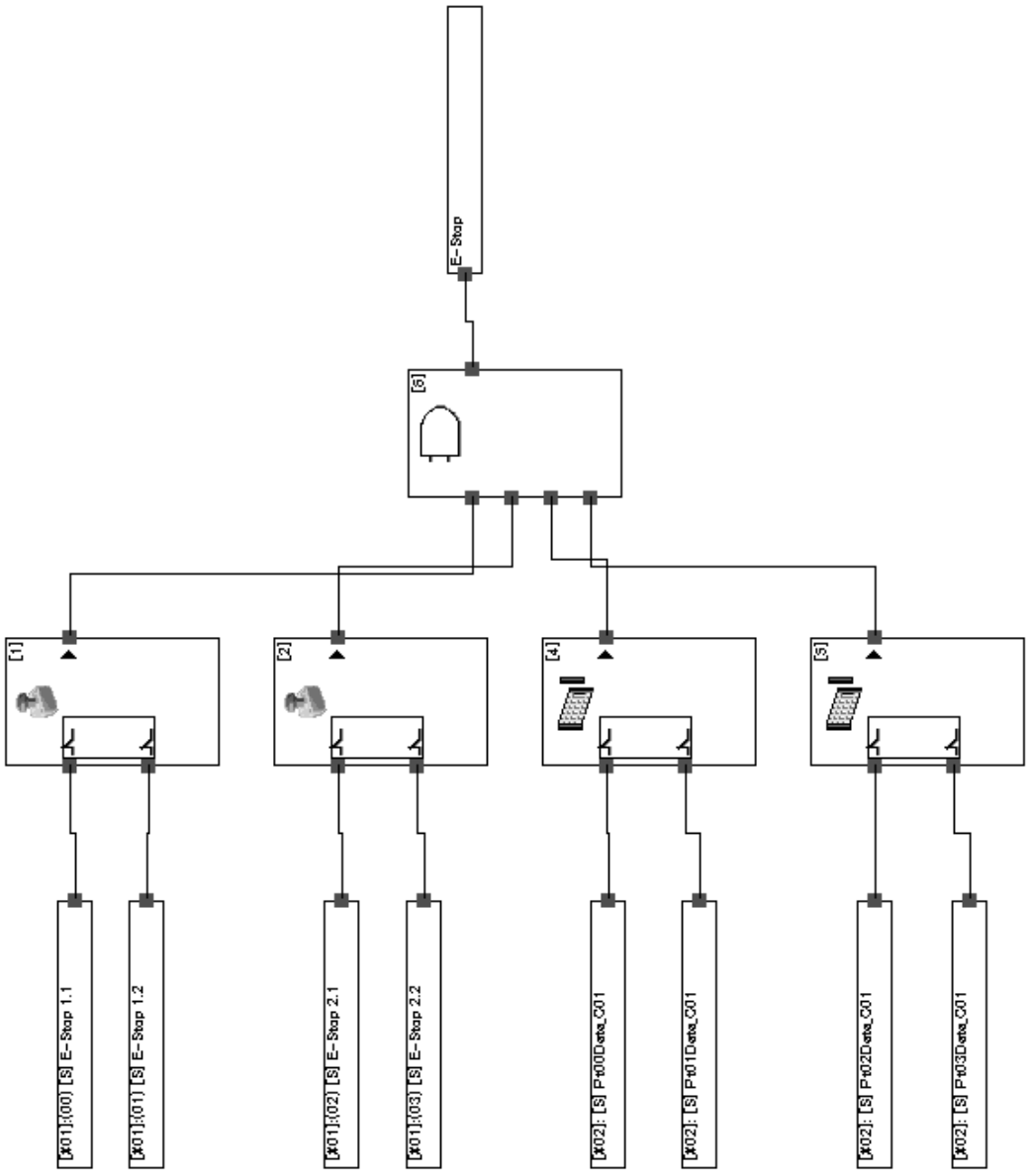


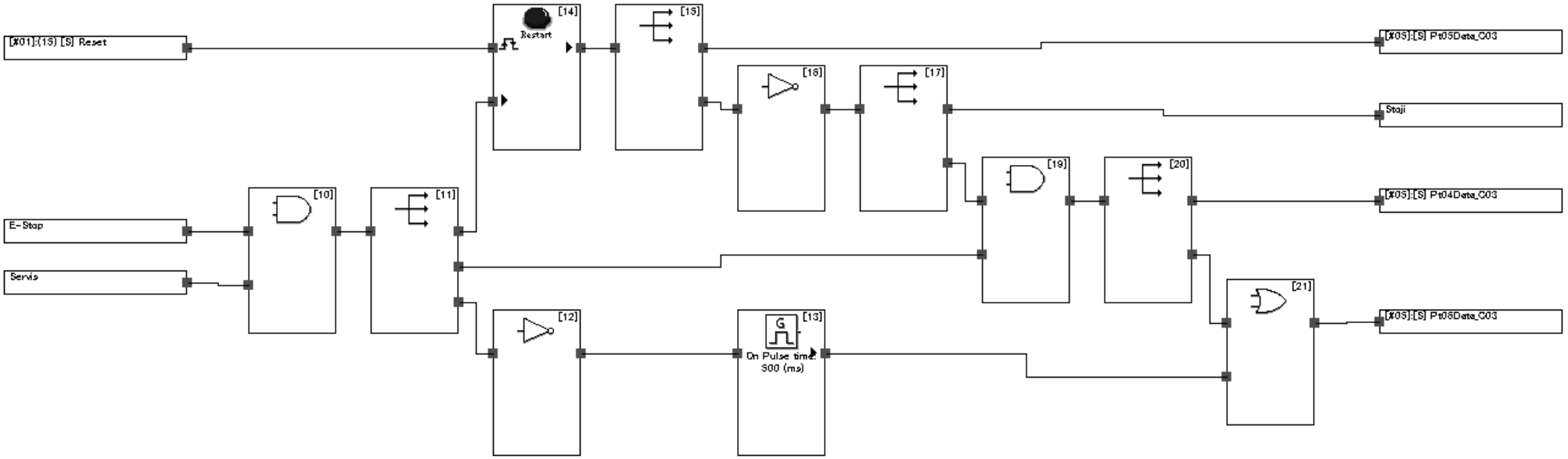
			Date	14.5.2016	Modul č. 2	FEKT VUTBR	OB8S_1.1		=	
			Ed.	Bc. Milan Šindelek					+	
			Appr		Diplomová práce - CIP Safety					Page 6
Modification	Date	Name	Original		Replacement of	Replaced by				Page 7

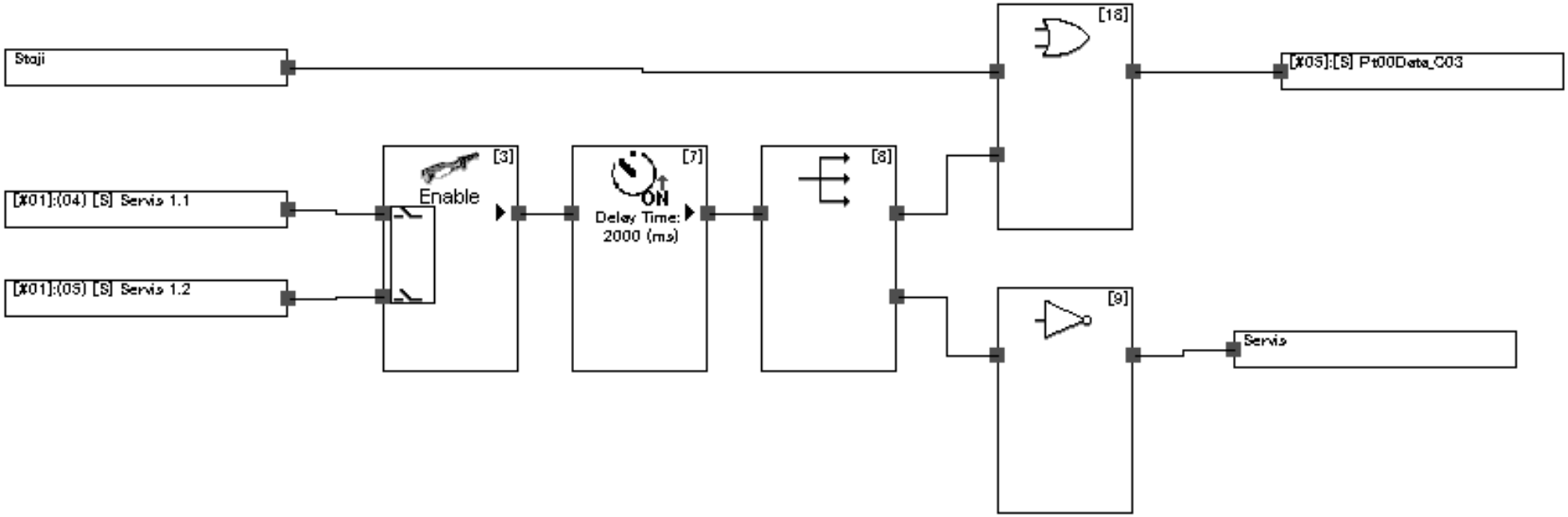


			Date	15.5.2016	Modul č. 2		FEKT VUTBR	OB8S_1.2	=
			Ed.	Bc. Milan Šindelek					+
			Appr		Diplomová práce - CIP Safety				Page 7
Modification	Date	Name	Original		Replacement of	Replaced by			Page 7

Příloha 3. Ovládací program PLC SmartGuard 600




[#01]:(15) [S] Reset
E-Stop
Servis
[10]
[11]
[12]
[13]
On Pulse time
500 (ms)
[14]
Restart
[15]
[16]
[17]
[19]
[20]
[21]
[#05]:[S] Pt05Data_C03
Staji
[#05]:[S] Pt04Data_C03
[#05]:[S] Pt06Data_C03


Stoji
[#01]:(04) [S] Servis 1.1
[#01]:(05) [S] Servis 1.2
[3]
Enable
[7]
ON
Delay Time:
2000 (ms)
[8]
[18]
[#05]:[S] Pt00Data_C03
[9]
Servis

Příloha 4: Obsah přiloženého CD-ROM

- DP_Šindelek_Milan_CIPSafety.pdf
- Projekt PLC 1756-L73S
- Sindelek_CIPSafety_vizualizace
- Logic_SG600_ESTOP.bmp
- Logic_SG600_LOGIKA.bmp
- Logic_SG600_RESET.bmp
- Report RSLogix 5000.pdp
- Report SISTEMA_Panel 1.pdf
- Report SISTEMA_Panel 2.pdf
- Report Vizualizace_Panel 2.pdf
- Schéma zapojení Panel 1.pdf
- Schéma zapojení Panel 2.pdf
- Sindelek_CIPSafety_DeviceNet.dnt
- Sindelek_CIPSafety_Logika.led
- Sindelek_CIPSafety_Report_Logika_SG600.html
- Sindelek_CIPSafety_Report_SG600.pdf