ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra řídicí techniky

BEZPEČNOSTNÍ FUNKCE PRO SIMATIC S7

Vedoucí práce:

Ing. Pavel Burget Ph.D.

Autor:

Petr Polák

Praha 2009

České vysoké učení technické v Praze - Fakulta elektrotechnická

Katedra řídicí techniky ***Školní rok:*** 2006/2007

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: Petr Polák

Obor: Technická kybernetika

Název tématu: Bezpečnostní funkce pro Simatic S7

Zásady pro vypracování:

1. Seznamte se s knihovnou S7 Distributed Safety.
2. Nastudujte vlastnosti profilu Profisafe pro Profibus DP, resp. Profinet IO.
3. Proveďte analýzu bezpečnostních rizik svářecího robota.
4. Realizujte bezpečnostní opatření pro svářecího robota, založená na využití Simatic S7 300, Profinet IO (případně Profibus DP) a S7 Distributed Safety.

Seznam odborné literatury: Dodá vedoucí práce.

Vedoucí diplomové práce: Ing. Pavel Burget

Termín zadání diplomové práce: zimní semestr 2006/2007

Termín odevzdání diplomové práce: leden 2008

prof. Ing. Michael Šebek, DrSc.
vedoucí katedry

L.S.

v zast.

prof. Ing. Zbyněk Škvor, CSc.
děkan

V Praze dne 21.02.2007

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil pouze podklady (literaturu, projekty, SW) uvedené v přiloženém seznamu.

V Praze dne 23. 01. 2009

Podpis: .....

Abstrakt

Tato práce má za úkol ukázat postup zabezpečení obsluhy robotického pracoviště s využitím Safety PLC firmy Siemens. Cílem je nastudovat a ukázat postup navržení bezpečnostních funkcí realizovaných bezpečnostním ovládacím systémem a zprovoznění bezpečnostního systému firmy Siemens, který je k dispozici na katedře řídicí techniky. Pro tento bezpečnostní systém pak vytvořit jednoduchý návod pro pozdější případné využití.

Abstract

Task of this work is to show the procedure of securing the operator of robotic station using the Safety PLC from Siemens. Goal is to get knowledge and show the process of creating safety functions that are realized by safety control system and putting the Siemens safety system into service. This system is available on Department of Control Engineering. Then will be created a simple guide for this safety system for further purposes.

Poděkování

Zde bych rád poděkoval lidem, kteří mi umožnili zdárné dokončení této práce. Především vedoucímu práce Ing. Pavlu Burgetovi Ph.D. za trpělivost a podporu v nelehké životní situaci. Dále panu Filipu Pelikánovi z firmy SICK za cenné rady a zasvěcení do problematiky bezpečnosti. Poté také samozřejmě rodině a přátelům za trvalou podporu nejen v období tvoření této práce, ale po celou dobu studia.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

V posledním období je v průmyslu kladen čím dál větší důraz na zajištění bezpečnosti, a to jak strojů, tak především obsluhy strojních zařízení. Ukazuje se, že zranění strojním zařízením je v průmyslu poměrně častý jev. Kromě možných fatálních následků s sebou nesou i pozdější velké finanční náklady při odstraňování způsobených škod. Zvýšením zabezpečení takového stroje snižujeme riziko způsobení škody a kromě ochrany obsluhy chráníme majitele a zaměstnavatele před případnými nepříjemnými výdaji.

Cílem této práce je seznámit čtenáře s problematikou bezpečnosti a předvést jeden z možných postupů návrhu bezpečnostního opatření strojního zařízení s využitím bezpečnostního systému firmy Siemens S7 Distributed Safety. Systém je k dispozici na katedře řídicí techniky.

Práce je rozdělena do čtyř částí. V první kapitole je ukázáno, že zajištění bezpečnosti je ve skutečnosti ze zákona povinné. V podkapitole je uveden postup návrhu bezpečnostního opatření dle normy ČSN EN ISO 13849–1. Splnění této normy je jednou z možných variant navržení zabezpečení strojního zařízení.

Druhá kapitola je zaměřena na popis PROFIsafe profilu. Jedná se o standardizovaný profil umožňující bezpečnostní komunikaci po průmyslových sběrnicích. Je zde rozebráno, na jakém principu tento profil pracuje.

Třetí kapitola popisuje bezpečnostní systémy firmy Siemens a především bezpečnostní systém S7 Distributed Safety, který se využívá pro zvýšení bezpečnosti strojních zařízení. Je zde nastíněna hardwarová konfigurace tohoto systému a způsob programování. Součástí této kapitoly je i Příloha 6, kde je vytvořen podrobnější návod na realizaci bezpečnostní aplikace za pomoci daného systému.

V poslední, čtvrté kapitole používáme získané znalosti z předchozích částí pro návrh zabezpečení robotického pracoviště v učebně K09 na katedře řídicí techniky.

1. Bezpečnost

Tato kapitola je zaměřena na téma „Co nám jako výrobci či provozovateli strojů předepisuje domovský stát (Česká republika) a Evropská unie“. Dále zde uvádím a částečně popisuji normy, které jsou pro problematiku bezpečnosti strojních zařízení nejdůležitější.

1.1 Legislativa

Vstupem České republiky do Evropské unie přizpůsobuje ČR své zákony a směrnice platné legislativě, vydaným směrnicím a normám EU. Tak je to i v tomto případě, kdy členské země mají za povinnost přijmout směrnici 2006/42/ES, kterou je nutno implementovat nejpozději do 29. prosince 2009. Česká republika přijala tuto směrnici Nařízením vlády č. 176/2008 Sb., s platností zákona právě od 29. prosince 2009. V současné době je v platnosti Nařízení vlády č. 24/2003 Sb. o Technických požadavcích na strojní zařízení [1].

1.1.1 Zákon č. 24/2003 Sb.

Zákon č. 24/2003 Sb. nám mimo jiné definuje podmínky při uvedení zařízení na trh nebo do provozu:

„Strojní zařízení nebo bezpečnostní součást, na které se vztahuje toto nařízení, mohou být uváděny na trh a do provozu pouze tehdy, neohrožují-li při správné instalaci, údržbě a při použití k určeným účelům zdraví a bezpečnost osob, popřípadě domácích a hospodářských zvířat nebo majetku."

Z výše uvedeného plyne zákonná povinnost výrobce a provozovatele strojního zařízení zabývat se bezpečností daného zařízení, bezpečností obsluhy zařízení a okolí stroje. Bližší požadavky na bezpečné provozování stojů a technických zařízení stanoví zákon č. 378/2001 Sb. [2]. Tento zákon nám předepisuje některé následující minimální požadavky na bezpečné provozování strojů a technických zařízení:

- *„zařízení používáme k účelům a za podmínek, pro které je určeno v souladu s provozní dokumentací; zaměstnavatel může stanovit další požadavky na bezpečnost místním provozním bezpečnostním předpisem, a to minimálně v rozsahu daném normovanou hodnotou*

[1] Nařízení vlády č. 24/2003 platí především pro výrobce strojních zařízení
[2] Nařízení vlády č. 378/2001 platí především pro „uživatele“, provozovatele strojních zařízení

- *zaměstnavatel stanoví bezpečný přístup obsluhy k zařízení a dostatečný manipulační prostor se zřetelem na technologický proces a organizaci práce, umožňující bezpečné používání zařízení*
- *přívod všech forem energií a i jejich odvod musí být proveden bezpečným způsobem*
- *vybavit zařízení zábranou nebo ochranným zařízením nebo přijetím opatření tam, kde existuje riziko kontaktu nebo zachycení zaměstnance pohybujícími se částmi pracovního zařízení nebo pádu břemene*
- *umístění ovládacích prvků ovlivňujících bezpečnost provozu zařízení mimo nebezpečné prostory, bezpečné ovládání, a to i v případech jejich poruchy nebo poškození, dobrá viditelnost, rozpoznatelnost a v určených případech příslušné označení; nemohou-li být ovládací prvky z technických důvodů umístěny mimo nebezpečné prostory, nesmí být jejich ovládání zdrojem nebezpečí, a to i v důsledku nahodilého úkonu*
- *spouštět zařízení pouze záměrným úkonem obsluhy pomocí ovládače, který je k tomuto účelu určen*
- *vybavit zařízení ovladačem pro úplné bezpečné zastavení; v době, kdy se zařízení nepoužívá jeho vypnutí a ve stanovených případech jeho odpojení od zdrojů energií a zabezpečení*
- *vybavení ovladačem pro nouzové zastavení, který zablokuje spouštěcí ovladače tam, kde je to nutné; současně se zastavením chodu zařízení nebo jeho nebezpečné části se musí vypnout přívody energií k jeho pohonům, s výjimkou případů, kdy by tím došlo k ohrožení života nebo zdraví zaměstnanců*
- *vybavit zařízení zřetelně identifikovatelnými zařízeními pro jeho odpojení od všech zdrojů energií; následné připojení zařízení nesmí znamenat pro zaměstnance žádné riziko*
- *obsluha musí mít možnost se přesvědčit, že v nebezpečných prostorech se nenachází žádný zaměstnanec, pokud nelze tento požadavek splnit, bezpečnostní zařízení musí vydávat zvukový nebo viditelný výstražný signál před jeho spuštěním, aby ostatní zaměstnanci měli dostatek času nebezpečný prostor opustit"*

Dále uvádím některé požadavky vyplývající z tohoto zákona na ochranná zařízení:

- *„musí mít pevnou konstrukci odolnou proti poškození*
- *musí být umístěno v bezpečné vzdálenosti od nebezpečného prostoru*

- *nesmí bránit montáži, opravě, údržbě, seřizování a dalším úkonům potřebným při obsluze stroje; přístup zaměstnance musí být omezen pouze na tu část zařízení, kde je prováděna činnost, a to pokud možno bez sejmutí ochranného zařízení*
- *nesmí být snadno odnímatelné nebo odpojitelné*
- *nesmí omezovat výhled na provoz více, než je nezbytně nutné"*

Zákon nám také předepisuje požadavky na provádění kontrol zabezpečení a funkčnosti stroje a na vyhotovení a uchovávání provozní dokumentace daného zařízení po celou dobu jeho života. Kontrola se má provádět minimálně jednou za 12 měsíců, nestanoví-li místní bezpečnostní předpis, právní předpis, průvodní dokumentace nebo normové hodnoty četnost bezpečnostních kontrol jinak.

1.1.2 Zákon č. 176/2008 Sb.

Jak již jsem zde uvedl, 29. prosince 2009 vejde v platnost zákon č. 176/2008 Sb., který nahradí zákon č. 24/2003. Z tohoto důvodu bych zde chtěl zmínit některé důležité body, ve kterých se tento zákon odlišuje od předešlého a co nám přináší při řešení zabezpečení stroje a jeho okolí.

Zákon v sobě nese směrnici 2006/42/ES Evropské Unie, která vznikla z důvodu vysokého nárůstu nákladů způsobených častými úrazy ve strojním průmyslu. Jelikož strojní průmysl patří k hlavním oborům hospodářství Evropského společenství, snaží se toto společenství počet úrazů, a tím vyplývajících nákladů snížit. Tato směrnice je jedním ze způsobů, jak lze tohoto dosáhnout. Členské státy jsou na svém území odpovědné za zajištění bezpečnosti a zdraví osob, zvířat a majetku vzhledem k nebezpečí, které může vzniknout použitím strojních zařízení

Důležité body a definice Nařízení vlády č. 176/2008 Sb.[3]:

Definice:

- *„Strojní zařízení, je soubor, který je vybaven nebo má být vybaven poháněcím systémem, který nepoužívá přímo vynaloženou lidskou nebo zvířecí sílu, sestavený z částí nebo součástí, z nichž alespoň jedna je pohyblivá, vzájemně spojených za účelem přesně stanoveného použití.*
- *Bezpečnostní součást, je součást, která plní bezpečnostní funkci, uvádí se na trh samostatně, jejíž selhání nebo chybná funkce ohrožuje bezpečnost osob a jejíž nepřítomnost nemá vliv na funkci stroje.*

[3] Snažím se uvést pouze body a definice, jež mají vztah s dalším směřováním této práce – návrh bezpečnostního opatření robota

- *Riziko, kombinace pravděpodobnosti a závažnosti poranění nebo škody zdraví, ke které může dojít v nebezpečné situaci.*
- *Ochranný kryt, část strojního zřízení, která se používá výhradně k zajištění ochrany, a to pomocí fyzické bariéry.*
- *Ochranné zařízení, zařízení (vyjma ochranného krytu), které snižuje riziko, a to samotné nebo ve spojení s ochranným krytem.*
- *Předpokládané použití, použití v souladu s návodem použití.*
- *Předvídatelné nesprávné použití, použití, jež není v návodu použití, ale dá se lehce předvídat z lidského chování.*
- *Nebezpečí je možný zdroj poranění nebo poškození zdraví.*
- *Nebezpečný prostor, je každý prostor uvnitř nebo okolo strojního zařízení, ve kterém je osoba vystavena nebezpečí, které ohrožuje její zdraví nebo bezpečnost.“*

Požadavky před uvedením na trh nebo do provozu:

- *„Zařízení může být uvedeno do provozu nebo na trh pokud je vyrobeno a provozováno tak, že neohrožuje zdraví nebo bezpečnost osob, zvířat nebo majetku.*
- *Před uvedením zařízení na trh nebo do provozu výrobce nebo zplnomocněný zástupce zajišťuje, aby byla k dispozici technická dokumentace, návody, vydává prohlášení o shodě s ES[4], opatřuje zařízení označením CE[5].*
- *Výrobce nebo jeho zplnomocněný zástupce zajišťuje posouzení rizika s cílem jeho snížení a určuje požadavky na ochranu zdraví a bezpečnosti, které platí pro strojní zařízení. Strojní zařízení musí být konstruováno s přihlédnutím k výsledkům posouzení rizika.*
- *Výrobce vymezuje použití strojního zařízení a jeho předvídatelné nesprávné využití.*
- *Výrobce určuje nebezpečí, která vyplývají ze strojního zařízení.*
- *Odhaduje rizika vzniku poškození zdraví a pravděpodobnost jejich výskytu.*
- *Vyhodnocuje rizika s cílem určit, zda je nutné snížit riziko nebezpečí vzniku například úrazu.*
- *Zajišťuje ochranná opatření k vyloučení nebo ke snížení příslušných rizik.“*

Zásady zajišťování bezpečnosti:

- *„Vyloučit nebezpečí již při návrhu a při konstrukci strojního zařízení.*
- *Učinit nezbytná ochranná opatření v případě nebezpečí, které nelze vyloučit.*

[4] ES směrnice Evropské Unie
[5] CE označení vyjadřuje splnění technického standardu Evropského společenství tzv. harmonizovanou evropskou normu. Označení CE je povinné pokud specifické směrnice nestanoví jinak.

- *Informovat uživatele o přetrvávajícím nebezpečí.“*

Bezpečnost a spolehlivost bezpečnostních systémů:

- *„Ovládací systémy musí být navrženy a konstruovány tak aby nedocházelo k nebezpečným situacím, musí snést zátěž běžného užívání, závada v technickém nebo programovém vybavení nesmí vést k nebezpečným situacím.*
- *Strojní zařízení nesmí být do chodu uvedeno neočekávaně.*
- *Nesmí být zabráněno zastavení stroje, pokud již k tomu byl vydán povel.*
- *Ochranné zařízení musí být plně funkční, pokud není, má ochranné zařízení, vydat povel k zastavení.*
- *Ovládací zařízení musí být umístěno vně nebezpečného prostoru, s výjimkou určitých ovládacích zařízení jako je například tlačítko nouzového zastavení.*
- *Z každého stanoviště obsluhy se musí být obsluha schopna ujistit, zda se někdo v nebezpečném prostoru nenachází, popřípadě musí být ovládací zařízení konstruováno tak, že se zamezí spuštění, pokud se někdo nachází v nebezpečném prostoru.“*

Spouštění a zastavení zařízení:

- *„Zařízení může být spuštěno pouze záměrným působením na ovládací zařízení, které je k tomu určeno, platí to i při opakovaném spouštění po zastavení zařízení z jakékoliv příčiny nebo při výrazné změně provozních podmínek.*
- *Opakované spouštění může být provedeno jiným ovládacím zařízením, než jaké je k tomu určeno, ale nesmí toto vést k nebezpečné situaci.*
- *V režimu automatického provozu může být automatické spuštění bez zásahu, pokud to nepovede k nebezpečné situaci.*
- *Strojní zařízení musí být vybaveno ovládacím zařízením, jímž může být bezpečně a úplně zastaveno.*
- *Povel pro zastavení musí být nadřazen povelům pro spouštění.*
- *Strojní zařízení musí být vybaveno jedním nebo několika zařízeními pro nouzová zastavení, která umožňují odvrácení skutečného nebo hrozícího nebezpečí.“*

Značení strojního zařízení – na zařízení musí být vyznačeny minimálně tyto údaje:

- *„Obchodní firma a úplná adresa výrobce, popřípadě jeho zplnomocněného zástupce,*
- *Označení strojního zařízení,*
- *Označení CE,*

- *Označení série nebo typu,*
- *Výrobní číslo pokud existuje,*
- *Rok výroby.“*

Dále tento zákon obsahuje požadavky na návody použití, technickou dokumentaci, na provedení prohlášení o shodě ES a upřesňující požadavky na strojní zařízení například lisy, pily, zařízení pro převážení osob, zdvihací zařízení atd.

Shrnu-li celý zákon, tak nám předepisuje minimální požadavky na výrobek, na jeho provozování. Jeho největší změnou oproti předešlému zákonu je předepsání provádění analýzy rizik strojního zařízení a toto zařízení pak navrhovat a konstruovat s přihlédnutím k výsledkům této analýzy.

1.2 Normy

České technické normy, označené ČSN, nejsou obecně závazné, jsou pouze doporučující. Jejich závaznost může vzniknout právním předpisem, kdy právní předpis, zákon, se na tuto normu odkazuje, a tím se stává norma závaznou.

V názvu norem se můžeme setkat s několika označeními:

- ČSN – norma platná na území ČR, norma schválená Českým normalizačním institutem ČNI;
- EN – norma vydaná Evropským normalizačním institutem;
- ISO, IEC – mezinárodní norma;
- ČSN EN, ČSN ISO – jedná se o přejatou normu z evropského nebo mezinárodního normalizačního institutu.

Typy bezpečnostních norem:

- Typ A – normy popisující základní pojmy a všeobecné zásady;
- Typ B – normy zabývající se jedním bezpečnostním hlediskem B1 nebo jedním typem bezpečnostních zařízení B2;
- Typ C – specifické normy pro určitá strojní zařízení.

V Příloze 5 uvádím přehled nejdůležitějších norem vztahujících se k bezpečnosti strojních zařízení. Dále se budu podrobně věnovat pouze jedné, která s mojí prací bezprostředně souvisí. Jde o normu ČSN EN ISO 13849–1: Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů, která specifikuje požadavky pro konstrukci a realizaci bezpečnostních částí ovládacích systémů strojních zařízení. Postup podle této normy může být předpokladem pro

splnění základních bezpečnostních požadavků. Norma je nástupcem normy ČSN EN 954–1, podobně jako norma ČSN EN 62061, pomocí které také můžeme provést návrh bezpečnostní části řídicího systému. Na konci této kapitoly uvádím srovnání použití těchto tří norem.

1.2.1 Základní definice normy ČSN EN ISO 13849–1

Norma popisuje bezpečnostní požadavky a pokyny pro zásady konstrukce a integrace bezpečnostních částí ovládacích systémů (SRP/CS), včetně návrhu software. Pro tyto části SRP/CS specifikuje norma vlastnosti požadované k vykonávání bezpečnostních funkcí. Norma platí pro bezpečnostní části řídicích systémů strojních zařízení bez ohledu na druh používané technologie a energie (hydraulická, pneumatická, elektrická, atd.). Norma však neuvádí bezpečnostní funkce nebo úrovně vlastností těchto funkcí pro jednotlivé případy, dále neuvádí požadavky na konstrukci výrobků, které jsou součástí ovládacích systémů.

Důležité termíny a definice:

V této části jsou popsány důležité termíny a definice, které jsou součástí normy, a které čtenáři umožní se lépe orientovat v následujícím textu.

Bezpečnostní část ovládacího systému SRP/CS (**S**afety-**R**elated **P**art of a **C**ontrol **S**ystem) – část ovládacího systému, která reaguje na bezpečnostní vstupní signály a vytváří bezpečnostní výstupní signály.

Kategorie (category) – klasifikace bezpečnostních částí ovládacího systému vzhledem k odolnosti proti závadám a jejich následnému chování v podmínce závady, kterých je dosaženo konstrukčním uspořádáním částí, detekcí závady, případně jejich spolehlivosti.

Nebezpečná porucha (dangerous failure) – porucha, která může uvést SRP/CS do stavu nebezpečí nebo selhání funkce.

Porucha se společnou příčinou CCF (**C**ommon **C**ause **F**ailure) – poruchy různých objektů vyplývající z jedné události, kde tyto poruchy nejsou vzájemným důsledkem každé z nich.

Systematická porucha (systematic failure) – porucha související s určitou příčinou, může být však vyloučena pouze modifikací konstrukce nebo výrobního procesu, provozních postupů, dokumentací nebo jiných relevantních faktorů.

Vyřazení (muting) – přechodné automatické přerušení bezpečnostní funkce bezpečnostními částmi ovládacího systému.

Posuzování rizika (risk assessment) – celkový proces zahrnující analýzu rizika a hodnocení rizika.

Bezpečnostní funkce (safety function) – funkce stroje, jejíž porucha může vést k okamžitému zvýšení rizika.

Monitorování (monitoring) – bezpečnostní funkce, která zajišťuje, že je iniciováno bezpečnostní opatření tehdy, je-li schopnost prvku nebo součásti k vykonávání své funkce snížena.

Programovatelný elektronický systém PES (**P**rogrammable **E**lectronic **S**ystem) – systém k ovládání, ochraně, monitorování, jehož činnost závisí na jednom nebo více programovatelných elektronických zařízeních, zahrnující všechny prvky systému (napájecí zdroje, senzory, stykače, apod.).

Úroveň vlastností PL (**P**erformance **L**evel) – diskrétní úroveň používaná k určení schopností bezpečnostních částí ovládacích systémů k vykonávání bezpečnostní funkce při předvídatelných podmínkách.

Požadovaná úroveň vlastností PL_r (required performance level) – úroveň vlastností PL používaná k tomu, aby bylo dosaženo pro každou bezpečnostní funkci požadovaného snížení rizika.

Střední doba do nebezpečné poruchy $MTTF_d$ (**M**ean **T**ime **T**o dangerous **F**ailure) – očekávaná střední doba do nebezpečné poruchy.

Diagnostické pokrytí DC (**D**iagnostic **C**overage) – míra účinnosti diagnostiky, která může být určena jako podíl intenzity detekovaných poruch a intezity všech nebezpečných poruch.

Úrověň integrity bezpečnosti SIL (**S**afety **I**ntegrity **L**evel) – diskrétní úroveň pro stanovení požadavků integrity bezpečnostních funkcí. S těmito úrovněmi pracuje norma ČSN EN 62061 nebo ČSN EN 61508.

Jazyk s omezenou variabilitou LVL (**L**imited **V**ariability **L**anguage) – typ jazyka, který poskytuje schopnost kombinovat předem definované, aplikačně specifické knihovní funkce pro realizaci bezpečnostních požadavků. Mezi tyto jazyky patří žebříčkový programovací jazyk (LAD) a programovací jazyk využívající funkční bloková schémata (FBD).

Jazyk s plnou variabilitou FLV (**F**ull **V**ariability **L**anguage) – jazyk, který umožňuje realizovat široký výběr funkcí a aplikací, například C, C++, Java, apod.

Software:

Norma nám udává požadavky na software a jeho programování. Dále popisuje postupy, jak pracovat s jejich softwarem a správně naprogramovat bezpečnostní funkce. K programování je doporučené využívat funkce z bezpečnostních knihoven dodané vývojářem softwaru. Jedná o certifikované funkce, které umožňují splnění požadavků příslušných norem. Dále by bezpečnostní programy měly být strukturované, snadno čitelné a přehledné. V současné době se jako bezpečnostní programovací jazyky využívají jazyky s omezenou variabilitou LVL.

1.2.2 Postup návrhu SRP/CS dle normy ČSN EN ISO 13849–1

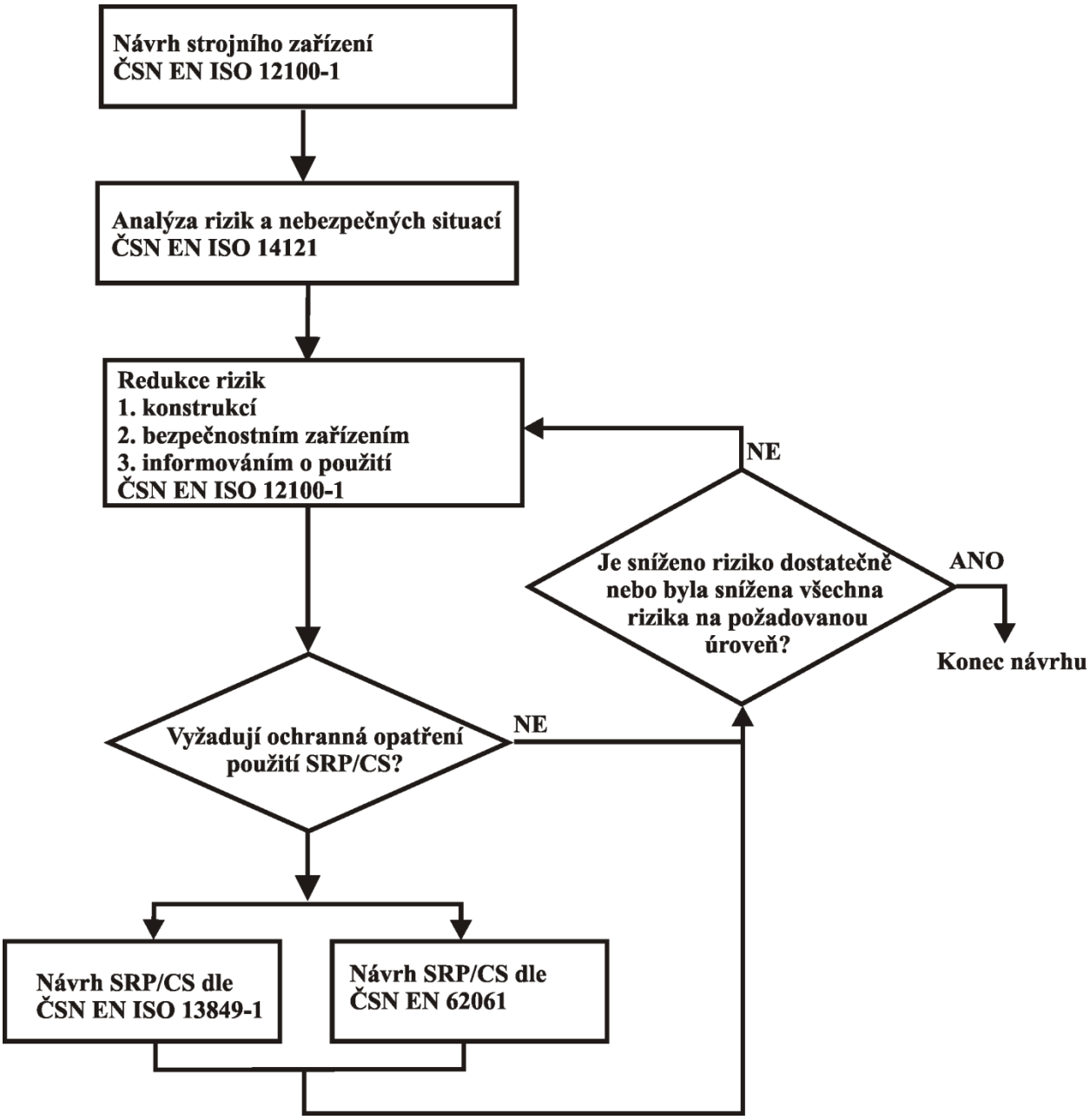
Při návrhu strojního zařízení postupujeme dle obrázku (Obrázek 1). Pokud provedením analýzy rizik a nebezpečných situací zjistíme, že případné riziko je vhodné odstranit nebo snížit na požadovanou úroveň použitím SRP/CS, postupujeme dle obrázku (Obrázek 2). Vždy definujeme bezpečnostní funkci, která má snížit příslušné riziko a k této funkci stanovíme její požadovanou úroveň PLr. Poté provedeme návrh realizace (konstrukce) bezpečnostní funkce a pro tuto konstrukci provedeme ověření splnění úrovně vlastností PL. Pokud je úroveň PL menší než PLr, proces opakujeme. Tento postup aplikujeme na všechny námi určené bezpečnostní funkce.

Úroveň vlastností PL je v této normě definována jako forma pravděpodobnosti nebezpečné poruchy za hodinu. Norma stanoví pět úrovní s definovanými rozsahy pravděpodobnosti poruchy za hodinu (viz Tabulka 1).

Tabulka 1: Úroveň vlastností (PL)

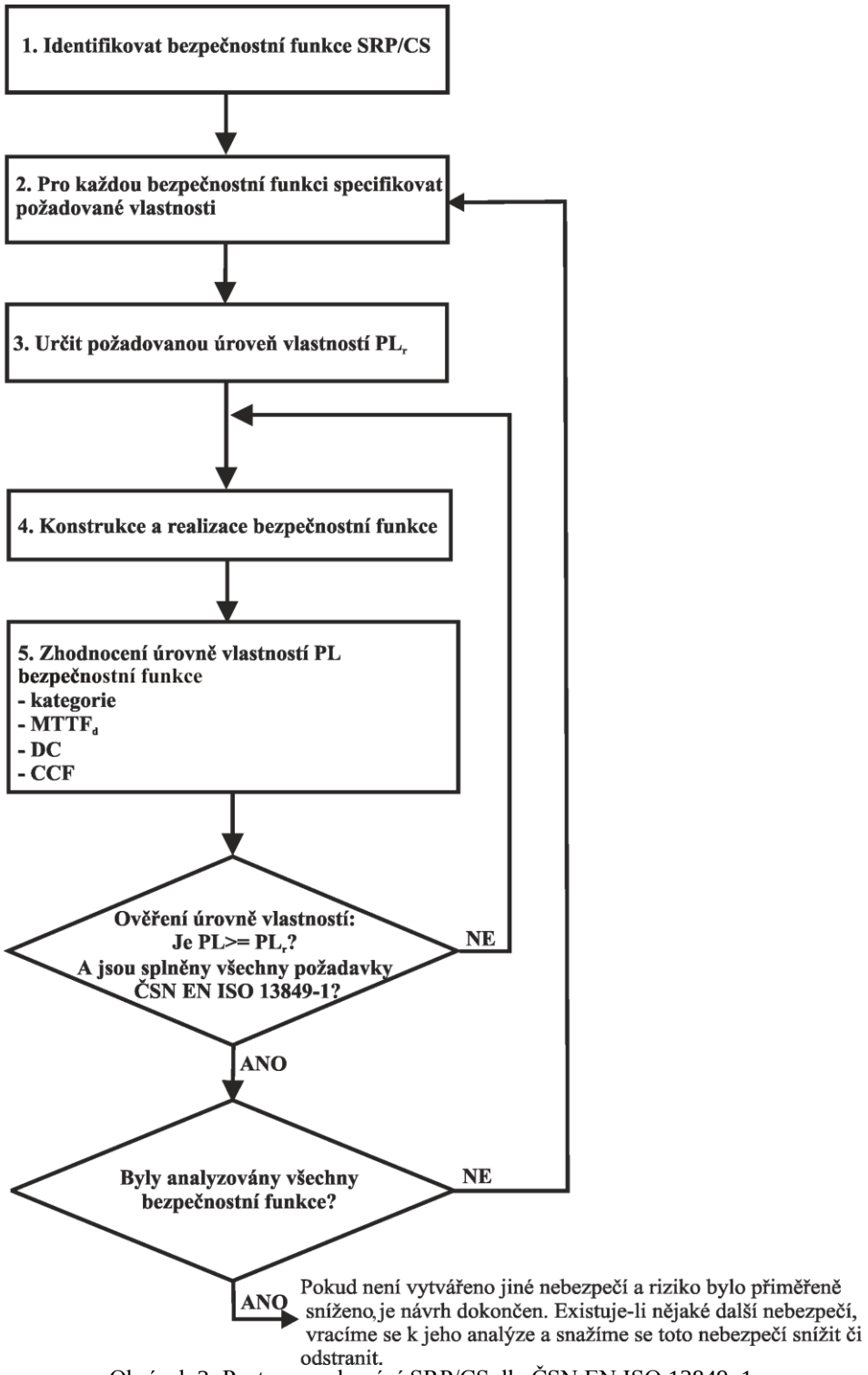
Úroveň vlastností PL	Průměrná pravděpodobnost poruchy za hodinu - 1/h
a	$<10^{-5}$; 10^{-4})
b	$< 3 \cdot 10^{-6}$;10^{-5})
c	$< 10^{-6}$; $3 \cdot 10^{-6}$)
d	$< 10^{-7}$; 10^{-6})
e	$<10^{-8}$; 10^{-7})

Zdroj: [6]



Obrázek 1: Postup návrhu bezpečného strojního zařízení

Zdroj: [5], vlastní úprava

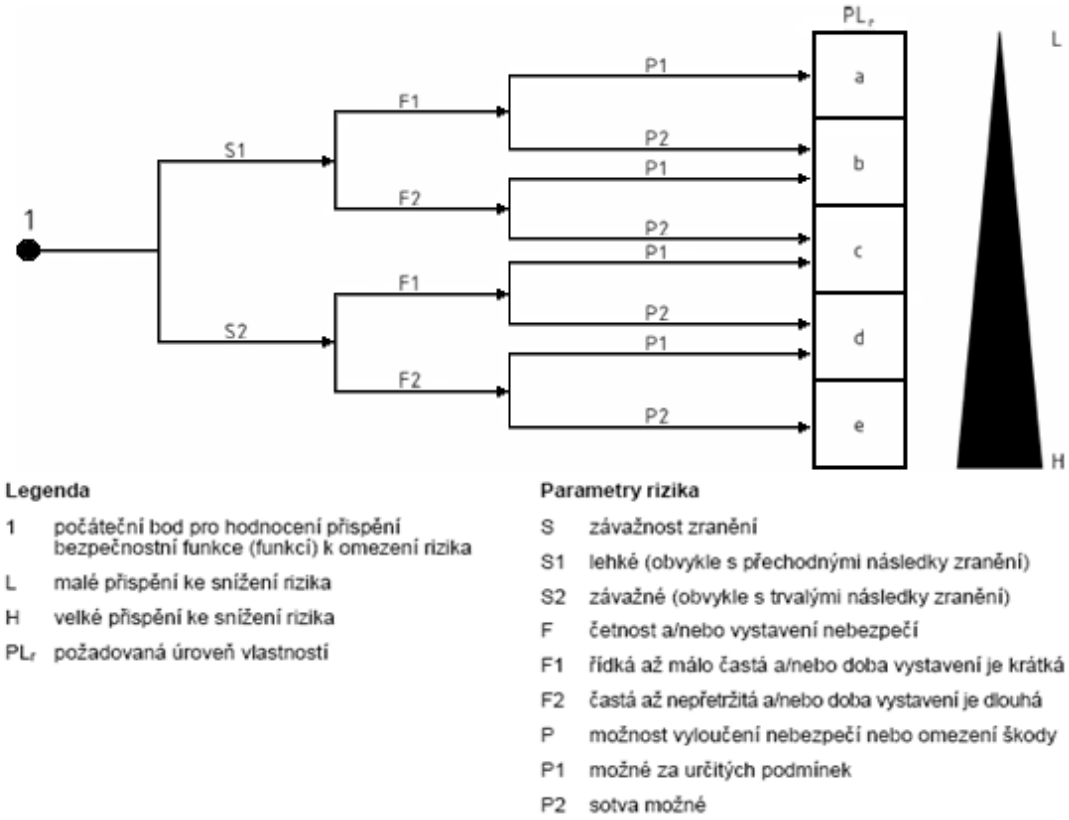


Obrázek 2: Postup navrhování SRP/CS dle ČSN EN ISO 13849–1

Zdroj:[6], vlastní úprava

Způsob určení požadované úrovně PL_r:

Norma ve své příloze popisuje návod na určení PL_r navržené bezpečnostní funkce. Čím je větší požadavek na snížení rizika bezpečnostními částmi ovládacího systému, tím musí být úroveň PL_r větší. Jedná se však pouze o odhad rizika, pokud by došlo k selhání bezpečnostní funkce. Úroveň PL_r určíme u obrázku (Obrázek 3), kdy postupným odhadem závažnosti zranění (S1, S2), četností a dobou vystavení nebezpečí (F1, F2) a možností vyloučení nebezpečí nebo omezení škody (P1, P2) vybereme příslušnou úroveň vlastností PL_r.

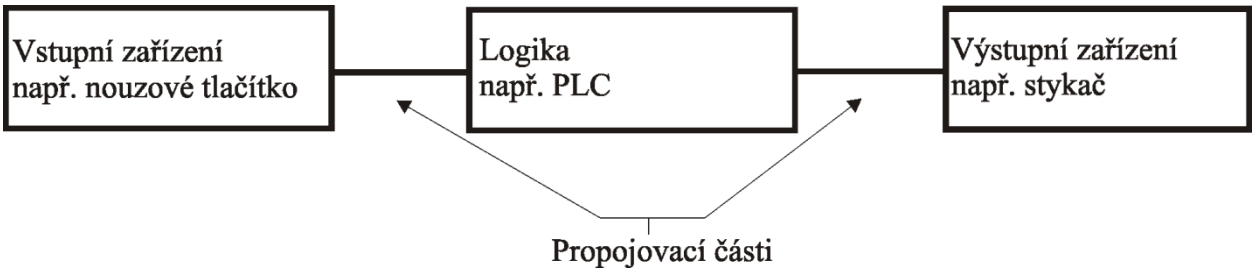


Obrázek 3: Stanovení PL_r

Zdroj: [6]

Konstrukce bezpečnostní funkce:

Konstrukcí bezpečnostní funkce se rozumí spojení bezpečnostních částí SRP/CS. Obvykle se skládá ze vstupního, vyhodnocovacího, výstupního modulu a propojovacích částí (viz Obrázek 4). Bezpečnostní funkce mohou využívat jednu část SRP/CS i více částí, např. mohou využívat jednu logickou jednotku. Je vhodné konstruovat bezpečnostní funkce již dle některé z doporučených architektur pro snadnější zařazení do příslušné konstrukční kategorie a tím snadnější určení PL. O kategoriích a příslušných architekturách se podrobněji zmiňuji v podkapitole Kategorie, architektury bezpečnostních částí.



Obrázek 4: Blokové schéma konstrukce bezpečnostní funkce

Zdroj: [6], vlastní úprava

Zhodnocení dosažení úrovně PL bezpečnostní funkce:

Úroveň PL bezpečnostní části je určená následujícími parametry:

- $MTTF_d$
- DC
- CCF
- Kategorií a architekturou konstrukce

$MTTF_d$:

Střední doba do nebezpečné poruchy kanálu se dělí na tři úrovně, označující dobu trvání, než dojde k nebezpečné poruše (viz Tabulka 2**)** a je to celková doba složená z $MTTF_d$ jednotlivých částí SRP/CS, které jsou využity pro konstrukci bezpečnostní funkce. Maximální hodnota $MTTF_d$ je 100 let. Norma uvádí čtyři možnosti určení $MTTF_d$ pro jednotlivé části SRP/CS: Metoda dobrých technických praxí, Metoda pro mechanické, pneumatické a elektromechanické součásti, Metoda pro hydraulické součásti a Metoda pro elektronické součásti.

Tabulka 2: Úrovně $MTTF_d$ každého kanálu

Označení doby $MTTF_d$ pro jednotlivý kanál	**Rozsah doby $MTTF_d$ pro jednotlivý kanál**
krátká	3 roky $\leq MTTF_d <$ 10 let
střední	10 let $\leq MTTF_d <$ 30 let
dlouhá	30 let $\leq MTTF_d \leq$ 100 let

Zdroj: [6]

Metoda dobrých technických praxí:

Pokud je součástka vyrobena podle základních a osvědčených zásad ČSN EN ISO 13849–2 nebo relevantní normy pro danou součástku, výrobce specifikuje vhodné použití a provozní podmínky pro uživatele. A pokud konstrukce SRP/CS splňuje opět základní a osvědčené zásady ČSN EN ISO 13849–2, pak lze $MTTF_d$ nebo hodnotu B_{10d} odhadnout z tabulky C. 1 přílohy C normy ČSN EN ISO 13849–1 (zdroj: [6]). Hodnota B_{10d} udává střední počet cyklů do doby, kdy 10 % součástí nebezpečně selže. Výpočty poruch předpokládají exponenciální rozdělení, pro pneumatické a elektromechanické je pravděpodobnější Weibullovo rozdělení. Pro praxi lze použít uvedený výpočet **(**zdroj: [6]).

Výpočet $MTTF_d$ a T_{10d} ze známého B_{10d}:

$$\boldsymbol{MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}} \qquad \text{(R.1)}$$

$MTTF_d$ – střední doba do nebezpečné poruchy;

B_{10d} – střední počet cyklů do doby, než 10 % součástí selže;

n_{op} – střední počet činností za rok;

$$\boldsymbol{n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{cyklu}}} \qquad \text{(R.2)}$$

h_{op} – střední doba provozu v hodinách za den;

d_{op} – střední doba provozu ve dnech za rok;

t_{cyklu} – střední doba mezi začátkem dvou po sobě následujících cyklů součásti v s/cyklus.

Doba provozu součásti vyjadřuje střední dobu T_{10d} do které 10 % součástí nebezpečně selže:

$$\boldsymbol{T_{10d} = \frac{B_{10d}}{n_{op}}} \qquad \text{(R.3)}$$

Příklad 1**(**zdroj: [6]):

Pneumatický ventil, jehož B_{10d} určil výrobce na 60 miliónů cyklů, se používá pro dvě přesunutí každý den, a to 220 dnů v roce. Střední doba mezi začátkem dvou po sobě následujících přesunutí ventilu je odhadnuta na 5 s.

h_{op} = 16 h za den;

d_{op} = 220 dnů za rok;

t_{cyklu} = 5 s/cyklus;

B_{10d} = 60 miliónů cyklů;

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600 s/h}{t_{cyklu}} = \frac{220 \cdot 16 \cdot 3600}{5} = 2,53 \cdot 10^6 \, cyklů/rok$$

$$T_{10d} = \frac{B_{10d}}{n_{op}} = \frac{60 \cdot 10^6}{2,53 \cdot 10^6} = 23,7 \, let$$

$$MTTF_d = \frac{B_{10d}}{0,1 \cdot n_{op}} = \frac{T_{10d}}{0,1} = \frac{23,7}{0,1} = 237 \, let$$

Pro provoz ventilu 23,7 let je předpokládaná střední doba do nebezpečné poruchy „dlouhá“.

Hydraulické součásti:

Pokud jsou hydraulické součásti vyrobeny dle základních a osvědčených bezpečnostních zásad ČSN EN ISO 13849–2 a výrobce specifikuje vhodné použití a provozní podmínky pro uživatele, je doba $MTTF_d$ hydraulické součásti odhadnuta na 150 let. Pokud toto není stanoveno, musí $MTTF_d$ stanovit výrobce.

Mechanické, pneumatické a elektromechanické součásti:

Pro tyto prvky bývá velice složité určit dobu $MTTF_d$. Při splnění požadavků na bezpečnou konstrukci dle normy ČSN EN ISO 13849–2 a výrobcem stanovené vhodné použití se využívá vzorců, které jsem uvedl výše (u bodu Metoda dobrých technických praxí). Uvedený příklad použití těchto vzorců názorně předvádí.

Elektrické součásti:

Norma obsahuje tabulky s údaji $MTTF_d$ běžně používaných elektronických prvků, nejsou však vyčerpávající a je povoleno i doporučeno používat i jiné databáze prvků s těmito údaji. Pokud se však jedná o ověřenou databázi.

Pokud určíme $MTTF_d$ pro jednotlivé součásti SRP/CS, provedeme odhad $MTTF_d$ pro celý kanál.

Metoda součtu částí:

Tato metoda je, jako ostatně většina metod, pouze přibližná, ale je plně dostačující pro výpočet požadované hodnoty. Touto metodou řešíme každý kanál samostatně, a to tak, že každá nebezpečná porucha jakékoliv součásti vede k nebezpečné poruše celého kanálu. Rovnice nám popisuje možnost výpočtu po jednotlivých součástech, nebo pokud se v dané realizaci bezpečnostní funkce nějaká součást opakuje nebo má stejnou $MTTF_d$, lze ji zjednodušeně zahrnout do výpočtu.

$$\boldsymbol{MTTF_d = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} = \sum_{j=1}^{N} \frac{n_j}{MTTF_{dj}}} \qquad \text{(R.4)}$$

$MTTF_d$ – střední doba do nebezpečné poruchy pro celý kanál;

$MTTF_{di}$ – výpočet po jednotlivých součástech SRP/CS;

$MTTF_{dj}$ – výpočet s opakující se součástí SRP/CS (udává hodnotu pro jednu součást);

n_j – počet opakování součásti SRP/CS.

Metoda pro různé kanály:

Tuto metodu využijeme, pokud zálohovací kanály mají jinou hodnotu $MTTF_d$ pro každý kanál. Architektury, neboli kategorie zapojení dle normy ČSN EN ISO 13849–1 uvažují s variantou, kdy kanály mají shodnou dobu $MTTF_d$ a je proto potřeba provést tzv. zesouměrnění $MTTF_d$. Metoda nám určuje dva možné postupy:

- Vzít nižší hodnotu $MTTF_d$ jako předpoklad horší varianty.
- Použít následující rovnici (zdroj[6]):

$$\boldsymbol{MTTF_d = \frac{2}{3}\left(MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right)} \qquad \text{(R.5)}$$

Zdroj: [6]

$MTTF_{dC1}$, $MTTF_{dC2}$ jsou dvě různé hodnoty pro dva různé zálohované kanály.

Tato úprava je nezbytná, pokud je podobná architektura použita pro využití zjednodušeného návrhu pomocí obrázku **(**zdroj: [6] – Obrázek 5) nebo tabulky (Tabulka 4).

DC:

Míru účinnosti diagnostiky a detekci závady lze dle normy zjednodušeně odhadnout z příslušných tabulek pro jednotlivé části SRP/CS (vstup, logika, výstup). Jednotlivé tabulky jsou uvedeny v části Příloha 1. Pro určení DC celého kanálu má však význam DC_{avg}, což je střední hodnota diagnostického pokrytí, kterou získáme dle rovnice R.6 výpočtem z DC a $MTTF_d$ jednotlivých částí SRP/CS. Jednotlivé úrovně DC_{avg} jsou uvedeny v tabulce (Tabulka 3).

Pokud se nespokojíme s touto zjednodušenou formou odhadu, lze pro určení DC_{avg} použít metodu režimu poruchy a analýzy poruchy (FMEA viz zdroj [7]) nebo podobnou metodu.

Tabulka 3: Střední hodnota diagnostického pokrytí

DC_{avg} označení	DC rozsah
žádné	DC < 60 %
nízké	60 % ≤ DC < 90 %
střední	90 % ≤ DC < 99 %
vysoké	99 % ≤ DC

Zdroj: [6]

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + .. + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + .. + \frac{1}{MTTF_{dN}}} \qquad \text{(R.6)}$$

CCF:

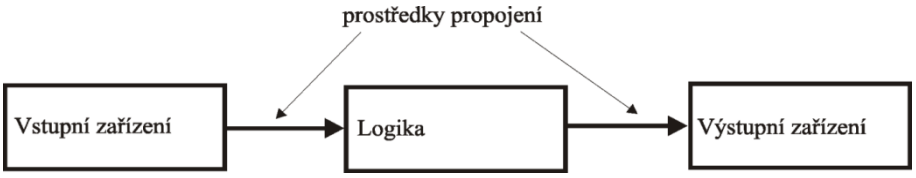
Porucha se společnou příčinou je parametr důležitý pro zvolení správné kategorie realizace bezpečnostní funkce. Kdy pro kategorii 2 a více je nutné provádět kontrolu, zda jsme dostatečně ošetřili poruchu se společnou příčinou. Pro tuto kontrolu norma obsahuje tabulku (viz. Příloha 2), jejímž vyplněním a bodovým ohodnocením zjistíme, zda jsme tyto chyby patřičně ošetřili. Bodové ohodnocení provádíme způsobem „vše nebo nic“. Tím mám na mysli, že pokud dané opatření splňujeme pouze z části, je to hodnoceno 0 body. Abychom mohli prohlásit, že se nám podařilo tyto poruchy ošetřit, musíme získat minimálně 65b.

Kategorie architektury bezpečnostní části:

Pokud navrhujeme části SRP/CS, musíme určit, do jaké kategorie konstrukčně patří. Norma uvádí pět kategorií (B, 1, 2, 3, 4). Tyto kategorie mají vliv na úroveň vlastností PL, a proto pro splnění požadovaného PL_r, podle jeho výše, je vhodné si dobře architekturu konstrukce bezpečnostní části promyslet. Protože dosažení požadovaného PL_r může být možné, dle jeho

úrovně, až od určité kategorie. Následně uvádím tabulku v Příloze 3 s přehledem kategorií, jejich vlastností a požadavků pro splnění uvedené kategorie. K příslušným kategoriím se váže i stanovená architektura bezpečnostní části. Doporučené architektury pro jednotlivé kategorie jsou zobrazené na následujících obrázcích (Obrázek 5, Obrázek 6, Obrázek 7). Na jednotlivé architektury je nutno pohlížet jako na logická schémata. Maximální dosažitelné úrovně vlastností PL pro jednotlivé kategorie:

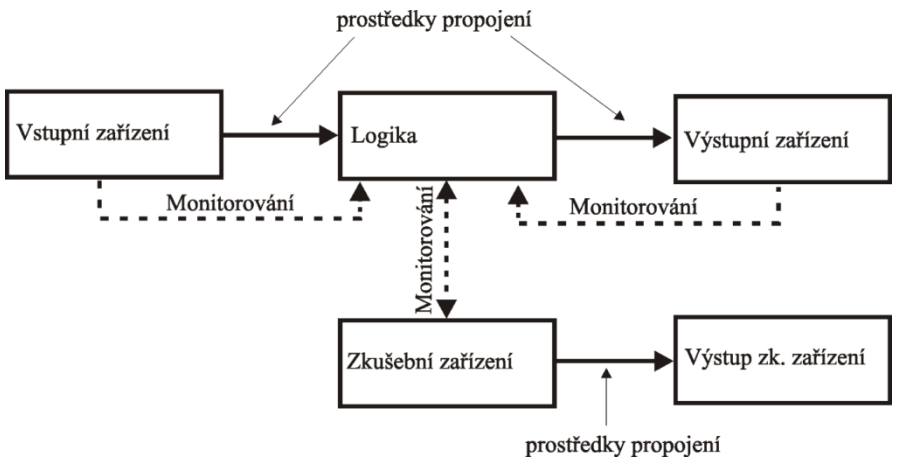
- Kategorie B PL = b;
- Kategorie 1 PL = c;
- Kategorie 2 PL = d;
- Kategorie 3 PL = d;
- Kategorie 4 PL = e.



Obrázek 5: Architektura pro kategorii B a 1

Zdroj: [6], vlastní úprava

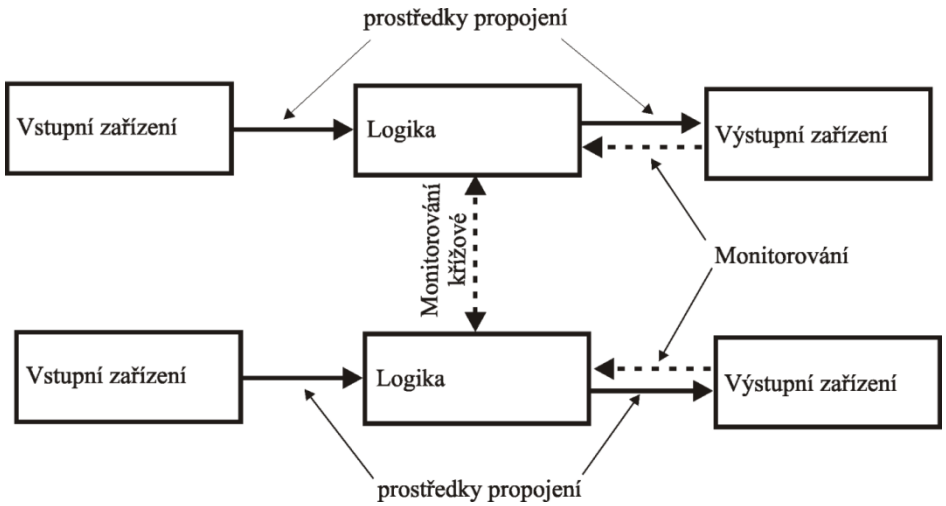
Rozdíl mezi architekturami B a 1 je pouze v použití komponent, kdy se pro kategorii 1 musí použít osvědčené komponenty.



Obrázek 6: Architektura pro kategorii 2

Zdroj: [6], vlastní úprava

Monitorování zde představuje způsob kontroly příslušného zařízení. Pod tímto názvem si můžeme představit například kontrolu pomocných kontaktů stykače nebo diagnostické testy prováděné PLC, kdy si toto PLC vyhodnocuje, zda jsou funkční vstupy a výstupy (například kontrolou deformace signálů). Křížové monitorování je způsob monitorování, kdy je zdvojena logika, například dva procesory, a ty provádí kontrolu jak vstupů a výstupů, tak samy sebe navzájem a výsledky porovnávají.



Obrázek 7: Architektura pro kategorii 3 a 4

Zdroj: [6], vlastní úprava

Rozdíl mezi architekturou kategorie 3 a 4 je pouze v diagnostickém pokrytí, kdy pro kategorii 4 je DC vysoké.

Podrobnější informace ke kategoriím a stanoveným strukturám naleznete v normě ČSN EN ISO 13849–1.

Určení vlastností PL:

Pro zjednodušený odhad PL bezpečnostní části SRP/CS nebo celého příslušného kanálu SRP/CS, uvádí norma tabulku (Tabulka 4). Bezpečnostní částí SRP/CS v tomto případě myslím například světelný závěs nebo nějaké jiné zapojení, jež má být částí bezpečnostní funkce, a u které chceme samostatně určit PL. Osvědčené bezpečnostní součástky mají PL nebo SIL již udávanou výrobcem (např. světelný závěs). Celým příslušným kanálem mám na mysli zapojení, např. tlačítko, PLC, stykač a hodnotu PL odhadujeme pro tuto architekturu zapojení. Pokud se kanál bezpečnostní funkce skládá z částí, které mají určenou hodnotu PL, můžeme celkové PL kanálu určit pomocí následující tabulky (Tabulka 5) a příslušných pravidel. Jedná se o sériové zapojení částí SRP/CS.

Pravidla pro určení úrovně PL kombinací částí SRP/CS tvořící bezpečnostní funkci:

- Zjištění nejnižší úrovně vlastností $PL_i = PL_{low}$ z jednotlivých částí SRP/CS;
- Zjištění počtu N_{low} částí SRP/CS, které dosahují PL_{low};
- Vyhledání PL v tabulce (Tabulka 5) .

Tabulka 4: Zjednodušený postup pro odhad PL SRP/CS

Kategorie	B	1	2	2	3	3	4
DC_{avg}	žádné	žádné	nízké	střední	nízké	střední	vysoké
$MTTF_d$ každého kanálu	**Úroveň vlastností PL**						
Krátká	a	-	a	b	b	c	-
Střední	b	-	b	c	c	d	-
Dlouhá	-	c	c	d	d	d	e

Zdroj: [6], vlastní úprava

Tabulka 5: Určení PL pro sériové zapojení SRP/CS

PL_{low}	N_{low}	Dosažené PL
a	**> 3**	**-**
	≤ 3	**a**
b	**> 2**	**a**
	≤ 2	**b**
c	**> 2**	**b**
	≤ 2	**c**
d	**> 3**	**c**
	≤ 3	**d**
e	**> 3**	**d**
	≤ 3	**e**

Zdroj: [6], vlastní úprava

1.2.3 Porovnání norem ČSN EN ISO 13849–1, ČSN EN 62061 a ČSN EN 954–1

Z důvodu možné volby dvou norem pro návrh bezpečnostního ovládacího zařízení, uvádím převodní tabulku mezi jejich úrovněmi bezpečnosti (PL, SIL) a kategoriemi bývalé normy ČSN EN 954–1 v tabulce (Tabulka 6). Z tabulky je patrné, že norma ČSN EN ISO 13849–1 je přímějším nástupcem ČSN EN 954–1. Normy ČSN EN ISO 13849–1 a ČSN EN 62061 se používají pro návrh bezpečnostních opatření strojních zařízení. Norma ČSN EN 62061 nabízí splnění vyšší úrovně návrhu bezpečnostního zařízení a tuto normu je vhodné, kromě návrhu bezpečnostních opatření pro strojní zařízení, použít i pro návrh bezpečnostních opatření v procesním průmyslu. Je vhodná pro oblast, kde mohou hrozit větší rizika a tím pádem i větší nebezpečí a je tedy požadavek na vyšší úroveň bezpečnostního opatření.

Tabulka 6: Porovnání úrovní (kategorií) bezpečnostních funkcí jednotlivých norem

Kategorie – ČSN EN 954–1	PL_r – ČSN EN ISO 13849–1	SIL – ČSN EN 62061
B	**a**	**-**
1	**b**	**1**
2	**c**	**1**
3	**d**	**2**
4	**e**	**3**
-	**-**	**4**

Zdroj: [5], vlastní úprava

Z tabulky (Tabulka 7) je patrné, že s normou ČSN EN ISO 13849–1 můžeme realizovat bezpečnostní funkce za využití i neelektrických technologií, kdežto norma ČSN EN 62061 se vztahuje na elektronická a elektromechanická zařízení, proto bychom dle této normy měli postupovat při návrhu řídicí jednotky. V části Příloha 4 uvádím pro doplnění formulář pro určení úrovně SIL dle normy ČSN EN 62061.

Tabulka 7: Doporučené použití ČSN EN ISO 13849–1 a ČSN EN 62061

	Technologie realizující bezpečnostní ovládací funkce	**ČSN EN ISO 13849–1**	**ČSN EN 62061**
A	Neelektrická (hydraulika, pneumatika atd.)	✔	✘
B	Elektromechanická	**až PL = e**[6]	**až SIL 3**
C	Úplná elektronika, např. programovatelná	**až PL = d**[6]	**až SIL 3**
D	A kombinovaná s B	**až PL = e**[6]	✔[7]
E	C kombinovaná s B	**až PL = d**[6]	**až SIL 3**
F	C kombinovaná s A nebo C kombinovaná s A a B	✔	✔[7]

Zdroj: [6]

1.2.4 Příklady bezpečnostních funkcí

Nouzové zastavení – nebezpečný proces musí být co nejrychleji zastaven bez vzniku dalších nebezpečí. Ovladače musí být jednoznačně identifikovatelné, dobře viditelné a snadno přístupné. Zařízení smí být uvedeno do chodu vyresetováním ovladače nouzového zastavení a následným povolením nového spuštění. Nouzové zastavení musí být nadřazeno všem ostatním funkcím a charakteristikou spadá do kategorie 0 nebo kategorie 1, viz dále.

Bezpečné zastavení – zastavení iniciované bezpečnostním zařízením (otevření ochranných krytů, překročení otáček, vstup do nebezpečné oblasti, atd.) musí uvést stroj do bezpečného stavu.

Zastavení dělíme do tří kategorií:

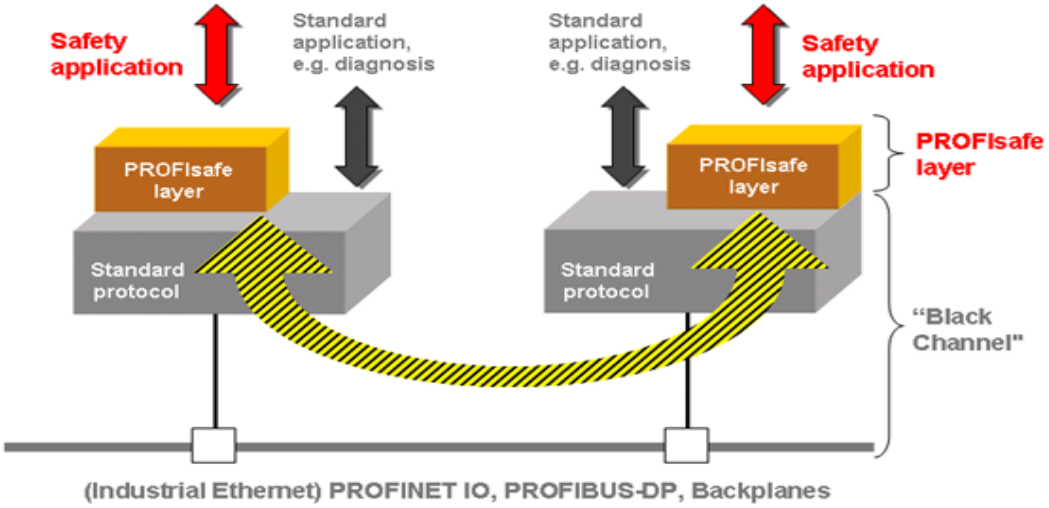
- Kategorie 0 – nekontrolované zastavení, řešení: vypnutím hlavního přívodu energie ke stroji;
- Kategorie 1 – kontrolované zastavení, řešení: nejprve uvedeme stroj do bezpečného stavu a pak vypneme hlavní přívod energie ke stroji;
- Kategorie 2 – kontrolované zastavení, řešení: uvedeme stroj do bezpečného stavu, ale hlavní přívody energie ponecháme zapnuté.

[6] Omezeno použitou architekturou
[7] Pro neelektrické části použít ČSN EN ISO 13849–1

2. ProfiSafe

V roce 1999 byla pro běžně používané průmyslové sběrnice PROFIbus a PROFInet vyvinuta specifikace, která umožňuje využití těchto sběrnic pro bezpečnostní komunikaci v průmyslu. Tato specifikace (protokol, profil) se nazývá PROFIsafe. Tento profil byl schválen a certifikován organizacemi BGIA[8] a TÜV[9].

PROFIsafe byla vyvinuta za účelem nalezení levnějšího, flexibilnějšího a komplexnějšího řešení bezpečnosti obsluhy strojů i vlastních zařízení v průmyslové automatizaci. S rozmachem elektroniky a vývojem PLC se stará hardwarová řešení zabezpečení v automatizaci např. pomocí relé, nahrazují spojením softwarové realizace s hardwarovou. PROFIsafe je vlastně přidaná aplikační vrstva (profil) k již existujícímu protokolu, jako je PROFIbus a PROFInet, ale jelikož se jedná o otevřenou specifikaci, je umožněno rozšíření i na jiné sběrnice a protokoly, například pro bezdrátové sítě. Tato nezávislost určení druhu přenosového média a standardního protokolu se v PROFIsafe specifikaci označuje jako „Black channel“ (Obrázek 8).



Obrázek 8: Ukázka principu připojení PROFIsafe aplikační vrstvy

Zdroj: [1]

Z obrázku (Obrázek 8) jasně vyplývá, že díky PROFIsafe protokolu nejsou pro zajištění bezpečnostních funkcí potřeba žádné speciální vodiče, sběrnice atd. pro zajištění bezpečnostních funkcí. Normální i bezpečnostní komunikace probíhá po té samé sběrnici a tím se snižuje

[8] BGIA je organizace zabývající se výzkumem a testováním pro Německou pojišťovnu German Social Accident.
[9] TÜV je společnost se zastoupením po celé Evropě, zabývající se inspekcí, certifikováním a testováním ve všech odvětvích průmyslu.

složitost i ekonomické náklady na zapojení. Bezpečnostní komunikace probíhá způsobem „dotaz-odpověď“, a to přináší určité bezpečnostní požadavky na protokol.

2.1 Bezpečnostní mechanismy protokolu

Consecutive number – pro detekci, zda příchozí zpráva přišla celá a ve správném pořadí;

Time-out – kontroluje, zda odpověď na dotaz přišla do stanovené doby, zda zařízení odpovídá;

Codename – zajišťuje jednoznačnost určení zařízení, pro správné určení kdo s kým komunikuje;

Data integrity – kontrola celistvosti a správnosti dat.

Následující tabulka (Tabulka 8) ukazuje, jaké chyby během přenosu dat můžeme pomocí těchto bezpečnostních opatření detekovat.

Tabulka 8: Detekce přenosových chyb pomocí bezpečnostních opatření profilu

Chyba \ Bezpečnostní opatření	Consecutive number	Time-out	Codename	Data integrity
nechtěné opakování dat	×			
ztráta dat	×	×		
parazitní data	×	×	×	
nespávné pořadí dat	×			
deformace dat				×
nepřijatelné zpoždění		×		
chyba adresování			×	
maskování (standardní data se vydávají za bezpečná)		×	×	×
opakovaná chyba paměti v přepínači	×			

Zdroj: [1], vlastní úprava

Bezpečnostní opatření probíhají tak, že každá zpráva má své pořadové číslo a přijímač kontroluje, zda tato čísla po sobě následují. Tím se snaží odhalit případnou ztrátu nebo nesprávné pořadí doručení zpráv. Přijetí zprávy vždy potvrzuje odesílateli. Požadavek na včasné doručení zprávy kontroluje tzv. „watch-dog“, jenž je vždy restartován po přijetí následují zprávy (s inkrementovaným Consecutive number). Jelikož se zde komunikuje „1:1“ (master-slave), je důležité zajistit jednoznačnost jednotlivých zařízení, aby nedocházelo k odeslání zpráv na nesprávné místo. Ošetřuje nám to bezpečnostní mechanismus Codename, což je ve skutečnosti F-adresa (bezpečnostní adresa, safety adresa) daného zařízení. Tuto adresu většinou nastavujeme a musíme dodržet rozdílnost adres jednotlivých zařízení. Celková zpráva je doplněna CRC kódem, pomocí něhož detekujeme poškozená data.

2.2 Formát PROFIsafe zprávy

PROFIsafe zpráva se skládá ze tří částí

1. Data od F I/O
2. Status/Control Byte
3. CRC kód

Rámec je znázorněn na obrázku (Obrázek 9) a je patrné, že jsou dvě možnosti délky této zprávy. Tento rozdíl ve velikosti zpráv je dán jejich použitím, tj. v jaké oblasti automatizace používáme PROFIsafe protokol. Pokud se jedná o průmyslovou automatizaci ve smyslu zajištění bezpečnosti strojů (robotů, linek), používá se kratší rámec, protože je požadavek na rychlé přenosy zpráv. U procesní automatizace je spíše požadavek na bezpečný přenos většího objemu dat, data s plovoucí řádovou čárkou a přenos dat může být tedy o trochu pomalejší.

Status/Control Byte nám udává, zda je příslušná zpráva odesílaná z master (Control) nebo slave (Status) zařízení, což je důležité pro synchronizaci komunikace.

Consecutive number není přenášen ve zprávě, ale každé zařízení má svůj vnitřní čítač a tyto čítače jsou synchronizovány právě pomocí Status/Control Byte. Správná synchronizace je kontrolována pomocí čítačů, jejichž hodnoty jsou zakomponovány v CRC.

F - I/O	Status/Control Byte	CRC (F-I/O data, F-parametr, Consecutive number)
•12 Byte •123 Byte	•1 Byte	•3 Byte •4 Byte

Obrázek 9: Struktura PROFIsafe zprávy

Zdroj: [1], vlastní úprava

Na obrázku (Obrázek 10) je znázorněna PROFIsafe vrstva pro master a slave zařízení a je zde ukázána komunikace pomocí zpráv mezi nimi.

iParametr – je soubor parametrů daných výrobcem a pro použití s PROFIbus a PROFInet tyto parametry obsahuje soubor GSD (General Station Description). Tento soubor se používá pro snadnější konfiguraci zařízení v systému.

F-Parametry – parametry důležité pro PROFIsafe vrstvu:

- F_S/D_Address
- F_WD_Time
- F_SIL
- F_iPar_CRC
- F_Par_CRC

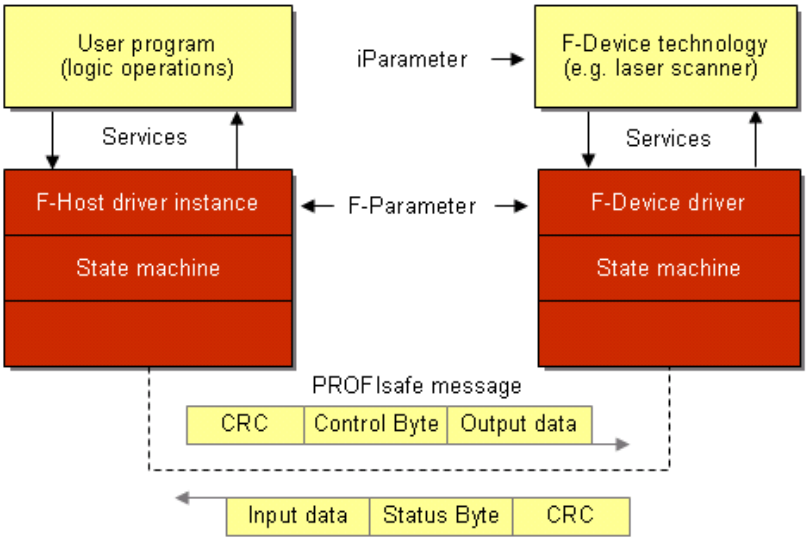
F_S/D_Address: jedinečná adresa v PROFIsafe;

F_WD_Time: hodnota watch dogu, jenž hlídá přijetí další platné zprávy [ms];

F_SIL: hodnota úrovně zabezpečení daného prvku SIL (kontroluje se s továrním nastavením);

F_iPar_CRC: zakódování iParametrů;

F_Par_CRC: zakódování F-Parametrů.



Obrázek 10: Struktura PROFIsafe vrstvy

Zdroj: [1]

PROFIsafe však není jen popis předepsané komunikace a daný protokol. PROFIsafe vyžaduje splnění požadavků na použité komponenty bezpečnostního systému dle příslušných norem daného státu. A obsahuje určitá omezení, např. u PROFInet jsme omezeni maximálně 100 směrovači v řadě a PROFIbus se nesmí větvit. Požaduje například, aby bezpečnostní zařízení splňovala normu IEC 61508.

3. Safety PLC a bezpečnostní prvky

To, že je bezpečnost v posledních letech velice diskutované a důležité téma, dokládá fakt, že všechny větší společnosti zabývající se automatizační technikou, ať řídicí částí, tak senzory, má ve své nabídce komponenty týkající se zajištění bezpečnosti obsluhy a strojů. Mezi nejznámější výrobce patří firmy jako SICK, Siemens, Rockwell, Omron, Pilz, Schneider a další. Jelikož je na katedře řídicí systém firmy Siemens, soustředím se ve své práci především na výrobky této firmy.

3.1 Safety systémy firmy Siemens

Firma Siemens má v současné době pro svůj řídicí systém Simatic S7 dvě možná řešení bezpečnostních systémů.

- **S7 Distributed Safety –** řešení zabezpečení strojních zařízení (linek, robotů, zařízení s hořáky, atd.);
- **S7 F/FH Systems** – řešení zabezpečení v procesní automatizaci, které vyžaduje vyšší odolnost proti poruchám, např. ropný a chemický průmysl. Umožňuje redundantní zapojení.

V tabulce (Tabulka 9) uvádím základní parametry těchto dvou systémů. Dalším možným řešením je využít bezpečnostních relé SIRIUS pro zajištění základních bezpečnostních funkcí.

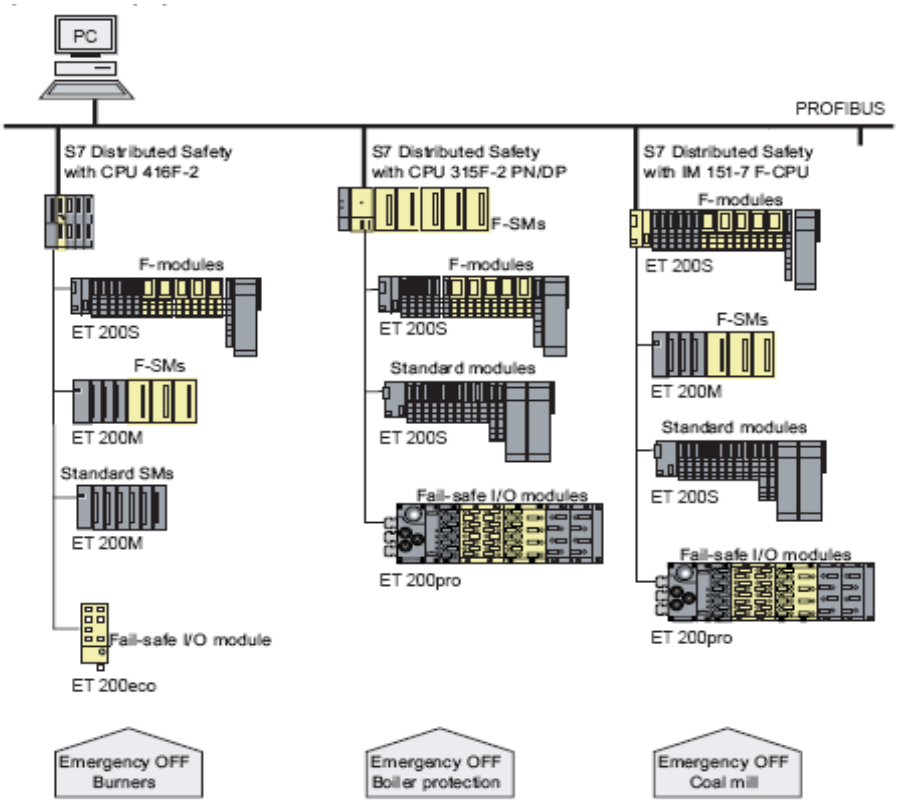
Tabulka 9: Základní vlastnosti bezpečnostních systémů firmy Siemens pro Simatic S7

Základní vlastnosti	S7 Distributed Safety	S7 F/FH Systems
Dosažitelná bezpečnostní třída	SIL3/Category 4	SIL3/Category 4
Odolnost proti chybám	NE	ANO
Využití	Bezpečnostní systém	Bezpečnostní systém odolný proti chybám
Komunikační sběrnice	PROFIBUS DP, PROFINET IO	PROFIBUS DP
Programovací jazyk	LAD, FBD	CFC
Reakce na chybu	Odpojení kanálů, F-I/O, F-CPU přechází do režimu STOP	Odpojení kanálů, F-I/O, F-CPU nepřechází do režimu STOP
Typická doba odpovědi F-Systému	100 ms až 200 ms	200 ms až 500 ms
Minimální doba odpovědi F-Systému	50 ms	100 ms
Aplikace	Ochrana zařízení, obsluhy, hořáky	Procesní automatizace, ropný průmysl

Zdroj: [9]

Základem výše uvedených systémů je tzv. Safety PLC, jedná se o bezpečnostní programovatelný automat, na kterém běží jak uživatelský program, tak i bezpečnostní program. Uživatelský program je spouštěn v organizačním bloku OB1 a bezpečnostní program běží v organizačním bloku OB35, který je volán v pevně stanovených cyklech. Bezpečnostní program přeruší vykonávání uživatelského programu, vykoná patřičné funkce a umožní pokračování uživatelského programu. PLC je možné rozšířit o standardní vstupní a výstupní karty, vstupní a výstupní bezpečnostní karty[10], jak digitální tak analogové a o karty pro speciální funkce (polohování, čítače, frekvenční měniče atd.). Tyto systémy nám umožňují jak centralizované, tak i decentralizované řízení. Dále obsahují PROFIsafe profil a umožňují komunikaci mezi bezpečnostními částmi pomocí tohoto profilu po sběrnicích PROFIbus a PROFInet[11].

Jelikož cílem práce je navržení a realizace bezpečnostního opatření pro průmyslového robota, zabývám se dále jen systémem S7 Distributed Safety a jeho součástmi. Příklad možných konfigurací tohoto systému vidíte na obrázku (Obrázek 11).



Obrázek 11: S7 Distributed Safety systém – příklady konfigurací

Zdroj: [9]

[10] Bezpečnostní karty vstupů, výstupů mívají označení F-DI, F-DO nebo se používá označení safety.
[11] Záleží, po jakých sběrnicích umožňuje PLC komunikaci.

3.2 Hardwarová konfigurace Safety PLC firmy Siemens

Hardwarová konfigurace Safety PLC se provádí stejně jako HW konfigurace standardních PLC. V programovacím prostředí SIMATIC Manager Step 7 v HW Config způsobem „drag and drop“ provedeme vložení příslušných hardwarových komponent do zvoleného „RACKu“. Jelikož nám tento systém umožňuje i decentralizované řízení, je možnost připojit komponenty pomocí sběrnice PROFIbus nebo PROFInet. Čím se však HW konfigurace Safety PLC odlišuje od standardní konfigurace běžných PLC, je nastavení potřebných vlastností CPU a bezpečnostních komponent. Dvojklikem na jednotlivé komponenty (CPU a moduly I/O) se dostaneme do karet vlastností pro zadání potřebných parametrů. Následně udávám parametry, jejichž nastavení je důležité pro vytvoření bezpečnostní aplikace.

Záložky parametrů CPU:

- **Cyclic Interrupts** – nastavení doby cyklického volání organizačního bloku OB35 obsahujícího bezpečnostní program;
- **Protection** – nastavení hesla zabezpečujícího přístup k bezpečnostnímu programu a hardwarovému nastavení. Důležité je zaškrtnutí políčka, kterým oznamujeme CPU, že obsahuje bezpečnostní program;
- **F parameters** – zde můžeme upravit rozsah rezervovaných čísel funkčních a datových bloků a nastavujeme základ PROFIsafe adresy, pro zařízení připojená pomocí sběrnice PROFIbus k tomuto zařízení. Ve většině případů lze ponechat přednastavené hodnoty.

Parametry vstupního a výstupních zařízení:

- **Operating mode** – umožňuje nastavit standardní nebo safety mód. U výstupních zařízení lze volit safety mód dle potřebné kategorie;
- **F – source_address a F – dest_address** – udávají společně PROFIsafe adresu
- **DIP switch settings** – znázorňuje nastavení DIP přepínače pro jednotlivé komponenty, je velice důležité toto nastavení dodržet;
- **Diagnostic Interrupt** – povolí odesílání diagnostických informací CPU;
- **F-monitoring time** – doba, do které musí přijít odpověď na PROFIsafe zprávu, jinak se vyhlásí chyba komunikace. Nastavený čas musí být větší než čas cyklického volání OB35;
- **Evaluation of the sensor –** způsob vyhodnocování senzorů 1 z 1 nebo 1 ze 2;
- **Sensor supply via module** – senzor je napájen z bloků vstupů, umožňuje diagnostické testy;
- **Short circuit test** – provádění testu na zjištění zkratu;

- **Group diagnostics** – odeslání diagnostických informací příslušného kanálu do CPU, pro nezapojené vstupy a výstupy nastavit jako neaktivní;
- **Type of sensor interconnection** – při dvoukanálovém zapojení určuje, zda má být vyhodnocována shoda kanálů nebo neshoda;
- **Discrepancy time** – při dvoukanálovém zapojení vyhodnocuje, zda došlo ke změně signálu do požadované doby. Při jednokanálovém zapojení je nastavena hodnota 10 ms
- **Disable light test** – provádí kontrolu výstupů, aktivní výstupy se po dobu < 1 ms vypnou (dark period) a neaktivní výstupy se po dobu < 1 ms sepnou (light period);
- **Behavior at CPU STOP** – ve standardním módu můžeme nastavit výchozí hodnotu výstupů v klidovém stavu (log. 1 nebo log. 0), v safety módu je přednastavená hodnota log. 0 (výstupy vypnuty);
- **Apply substitute value „1“** - nastavení hodnoty výstupu ve standardním módu;
- **Behavior after channel faults** - nastavujeme, zda se při chybě do bezpečného stavu nastaví pouze kanál nebo celý modul.

Jednotlivé parametry závisí na použitém modulu, moduly pak nemusí mít všechny parametry nebo naopak mohou mít nějaké navíc. Ve vlastnostech I/O modulů se nachází záložka Addresses, ve které nastavujeme hodnotu logických adres pro přístup programu k příslušným I/O modulům. V některých případech se logická adresa může shodovat s PROFIsafe adresou.

HW konfiguraci je na závěr nutné zkompilovat a uložit, poté v hierarchickém stromě projektu v záložce „Blocks“ vidíme automaticky vytvořené F-datové bloky a F-funkce pro obsluhu I/O modulů. Pokud se funkční a datové bloky nepřidají, byla provedena chyba v HW konfiguraci. Je potřeba zkontrolovat, zda je zaškrtnuto políčko na kartě vlastností CPU Protection tzn., že CPU obsahuje bezpečnostní program. Podrobný popis HW konfigurace je uveden na příkladu v příloze 6.

3.3 Programování Safety PLC firmy Siemens

Postup vytvoření bezpečnostního programu je následující. Po vytvoření hardwarové konfigurace v projektu v záložce „Blocks“ vytvoříme organizační blok OB35[12] a následně funkci FC1. Při vytváření funkce FC1 musíme kromě volitelně vyplnitelných parametrů, jako je symbolický název, vybrat položku „Create in Language“ a nastavit ji na F-CALL. Vložením volání funkce FC1 do OB35 vytvoříme rozhraní pro bezpečnostní program. Pro vlastní bezpečnostní program

[12] Pravé tlačítko myši a vybereme Insert New Object

je potřeba vytvořit funkční blok FBxx nebo další funkci FCxx. Číselné označení se nesmí shodovat s označením bezpečnostních funkčních bloků a funkcí, které obsahuje knihovna S7 Distributed Safety. Doporučuje se používat nízká čísla. Při vytváření tohoto bloku si zvolíme programovací jazyk. Povolené programovací jazyky pro bezpečnostní program jsou LVL jazyky, jako bezpečnostní programovací jazyk funkčních bloků F-FBD nebo bezpečnostní programovací jazyk žebříčkových schémat F-LAD. Po zvolení programovacího jazyka a odsouhlasení se dostaneme do programovací části, ve které vytváříme bezpečnostní program využitím certifikovaných bezpečnostních funkcí z knihovny S7 Distributed Safety, základních logických operací a reintegrace („znovu aktivování“) bezpečnostních modulů. Po vytvoření programu a jeho uložení je nutné provést jeho kompilaci. Vrátíme se do hlavního stromu projektu na záložku „Blocks“ a zde existují dva způsoby vyvolání tabulky pro kompilování programu. Dvojklikem na F-CALL funkci FC1 nebo stisknutím tlačítka pro kompilaci bezpečnostního programu[13]. Před vlastní kompilací nejprve musíme nastavit a zkontrolovat potřebné parametry v tabulce Edit F-Runtime Groups[14] :

- F-program blocks – funkční blok/funkce, která obsahuje bezpečnostní program;
- I-DB for F-program block – nastavení příslušného datového bloku pro funkční blok;
- Max. cycle time of the F-runtime in ms – monitorovací doba, do které se musí vyvolat blok OB35 a tato F-runtime group, jinak nastane chyba, hodnota musí být větší než hodnota nastavená u OB35.

Ukázka vytvoření bezpečnostního programu je uvedena na příkladu v příloze 6.

Při programování bezpečnostního programu by měl programátor dodržet následující pravidla:

- Bezpečnostní funkci v programu volat pouze jednou;
- Pokud využívá pomocné paměťové bity Mxx, tak při zápisu v bezpečnostním programu z nich ve standardním programu pouze číst a naopak.

Reintegrace:

Pokud nastane chyba komunikace nebo závada na modulu či kanálu, dojde k uvedení karty do bezpečného stavu tzv. pasivace. Po odstranění problému je však třeba uvést moduly/kanály opět do provozu a k tomuto účelu nám slouží právě reintegrace. Před uvedením postupu provedení

[13] Tlačítko je označeno na obrázku (Obrázek 33).
[14] Tabulka se při dvojkliku na funkci FC1 zobrazí automaticky, při postupu přes tlačítko kompilace safety programu je nutné v následné tabulce stisknout tlačítko F-Runtime groups.

reintegrace, uvádím v následující tabulce (Tabulka 10) důležité proměnné F-datových (bezpečnostních) bloků bezpečnostních I/O modulů:

Tabulka 10: Popis proměnných F-DB příslušné F-I/O karty

Proměnná	Funkce	Implicitně
PASS_ON	1 – povolí softwarovou pasivaci karet	0
ACK_NEC	1 – požadavek na potvrzení provedení reintegrace 0 – automatická reintegrace	1
ACK_REI	1 – potvrzení provedení reintegrace	0
PASS_OUT	Signalizace pasivované karty	1
QBAD	Signalizace chyby karty nebo kanálu	1
ACK_REQ	1 – požadavek na provedení reintegrace (signalizuje karta, pokud je chyba odstraněna)	0
DIAG	Servisní informace (Byte)	
QBAD_I_xx	Signalizace poruchy příslušného kanálu vstupního zařízení	1
QBAD_O_xx	Signalizace poruchy příslušného kanálu výstupního zařízení	1

Zdroj: [14], vlastní úprava

Pro správnou funkci je tedy nejprve nutné rozhodnout, zda se karta má automaticky reintegrovat po odstranění problému, anebo až po potvrzení operátorem. V prvním případě nastavíme hodnotu ACK_NEC příslušné karty na hodnotu log. 0, karta si sama diagnostickými testy zjistí, zda byla odstraněna příčina problému. Diagnostika trvá zhruba 30 s. V druhém případě ji ponecháme nastavenou na hodnotu log. 1. Dále popisuji postup reintegrace druhého případu. V prvním případě proběhne automaticky.

Nastavení kanálu a příslušné karty F-I/O do bezpečného stavu je signalizováno nastavením proměnné QBAD. Po odstranění závady karta vygeneruje požadavek reintegrace ACK_REQ = log. 1. Když je tento signál v log. 1, umožní nám to nastavit ACK_REI = log. 1 a provedeme reintegraci, zároveň dojde i k vynulování ACK_REQ.

3.4 S7 Distributed Safety knihovna

S7 Distributed Safety je knihovna vytvořená firmou Siemens pro vytváření bezpečnostních aplikací strojních zařízení a hořáků. Obsahuje certifikované bezpečnostní funkce. Funkce jsou rozděleny do dvou složek:

- F – System Blocks
- F – Application Blocks

F – Systém Blocks obsahuje systémové funkce například pro vnitřní kontrolu funkčnosti I/O modulů. K těmto funkcím nemá uživatel přístup.

F – Application Blocks obsahuje aplikační funkce, se kterými uživatel může pracovat. Výčet těchto funkcí uvádím v následující tabulce (Tabulka 11).

Tabulka 11: Výpis funkcí S7 Distributed Safety knihovny

Číslo F-Bloku	Název funkce	Popis
FB 179	F-SCA_I	Přepočet hodnot typu INT
FB 181	F_CTU	Vzestupný čítač
FB 182	F_CTD	Sestupný čítač
FB 183	F_CTUD	Obousměrný čítač
FB 184	F_TP	Časovač vytvářející impuls
FB 185	F_TON	Časovač zpožděného sepnutí
FB 186	F_TOF	Časovač zpožděného rozepnutí
FB 187	F_ACK_OP	Bezpečnostní potvrzení z operátorského panelu
FB 188	F_2HAND	Obouruční ovládání, monitorování
FB 189	F_MUTING	Potlačení bezpečnostní funkce
FB 190	F_1oo2DI	Vyhodnocení 1 ze 2
FB 211	F_2H_EN	Obouruční ovládání, monitorování s potvrzením
FB 212	F_MUT_P	Paralelní potlačení bezpečnostní funkce
FB 215	F_ESTOP1	Nouzové zastavení až do kategorie 1
FB 216	F_FDBACK	Zpětnovazebné monitorování
FB 217	F_SFDOOR	Monitorování bezpečnostních dveří
FB 219	F_ACK_GL	Potvrzení pro reintegraci všech F-I/O v F-Runtime group
FB 223	F_SENDDP	Odeslání dat přes PROFIbus (velikost 2 INT)
FB 224	F_RCVDP	Přijmutí dat z PROFIbus (velikost 2 INT)
FB 225	F_SENDS7	Odeslání dat přes S7 spojení (PROFInet)
FB 226	F_RCVS7	Přijmutí dat přes S7 spojení (PROFInet)
FC 174	F_SHL_W	Posun 16 bitů vlevo
FC 175	F_SHR_W	Posun 16 bitů vpravo
FC 176	F_BO_W	Převod z typu BOOL na WORD
FC 177	F_W_BO	Převod z typu WORD na BOOL
FC 178	F_INT_WR	Zápis hodnoty INT do F-DB nepřímým adresováním
FC 179	F_INT_RD	Čtení hodnoty INT z F-DB nepřímým adresováním

Zdroj: [14], vlastní úprava

3.5 Bezpečnostní prvky

Safety PLC

Bezpečnostní PLC, jak jsem uvedl již v úvodu této kapitoly, je PLC, které umožňuje vykonávání standardního uživatelského programu a bezpečnostního programu zároveň. Snižuje tím náklady na připojování dalšího externího zařízení. Modulární typy PLC se skládají z bezpečnostní řídicí jednotky (CPU), standardních vstupů, výstupů, bezpečnostních vstupů a výstupů a dalších speciálních karet. Bezpečnostní prvky připojíme k bezpečnostním vstupům a výstupům a následně pomocí certifikovaných bezpečnostních funkcí, které jsou součástí softwaru Safety PLC, danou bezpečnostní funkci realizujeme. Safety PLC bývají certifikované až do kategorie 4 dle ČSN EN 954–1 (úroveň PL = e dle ČSN EN ISO 13849–1, SIL 3 dle ČSN EN 62061).

Bezpečnostní relé:

Relé vykonávající bezpečnostní funkce jako např. nouzové zastavení, monitorování ochranných krytů a možnosti připojení optických ochranných prvků typu světelné závory atd. U optických prvků umožňují tzv. funkci muting. Této funkci se podrobněji věnuji v podkapitole Světelné závory a závěsy. Výběr parametrů záleží na vybraném bezpečnostním relé, ale hlavní funkcí je vždy nouzové zastavení. Výrobci certifikují při správném zapojení relé splnění požadavků až do kategorie 4 dle ČSN EN 954–1.

Bezpečnostní spínače:

- Polohové spínače
- Magnetické spínače
- Nožní spínače
- Dvouruční ovládací pulty
- Tlačítka nouzového vypnutí

Tyto vstupní komponenty jsou konstruovány z důvodů snížení rizika poruchy s vyšším důrazem na zpracování, např. mají zdvojené pohyblivé kontaktní můstky a mají minimálně 2 kontakty. Správným zapojením lze splnit požadavky až kategorie 4 dle ČSN EN 954–1. Výrobci garantují splnění požadovaných norem pro daný výrobek.

Světelné závory, závěsy a mříže:

Optoelektronické bezpečnostní prvky (závory, závěsy a mříže) slouží k ochraně pracovního prostoru a používají se k ochraně prstů, rukou a vstupu osob či materiálu do nebezpečné oblasti. Principem je vysílání a příjem laserového paprsku. Pokud je paprsek přerušen, je signalizována

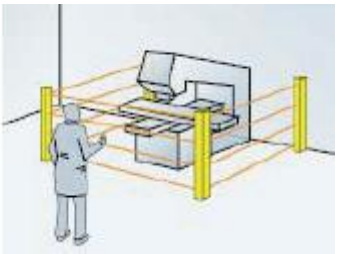
chyba. Prvky mají několik důležitých parametrů, kterými jsou například rozlišovací schopnost, dosah, počet paprsků, doba odezvy a především jakou bezpečnostní kategorii splňují dle ČSN EN 954–1 (případně dle jiné normy). Obvykle splňují kategorii 2 nebo kategorii 4 dle ČSN EN 954–1. Lze je umístit jak svislým tak vodorovným způsobem, případně některé typy naklonit. Pomocí těchto prvků lze, pokud to umožňuje daný typ, realizovat funkce muting a blanking.

- Muting – dočasné přerušení ochranné funkce
- Blanking – zaclonění paprsků (pevné, pohyblivé, omezené rozlišení)

Využití světelných závor, závěsů a mříží dle jejich parametrů:

- Rozlišovací schopnost – 14 – 50 mm ochrana prstů a rukou;
- Rozlišovací schopnost – 50 – 90 mm ochrana vstupu vodorovným zapojením do úrovně stehen;
- Rozlišovací schopnost – větší jak 90 mm ochrana vstupu do nebezpečné oblasti svislým zapojením.

Příklad využití světelné závory:



Obrázek 12: Příklad použití světelných závor

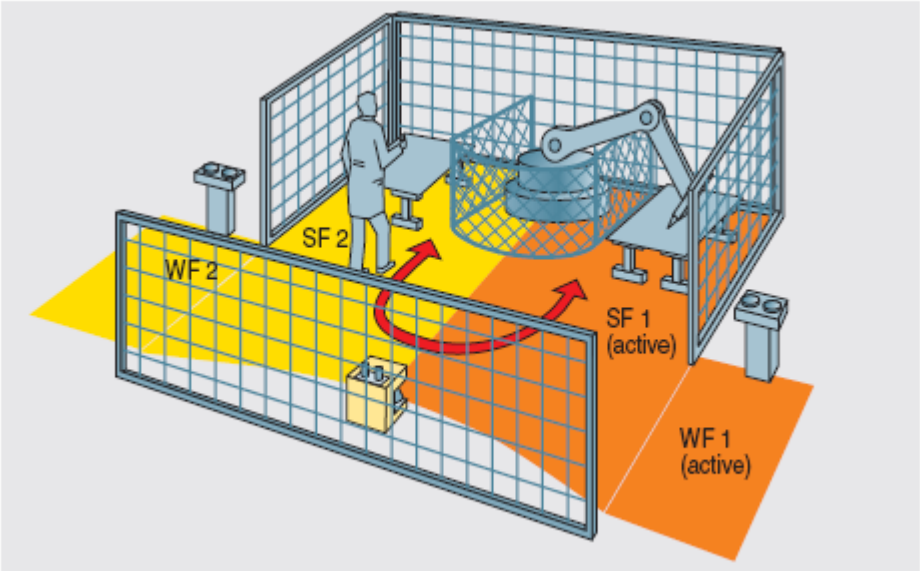
Zdroj: [12]

Laserový skener:

Optoelektronický bezpečnostní prvek používaný ke kontrole bezpečného prostoru. Laserový skener umožňuje hlídat prostor buď ve svislém, nebo vodorovném směru, a lze s ním hlídat stacionární prostor nebo ho připevnit na mobilní zařízení. Principem senzoru je vysílání laserového paprsku a jeho následné snímání. Při zjištění objektu v nebezpečné zóně (ochranném poli) dojde k nastavení bezpečných výstupů na senzoru. Starší typy senzorů měly jednu bezpečnostní zónu (cca 4m) a jednu výstražnou zónu (cca 15m)[15]. Dnešní skenery např. firmy SICK mohou mít až 8 ochranných polí a 8 výstražných polí. Jednotlivá pole, jejich rozměry a typ, lze pomocí příslušného softwaru upravovat. Skenery pracují s maximálním úhlem cca 190°

[15] Parametry skeneru závisí na vybraném typu a výrobci. Ochranná zóna vyvolá nouzové zastavení, výstražná zóna může spustit například výstražný signál nebo omezit pohyb stroje.

při 60 ms až 120 ms odezvě, umožňují také připojení na sběrnice jako například PROFIbus. Skenery splňují kategorii 3 dle ČSN EN 954–1. Obrázek 13 znázorňuje použití laserového skeneru, ochranné zóny jsou označeny SF 1,2 a varovné zóny jsou označeny WF 1,2.



Obrázek 13: Příklad použití laserového skeneru

Zdroj: [13]

4. Návrh bezpečnostního zařízení pro Robotické pracoviště v učebně K09

V učebně K09 je instalován starý svářecí robot OJ-10RS vyrobený firmou ZTS Detva, v současné době na něm probíhají úpravy, nové rozvody kabeláže, výměna řídicí jednotky apod. Myslím si, že budoucí využití robota pro studijní účely bude případně spíše manipulátor, než svařovací robot. Pro seznámení zde uvádím základní parametry robota a pro představu i jeho fotografii (Obrázek 14). Parametry jsou získány od firmy Rapčan, která v současné době provozuje totožného robota. Originální dokumentace k dispozici bohužel není. Samotným řízením a technickými parametry robota se zabývali v minulosti ve svých bakalářských pracích pánové Bc. Matěj Šiška (zdroj:[15]) a Bc. Václav Sedláček (zdroj:[16]).

Obrázek 14: Robot OJ-10RS

Robot 0J-10RS:

Jedná se o pětiosého robota, kde každá osa je poháněna samostatným stejnosměrným motorem. Na přiloženém obrázku (Obrázek 14) jsou zaznamenány jednotlivé motory pro dané osy a v tabulce příslušné parametry robota. Motor M1 slouží k rotaci robota kolem základny a jeho pracovní rozsah je 260°, motor M2 obsluhuje první rameno (na obrázku označeno R1) s pracovním rozsahem ±40°, motor M3 obsluhuje druhé rameno (označeno R2) motory M4, M5 obsluhují „zápěstí“ robota. Parametry jsou převzaty z dokumentace robota stejného typu, provozovaného firmou Rapčan na Slovensku.

Tabulka 12: Parametry robota OJ-10RS a motorů

Parametry Robota	**Hodnota**	**Poznámka**
Max. nosnost	10 kg	
Max. moment setrvačnosti	0,78 kg·m^2	
Max. statický moment	19,62 Nm	
Počet stupňů volnosti	5	
Hmotnost robota	295 kg	
Krytí	IP 43	
Pracovní teplota	+ 5 °C až 40 °C	
Druh prostředí	obyčejné	
Střední technická životnost	40 000 hod	
Rychlost rotace základny	1,3 rad/s (75,1°/s)	Max. okamžité rychlosti
Vodorovná rychlost koncového bodu	0,8 m/s	Max. okamžité rychlosti
Vertikální rychlost koncového bodu	1,0 m/s	Max. okamžité rychlosti
Parametry motorů	**Hodnoty**	**Poznámka**
SRD 350	I_n = 7,4 A; U_n = 62 V; P = 350 W; n = 3000 min^{-1}	Motory M1,2,3
SRD 80	I_n = 13,6 A; U_n = 15,5 V; P = 100 W; n = 3000 min^{-1}	Motory M4, M5

Zdroj: [15], vlastní úprava

V současné době je k řízení robota využívaná řídicí jednotka MARS 8b (Obrázek 15), vyrobená firmou PIKRON s.r.o. Řídicí jednotka v sobě sdružuje jak řídicí část tak i výkonovou. Lze s ní řídit až osm stejnosměrných motorů s možností připojit stejný počet IRC čidel pro určení polohy a rychlosti řízených motorů. Umožňuje připojit limitní spínače a další digitální senzory. K řídicí

jednotce lze připojit analogový joystick se třemi potenciometry, pomocí RS 232/485 nadřazené PC, lze využít sběrnici CAN[16] pro připojení nadřazeného řídicího systému, anebo rozhraní SPI či I^2C pro připojení dalších periférií a jednotka obsahuje vstup pro připojení tlačítka nouzového zastavení.

Obrázek 15: Řídicí jednotka MARS 8b firmy PIKRON

Zdroj: PIKRON s.r.o.

4.1 Analýza rizik

Postup provádění analýzy rizik strojního zařízení je uveden v kapitole 1.2.2 na obrázku (

Obrázek 1).

Při konstrukci strojního zařízení se konstruktér snaží splnit všechny požadavky na bezpečné zařízení dané v současné době normou ČSN EN ISO 12100. Po zkonstruování robota provedeme

[16] Implementována je varianta CAN HighSpeed

analýzu jeho mezních hodnot a případných nebezpečí a rizik dle ČSN EN ISO 14121. Existuje několik metod analýzy rizik, které jsou uvedené v příslušných normách. Jednou z nejpoužívanějších metod je metoda „Co se stane, když …“ tzv. W-I metoda. Postupem u této metody je kladení si otázek, co se stane při poruše nebo co se může stát při vstupu osoby do nebezpečného prostoru a jejich následné zodpovězení. Standardně při vývoji stroje provádíme analýzu pro různé fáze stroje (pracovní režim, údržba, instalace, demontáž). Pokud jsou zjištěna přetrvávající rizika, nebezpečné situace, je úkolem toto riziko odstranit, případně snížit. Nejprve konstrukční úpravou nebo přidáním ochranného krytu. Pokud nedojde k odstranění rizika nebo jeho snížení na přijatelnou úroveň, pokusíme se ho odstranit přidáním přídavného ochranného opatření, například bezpečnostního ovládacího zařízení. Pokud ani poté nedokážeme riziko přijatelně snížit, je třeba informovat obsluhu v návodu k použití.

Jelikož v rámci projektu máme k dispozici robota, který je již postaven, orientuji se tedy na úpravu bezpečnosti. Posuzuji a navrhuji dodatečná ochranná opatření pro zajištění bezpečnosti obsluhy robota pro normální provoz stroje a pro fázi údržby.

Potencionální nebezpečí identifikovaná u robota umístěného v učebně[17]:

1. Možnost naražení, stlačení, případně zachycení osoby robotem;
2. Ostré hrany a rohy ochranných krytů;
3. Nestabilita robota vzhledem k jeho dynamickým vlastnostem (především brzdění);
4. Nebezpečí dotyku živých a neživých elektrických části;
5. Nebezpečí vytvářené elektromagnetickým polem;
6. Nebezpečný pohyb robota, možný náraz do pracovního stolu.

Ostré hrany a rohy byly sice konstrukčně odstraněny vhodnými kryty již výrobcem, přesto je nutná pravidelná kontrola pevného připevnění, jelikož často dochází k jejich uvolňování.

Pospojováním a následným zemněním je provedena ochrana před dotykem neživých částí, živé části jsou před dotykem chráněny izolací a zakrytováním. Jako ochrana proti nadproudu je použito vhodné jištění.

V případě nestability robota, například při brzdění, je robot uzpůsoben k pevnému připevnění k podložce deskou s předvrtanými otvory pro šrouby. Jelikož konstruktér robota znal dynamické vlastnosti zařízení, přizpůsobil tomu i následnou konstrukci připojovací desky a velikosti otvorů dimenzované pro šrouby s dostatečnými rozměry k upevnění robota na požadované místo. Dnes

[17] Nebezpečí byla určena dle přílohy A normy ČSN EN 1050, předchůdce normy ČSN EN ISO 14121, která je v platnosti od května roku 2008 a normy ČSN EN ISO 10218 – Roboty pro výrobní prostředí.

je robot upevněn pouze dvěma šrouby, a to je nedostatečné, ačkoliv je robot provozován zhruba na polovinu svého výkonu a při použití tlačítka total stop se robot jen neznatelně zakymácí. Je však potřebné provést zabezpečení robota pro jeho plný pracovní výkon, z čehož vyplývá připevnit robota šrouby o průměru daném montážními otvory v desce a s pevností šroubu minimálně 8,8 dle normy ISO 898.

Při návrhu robota jsou použity komponenty, které splňují požadavky na vyzařování a odolnost proti elektromagnetickému rušení. Pokud je provedena elektroinstalace dle doporučení výrobce, předpokládá se splnění požadavků příslušných norem.

Omezení pracovního prostoru a zabránění případného nárazu robota do pracovního stolu se zajišťuje softwarově, kdy programátor vymezuje pracovní prostor. Pokud dojde přeci jen ke srážce, tak řídicí jednotka vyhodnocuje proudové zatížení jednotlivých os a pokud dojde k překročení limitního proudu, je robot zastaven.

Nebezpečí stlačení nebo naražení robotem nelze řešit konstrukční úpravou. V tomto případě je zde požadavek na vymezení bezpečného prostoru a bezpečnostní funkci, která tento prostor bude zajišťovat proti vniknutí a dále je nutné vhodně rozmístit tlačítka nouzového zastavení stroje tzv. total stop.

4.2 Návrh bezpečnostního opatření

Při návrhu bezpečnostního opatření ovládacího obvodu postupujeme dle schématu popsaném v kapitole 1.2.2 (Obrázek 2). Navrhované bezpečnostní funkce pro rizika stlačení nebo naražení obsluhy tohoto robota jsou:

- Funkce nouzového zastavení při stisknutí nouzového tlačítka;
- Funkce bezpečného zastavení při narušení bezpečné vzdálenosti od robota.

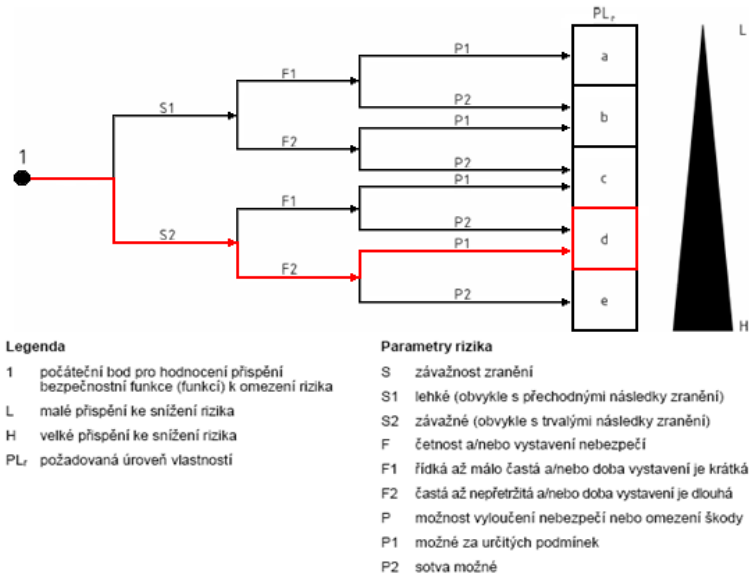
Norma ČSN EN ISO 10218 udává požadavky na vlastnosti bezpečnostního řídicího systému robota. Bezpečnostní části musí být konstruovány dle kategorie architektury 3 normy ČSN EN ISO 13849–1, pokud analýza rizik nezjistí požadavek na kategorii architektury 2 nebo 4. Rozmístění a použití bezpečnostních prvků může být různé, následný výpočet je uvažován pro rozmístění prvků dle obrázku (Obrázek 44) v Příloze 7.

Určení PL_r:

Pro jednotlivé bezpečnostní funkce nyní musíme stanovit jejich požadovanou úroveň vlastností PL_r. Pro obě tyto funkce dostáváme stejný graf a tedy totožnou hodnotu PL_r. Proto zde uvedu postup určení PL_r pouze pro funkci nouzového zastavení.

Při zjišťování hodnoty PL_r postupujeme dle návodu, který je popsán v kapitole 1.2.2 (Obrázek 3). V našem případě je tedy cesta následující. Pro snadnější pochopení je vše vyznačeno na obrázku (Obrázek 16).

Vycházíme z bodu 1 a nejprve musíme udělat rozhodnutí, zda robot může způsobit zranění s vážnými následky kategorie S2 nebo zranění, která nemají trvalý charakter a lze je snadno ošetřit, tedy kategorie S1. Protože robot může způsobit při svém pohybu úder do hlavy a následný pád může mít fatální dopad na zdraví obsluhy robota, zvolíme větev S2. V dalším kroku, četnost vystavení nebezpečí, je rozhodnutí složitější. Při předpokladu využití robota tak na 14 hodin týdně v rámci výuky, bych zvolil parametr F1. Avšak na základě požadavku na trvání bezpečnostní funkce a s ohledem na velmi pravděpodobné větší množství studentů v okolí robota a jejich možnému vstupu do nebezpečného prostoru, musíme zvolit parametr F2. U volby možnost vyloučení nebezpečí určujeme variantu P1, protože pohyb robota je vidět a tím se nebezpečí dá vizuálně předpokládat a nebezpečnému prostoru se vyhnout. Provoz robota je signalizován žárovkou umístěnou na rameni robota R2. Výsledkem je tedy PL_r = d.

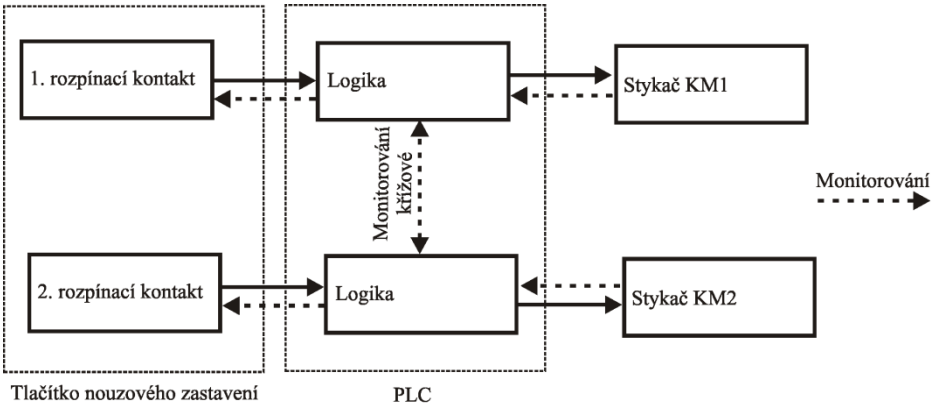


Obrázek 16: Určení PL_r robota

Zdroj: [6], vlastní úprava

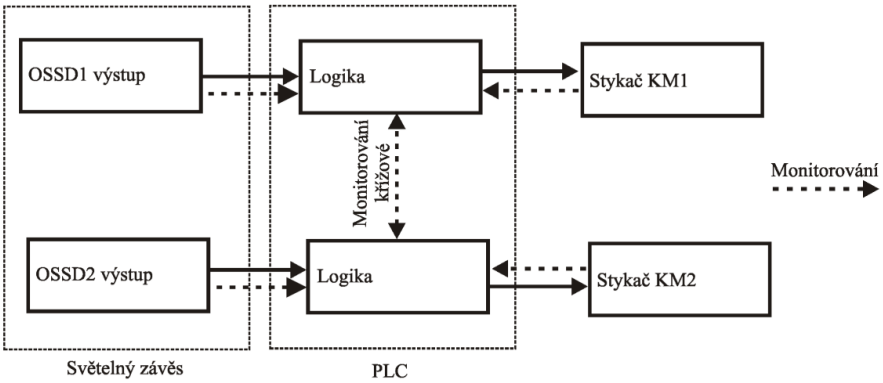
Konstrukce bezpečnostní funkce:

Vezmeme-li v úvahu normu ČSN EN ISO 10218 a tabulku pro zjednodušené určení hodnoty PL z kapitoly 1.2.2 (Tabulka 4), jeví se jako nevhodnější pro obě bezpečnostní funkce kategorie architektury 3. Bezpečnostní funkci nouzového zastavení vytvoříme zapojením tlačítka nouzového zastavení, PLC a sériovou kombinací dvou stykačů (Obrázek 17), které odpojují přívod energie do výkonové části řídicí jednotky, čímž dojde k zastavení robota.

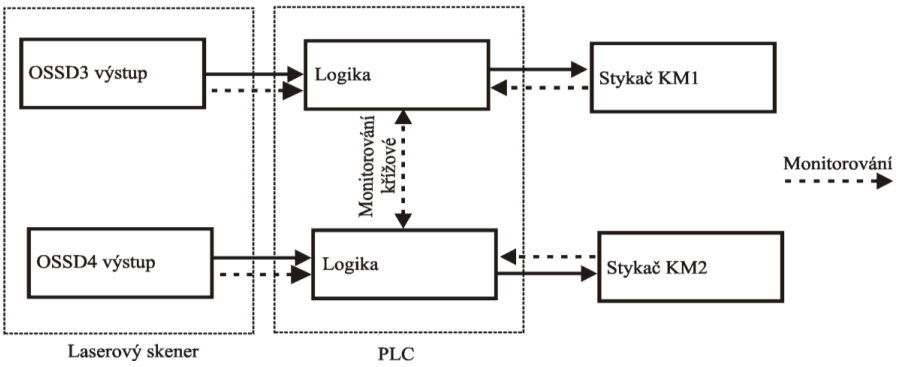


Obrázek 17: Bezpečnostní funkce nouzového zastavení

Bezpečnostní funkci bezpečného zastavení realizuji pomocí světelného závěsu, stejného PLC i stykačů (Obrázek 18). Jelikož světelný závěs vyhodnotí pouze vstup do nebezpečné zóny, ale ne stálou přítomnost osoby v nebezpečné zóně, připojíme k PLC i laserový skener (Obrázek 19). V případě vhodného umístění robota by stačil pro tuto funkci pouze laserový skener, ale, jak je znázorněno na obrázcích v Příloze 7, dosah robota je i mimo viditelné plochy laserového skeneru. Jedním z řešení je použití výše uvedené kombinace či zajištění ochrany míst, na které skener „nevidí“, oplocením.



Obrázek 18: Bezpečnostní funkce bezpečné zastavení, světelný závěs



Obrázek 19: Bezpečnostní funkce bezpečné zastavení, laserový skener

Určení PL jednotlivých bezpečnostních funkcí:

Při určení PL jednotlivých funkcí budeme postupovat způsobem, kdy určíme parametry PL jednotlivých bloků a pomocí tabulky pro zjednodušené určení úrovně PL (Tabulka 4, kapitola 1.2.2) určím celkové PL jednotlivého bloku. Pro určení celkového dosaženého PL kanálu využiji tabulku pro určení úrovně PL sériového zapojení (Tabulka 5, kapitola 1.2.2).

Funkce nouzového zastavení:

Vstupní blok: tlačítko nouzového zastavení M22-PV/KC02/IY, výrobce Moeller

$B_{10d} = 1.10^5$ – udává výrobce

- **Výpočet $MTTF_d$:** použité rovnice R.1, R.2 a R.3 z kapitoly 1.2.2

Hodnoty pro výpočet $MTTF_d$ musíme odhadnout úvahou. Robot se bude využívat 14 hodin týdně a odhadem 60 dnů v roce. Robota budou používat studenti, z čehož lze usoudit použití nouzového tlačítka 5x za vyučovací hodinu. Výsledné parametry potřebné pro výpočet:

h_{op} = 14 hod/den;

d_{op} = 60 dnů za rok;

t_{cyklu} = 1,5 hod/5 = 1080 s/cyklus

$B_{10d} = 1 \cdot 10^5$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{cyklu}} = \frac{60 \cdot 14 \cdot 3600}{1080} = 2800\ cyklů/rok$$

$$T_{10d} = \frac{B_{10d}}{n_{op}} = \frac{1 \cdot 10^5}{2800} = 35,7\ let$$

$$MTTF_d = \frac{B_{10d}}{0,1 \cdot n_{op}} = \frac{T_{10d}}{0,1} = \frac{35,7}{0,1} = 357\ let$$

Za pomoci tabulky rozřazení hodnoty $MTTF_d$ do kategorií (Tabulka 2, kapitola 1.2.2) snadno zjistíme danou kategorii $MTTF_d$. Všechny hodnoty $MTTF_d$ vyšší jak 100 let jsou považovány za hodnotu 100 let. Pro provoz tlačítka nouzového zastavení v délce trvání 35,7 let je tedy předpokládaná střední doba do nebezpečné poruchy „dlouhá“. Při sériovém zapojení více tlačítek nouzového zastavení je nutné provést korekci výpočtu $MTTF_d$ dle rovnice R.4 kapitola 1.2.2.

- **Určení DC:** Tuto hodnotu určíme z tabulky v Příloze 1 pro vstupní zařízení. PLC vykonává křížové monitorování vstupů s testy případného zkratu. Proto určím hodnotu DC 99 %. A následně z tabulky pro určení kategorie DC (Tabulka 3, kapitola 1.2.2) určíme DC = „vysoké“.
- **Určení CCF:** požadované hodnoty získáme vyplněním formuláře z Přílohy 2. Vyplněný formulář se nachází v Příloze 8. Je splněn požadavek na opatření proti chybám se společnou příčinou.

Ze zjištěných výsledků a následným určením hodnoty PL z tabulky pro zjednodušené určení hodnoty PL (Tabulka 4, kapitola 1.2.2) nám vychází hodnota PL pro vstupní zařízení PL = d.

Logický blok: PLC 315F – 2DP s bezpečnostními vstupy a výstupy firmy Siemens.

Výrobce zaručuje úroveň vlastností PL = e.

Výstupní blok: sériově zapojené stykače DILM12-01 firmy Moeller a stykač LC1 K1201B7 firmy Schneider Electric.

- **Výpočet hodnoty $MTTF_d$:**

Jelikož se jedná o dva různé výrobky a dvoukanálové zapojení, vyřešíme nejprve každý kanál samostatně a pak určíme celkovou hodnotu $MTTF_d$ pro celé zapojení.

DILM12-01 (24VDC): B_{10d} – $1,3 \cdot 10^6$ udává výrobce

LC1 K1201B7: B_{10d} – $2 \cdot 10^6$, převzato z normy ČSN EN ISO 13849-1 pro obecný stykač

Pro výpočet vezmeme totožné hodnoty jako při výpočtu $MTTF_d$ u vstupního zařízení. Pouze změníme hodnotu t_{cyklu}, protože stykač budeme ovládat funkcí bezpečné zastavení a předpokládané zastavení robota bude častější. Odhadujeme tak 10x za vyučovací hodinu.

h_{op} = 14 hod/den;

d_{op} = 60 dnů za rok;

t_{cyklu} = 1,5 hod/10 = 540 s/cyklus

Pro stykač firmy Moeller:

$B_{10dDILM} = 1{,}3 \cdot 10^6$

$$\boldsymbol{n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{cyklu}} = \frac{60 \cdot 14 \cdot 3600}{540} = 5600\ cyklů/rok}$$

$$\boldsymbol{T_{10d} = \frac{B_{10dDILM}}{n_{op}} = \frac{1{,}3 \cdot 10^6}{5600} = 232{,}1\ let}$$

$$\boldsymbol{MTTF_{dDILM} = \frac{B_{10dDILM}}{0{,}1 \cdot n_{op}} = \frac{T_{10d}}{0{,}1} = \frac{232{,}1}{0{,}1} = 2321\ let}$$

Pro stykač Schneider Electric:

$B_{10dLC1} = 2 \cdot 10^6$

$$\boldsymbol{n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600 s/h}{t_{cyklu}} = \frac{60 \cdot 14 \cdot 3600}{540} = 5600\ cyklů/rok}$$

$$\boldsymbol{T_{10d} = \frac{B_{10dLC1}}{n_{op}} = \frac{2 \cdot 10^6}{5600} = 357{,}1\ let}$$

$$\boldsymbol{MTTF_{dLC1} = \frac{B_{10dLC1}}{0{,}1 \cdot n_{op}} = \frac{T_{10d}}{0{,}1} = \frac{357{,}1}{0{,}1} = 3571\ let}$$

Pro určení hodnoty $MTTF_d$ celého zapojení dosadíme do rovnice R.5 z kapitoly 1.2.2.

$$MTTF_d = \frac{2}{3}\left(MTTF_{dDILM} + MTTF_{dLC1} - \frac{1}{\frac{1}{MTTF_{dDILM}} + \frac{1}{MTTF_{dLC1}}}\right) =$$

$$= \frac{2}{3}\left(2321 + 3571 - \frac{1}{\frac{1}{2321} + \frac{1}{3571}}\right) = 2990{,}2\ let$$

$MTTF_d$ = 2990,2 let => „dlouhá“.

- **Určení DC:** Tuto hodnotu určíme z tabulky v příloze 1 pro výstupní zařízení. PLC vykonává křížové monitorování výstupů s příslušnými diagnostickými testy a provádíme monitorování stykačů pomocí jejich rozpínacích kontaktů. DC má z tohoto důvodu hodnotu 99 % => DC = „vysoké“. Diagnostické testy výstupů PLC jsou nastaveny pro kategorii SIL 2 a ta odpovídá PL = d.
- **Určení CCF:** požadované hodnoty získáme vyplněním formuláře z Přílohy 2. Vyplněný formulář se nachází v Příloze 8. Je splněn požadavek na opatření proti chybám se společnou příčinou.

Ze zjištěných výsledků a následným určením hodnoty PL z tabulky (Tabulka 4) nám vychází hodnota PL pro výstupní zařízení PL = d.

Určení PL pro celou bezpečnostní funkci nouzového zastavení:

Podle tabulky pro určení PL sériového zapojení (Tabulka 5, kapitola 1.2.2) určíme hodnotu PL pro celou bezpečnostní funkci ze znalosti PL jednotlivých bloků funkce.

PL_{low} = d;

N_{low} = 2;

Dosažené PL pro celou funkci: PL = d.

Určení PL pro funkci bezpečného zastavení, zapojení dle obrázku (Obrázek 18)**:**

Zde je výpočet jednodušší. Jako vstupní zařízení je použit světelný závěs C4000 Standard firmy SICK. Při dodržení zapojení daného výrobcem garantuje výrobce PL = e.

Z předchozího výpočtu funkce nouzového zastavení máme zjištěno PL = e pro PLC a PL = d pro zapojení stykačů. Provedu-li postup podle tabulky (Tabulka 5), je dosažené PL = d.

Určení PL pro funkci bezpečného zastavení, zapojení dle obrázku (Obrázek 19)**:**

Určení dosaženého PL zjistíme stejným způsobem jako pro zapojení se světelným závěsem. V tomto případě se liší pouze hodnota PL laserového skeneru S3000 Standard, u něhož výrobce garantuje při správném zapojení hodnotu PL = d. Hodnoty PL pro PLC a kombinace stykačů zůstávají stejné.

Opět dle tabulky (Tabulka 5) má dosažené PL hodnotu PL = d.

Ve všech případech jsme splnili požadovanou hodnotu $PL \geq PL_r$.

Při faktické realizaci však narážíme na problém, kdy řídicí jednotka byla navrhována dle praktických znalostí výrobce a nebyla zohledněna možnost připojení externího bezpečnostního systému s požadovanou úrovní vlastností PL = d a vyšší. Využitelným bezpečnostním vstupem pro řídicí jednotku je vstup tlačítka nouzového zastavení. Tímto vstupem přímo ovládáme stykač zapojený ve výkonové části řídicí jednotky. Kdy rozpojením napájecího obvodu ovládací cívky stykače dojde k rozpojení silových kontaktů stykače. Jelikož pomocné kontakty tohoto stykače využívá řídicí jednotka pro vlastní monitorování, nelze je využít pro monitorování bezpečnostním systémem. Z těchto důvodů splňujeme daným zapojením kategorii architektury 1 a pomocí tabulky pro zjednodušené určení PL (Tabulka 4, kapitola 1.2.2) zjistíme, že s touto kategorií můžeme, při splnění určitých podmínek především hodnoty $MTTF_d$ = „dlouhá“ celého kanálu, dosáhnout nejvýše PL = c. Tato úroveň je nedostatečná. Problém lze odstranit přidáním sériové kombinace stykačů před řídicí jednotku nebo přímo do řídicí jednotky. Přikláním se k přidání kombinace stykačů do řídicí jednotky a navrhoval bych případnou úpravu řídicí jednotky dle normy ČSN EN 62061 pro bezpečnostní úroveň alespoň SIL 2 nebo dle konstrukčních zásad normy ČSN EN ISO 13849–1 tak, aby umožňovala dosažení úrovně alespoň PL = d. Pokud by došlo k úpravám řídicí jednotky, představoval bych si tyto vstupy bezpečnostních funkcí:

- Vstup nouzového zastavení – přímé ovládaní stykačů ve výkonové části;
- Vstup bezpečného zastavení – možnost zastavení pomocí kategorie 1 pro funkci zastavení. Kdy je stroj nejprve zastaven a pak jsou odpojeny stykače ve výkonové části;
- Vstup údržby – funkce omezení rychlosti pohybu a výkonu robota, kdy údržba může bypassem obejít bezpečnostní prvky světelných závěsů a laserového skeneru a následně se pohybovat v nebezpečném prostoru při chodu robota. Monitorování rychlosti robota by prováděla vlastní řídicí jednotka.

V současné době lze pouhým přidáním stykačů do výkonové části realizovat pouze funkci nouzového zastavení. A to jak připojením nouzových tlačítek, tak i připojením laserového skeneru, případně světelného závěsu na případně přidanou stykačovou kombinaci.

Určení bezpečné vzdálenosti:

Návrhem bezpečnostních funkcí a zařízení proces zabezpečování nekončí. Je nutné tyto bezpečnostní prvky umístit do správné bezpečné vzdálenosti. Základní vzorec pro určení bezpečné vzdálenosti při přiblížení je (dle normy ČSN EN 999):

$$S = v \cdot T + C \qquad \text{(R.7)}$$

S – bezpečná vzdálenost (mm);

v – rychlost přiblížení lidského těla nebo jeho části (mm/s);

T – čas doběhu stroje (s);

C – přídavná konstanta v závislosti na použitém ochranném prvku (mm).

Při použití ochranného optického prvku, například světelného závěsu, musíme určit hodnotu konstanty C.

- Pro rozlišení světelného závěsu do 40 mm podle rovnice (R.8);
- Pro rozlišení světelného nad 40mm je hodnota konstanty C = 850 mm.

$$C = 8 \cdot (d - 14) \qquad \text{(R.8)}$$

d – rozlišení optického prvku, d < 40 mm

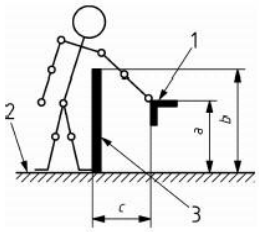
Normou stanovena rychlost přiblížení člověka chůzí je 1600 mm/s.

Dobu doběhu robota určíme měřením délky trvání zastavení robota na podnět bezpečnostního prvku. Nasčítávají se zde hodnoty vlastního doběhu robota a doba, než dokáže bezpečnostní systém zareagovat. V současné době se musí provést měření na robotu a doporučuji, po konzultaci s p. Ing. Pavlem Píšou, provést toto měření pro nejhorší možný případ, tj. když dojde ve chvíli požadavku vypnutí robota k odtržení napájecího kabelu k příslušným motorům robota. Řídicí jednotka po vyhodnocení poklesu napětí ve výkonové části provede brzdění robota. Není ale zajištěno brzdění, pokud by došlo právě k odtržení kabelu vedeného z řídicí jednotky k motoru. Motory nemají instalovány jiné brzdné mechanismy, které by ošetřily tento případ.

Pouze bezpečná vzdálenost od zařízení v rámci přiblížení osoby může být nedostatečná. Musíme zajistit i splnění bezpečné vzdálenosti v rámci dosahu do nebezpečného prostoru. Požadavky na výšku bezpečnostního opatření a minimální bezpečnou vzdálenost nám udává norma ČSN EN ISO 13857. Na obrázku (Obrázek 20) vidíme, jak určit potřebné parametry pro vyhledání výšky bezpečnostního prvku a určení bezpečné vzdálenosti, které následně zjistíme z tabulky na obrázku (Obrázek 21). Robot má největší vodorovný dosah ve výšce chapadla 1420 mm (viz Příloha 9). Jelikož chceme ochránit dospělého člověka, mít co nejkratší bezpečnou vzdálenost a také se dostat na co nejnižší cenu, zvolíme dle obrázku (Obrázek 21) a = 1600 mm a b = 1800 mm. Následně určíme z tabulky na tomto obrázku hodnotu bezpečné vzdálenosti. V našem případě nám tedy vychází c = 500 mm.

4.2.2 Dosah přes ochranné konstrukce

Obrázek 2 ukazuje bezpečnou vzdálenost pro dosah přes ochrannou konstrukci.



Legenda

a	výška nebezpečného prostoru	1	nebezpečný prostor (nejbližší bod)
b	výška ochranné konstrukce	2	referenční rovina
c	vodorovná bezpečná vzdálenost k nebezpečnému prostoru	3	ochranná konstrukce

Obrázek 20: Určení dosahových parametrů

Zdroj: ČSN EN ISO 13857¨

4.2.2.1 Hodnoty

4.2.2.1.1 K určení odpovídajícího rozměru (rozměrů) výšky nebezpečného prostoru, výšky ochranných konstrukcí a vodorovné bezpečné vzdálenosti k nebezpečnému prostoru musí být použity hodnoty uvedené v tabulce 1. Pokud je zde malé riziko (viz 4.1.2), které vzniká od nebezpečného prostoru, musí být jako minimální hodnoty použity hodnoty uvedené v tabulce 1.

Hodnoty uvedené v tabulce 1 nesmí být interpolovány. Proto tedy, pokud známé hodnoty *a*, *b* nebo *c* leží mezi dvěma hodnotami v tabulce 1, musí být použita větší bezpečná vzdálenost nebo vyšší ochranná konstrukce nebo změna ve výšce (vyšší nebo nižší) nebezpečného prostoru.

Příloha A uvádí příklady použití tabulek 1 a 2.

Tabulka 1 – Dosah přes ochrannou konstrukci – Malé riziko

Rozměry v milimetrech

Výška nebezpečného prostoru[b] *a*	Výška ochranné konstrukce[a] *b*								
	1 000	1 200	1 400	1 600	1 800	2 000	2 200	2 400	2 500
	Vodorovná bezpečná vzdálenost k nebezpečnému prostoru *c*								
2 500	0	0	0	0	0	0	0	0	0
2 400	100	100	100	100	100	100	100	100	0
2 200	600	600	500	500	400	350	250	0	0
2 000	1 100	900	700	600	500	350	0	0	0
1 800	1 100	1 000	900	900	600	0	0	0	0
1 600	1 300	1 000	900	900	500	0	0	0	0
1 400	1 300	1 000	900	800	100	0	0	0	0
1 200	1 400	1 000	900	500	0	0	0	0	0
1 000	1 400	1 000	900	300	0	0	0	0	0
800	1 300	900	600	0	0	0	0	0	0
600	1 200	500	0	0	0	0	0	0	0
400	1 200	300	0	0	0	0	0	0	0
200	1 100	200	0	0	0	0	0	0	0
0	1 100	200	0	0	0	0	0	0	0

[a] Ochranné konstrukce o výšce nižší než 1 000 mm nejsou uvedeny, protože tyto ochranné konstrukce nedostatečně omezují pohyb těla.

[b] Pro nebezpečné prostory nad 2 500 viz 4.2.1.

Obrázek 21: Určení bezpečné vzdálenosti před nebezpečným dosahem

Zdroj: ČSN EN ISO 13857

Manuál pro rychlé určení bezpečné vzdálenosti existuje nejen pro optické bezpečnostní prvky, ale samozřejmě také i pro pevné oplocení. Zde bezpečná vzdálenost závisí na rozměrech štěrbin daného oplocení. Tabulku uvádím na následujícím obrázku (Obrázek 22).

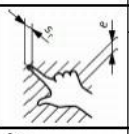
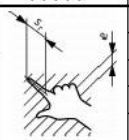
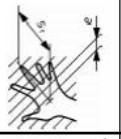
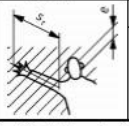
Tabulka 4 uvádí bezpečné vzdálenosti s_r pro pravidelné otvory pro osoby ve věku 14 roků a starší.

Rozměr otvoru e odpovídá straně čtvercového otvoru, průměru kruhového otvoru a nejužšímu rozměru štěrbinového otvoru.

Pro otvory > 120 mm musí být použity bezpečné vzdálenosti podle 4.2.2.

Tabulka 4 – Dosah skrz pravidelné otvory – Osoby ve věku 14 roků a starší

Rozměry v milimetrech

Část těla	Znázornění	Otvor	Bezpečná vzdálenost s_r		
			Štěrbina	Čtverec	Kruh
Špička prstu		$e \leq 4$	≥ 2	≥ 2	≥ 2
		$4 < e \leq 6$	≥ 10	≥ 5	≥ 5
Celý prst až ke kořenu		$6 < e \leq 8$	≥ 20	≥ 15	≥ 5
		$8 < e \leq 10$	≥ 80	≥ 25	≥ 20
Ruka		$10 < e \leq 12$	≥ 100	≥ 80	≥ 80
		$12 < e \leq 20$	≥ 120	≥ 120	≥ 120
		$20 < e \leq 30$	≥ 850[a)]	≥ 120	≥ 120
Paže až po ramenní kloub		$30 < e \leq 40$	≥ 850	≥ 200	≥ 120
		$40 < e \leq 120$	≥ 850	≥ 850	≥ 850
Zesílené rozhraní uvnitř tabulky znázorňuje, která část těla je omezena velikostí otvoru.					

[a)] Jestliže je délka štěrbinového otvoru ≤ 65 mm, palec omezuje vniknutí a bezpečná vzdálenost může být snížena na 200 mm.

Obrázek 22: Určení bezpečné vzdálenosti – pevné oplocení

Zdroj: ČSN EN ISO 13857

Je zřejmé, že při aplikaci robota musíme dodržet tu největší minimální bezpečnou vzdálenost a ostatní požadavky na bezpečnostní prvky.

Přidáním potřebných bezpečnostních prvků dojde ke snížení pracovních míst a průchodnosti prostoru v okolí robota. Je to patrné z obrázků v příloze 7. Proto doporučuji zvážit umístění robota do jiné části učebny.

4.3 Návrh konfigurace a bezpečnostního programu pro bezpečnostní systém zabezpečující robota v učebně K09

V následujícím textu popisuji konfiguraci zabezpečovacích komponent, pokud by bylo zvoleno řešení z obrázku (Obrázek 44, Příloha 7) s využitím PLC firmy Siemens, světelným závěsem C4000 firmy SICK, laserovým skenerem S3000 Standard firmy SICK a tlačítek nouzového zastavení například firmy Moeller. Předpokládám úpravu řídicí jednotky dle předcházející kapitoly tj. vložení dvou sériově zapojených stykačů do výkonové části řídicí jednotky. Orientační blokové schéma zapojení naleznete na obrázku (Obrázek 23), podrobnější schéma zapojení je uvedeno v příloze 10. Jedná se pouze o předpoklad, protože se uvažuje o přestavbě

učebny K09 a zatím je umístění robota neznámé. V konfiguraci se předpokládá použití těchto prvků příslušných firem:

Siemens:

- Zdroj napětí 24V DC 5A;
- PLC – CPU 315F-2DP (6ES7 315–6FF01-0AB0);
- Komunikační karta – ET200M (6ES7 153–2BA00-0XB0);
- Modul DI/DO – SM 326 DI (6ES7 323 – 1BH01 – 0AA0);
- Přepěťová ochrana – Safety Protector;
- Modul F-DI – SM 326F DI24xDC24V (6ES7 326–1BK00-0AB0);
- Modul F-DO – SM 326F DO10xDC24V/2A (6ES7 326–2BF01-0AB0).

SICK:

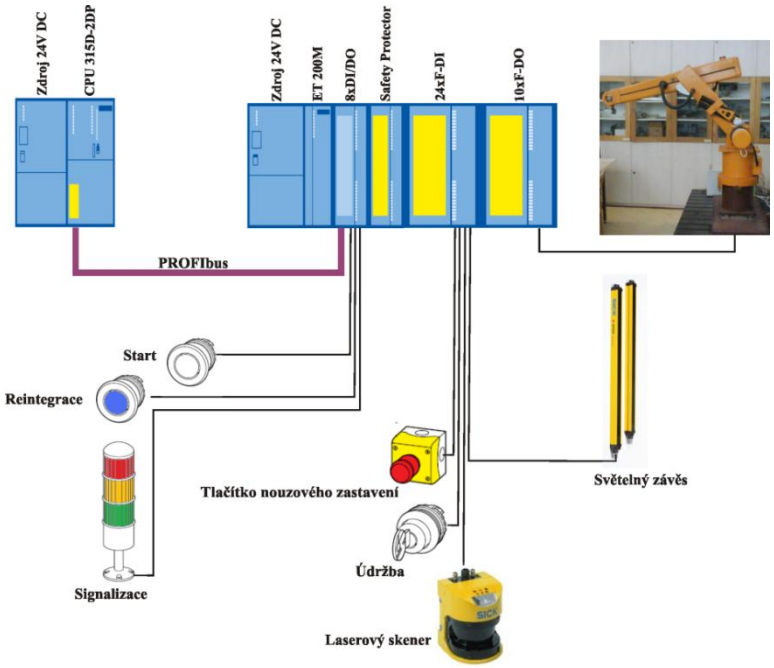
- Laserový skener – S3000 standard[18];
- Světelný závěs – C4000 Standard[17].

Moeller:

- Tlačítko nouzového zastavení – M22-PV/KC02/IY;
- Tlačítka Start a Reintegrace – příslušná sestava tlačítka bez aretace;
- Tlačítko Obsluha – sestava tlačítka ovládaného klíčem;
- Signální sloupek.

Jedná se o decentralizované řízení, kdy z bezpečného místa obsluhy ovládáme vstupy a výstupy zapojené v blízkosti robota. Při zapojení je důležité dodržet požadavky jednotlivých výrobců komponent a oddělení bezpečnostních modulů Siemens Safety Protectorem od standardních modulů. Safety Protector je přepěťová ochrana bezpečnostních modulů.

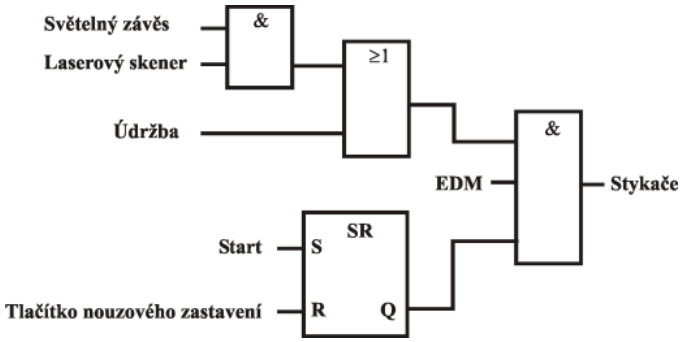
[18] Přesný typ nutno konzultovat s výrobcem, světelný závěs navrhuji C40S-1804CA010



Obrázek 23: Orientační blokové zapojení

Zdroj: SICK,Siemens, Moeller, vlastní úprava

Na následujícím schématu (Obrázek 24) je naznačen princip bezpečnostního programu. Robota lze spustit pouze po stisknutí tlačítka Start, musí být ale splněny určité podmínky. Především musí být splněna podmínka nestisknutého tlačítka nouzového zastavení. Dalšími podmínkami je nenarušení prostoru kontrolovanými laserovým skenerem a světelným závěsem. Tuto podmínku lze obejít tlačítkem pro údržbu. Toto tlačítko musí být příslušně zabezpečeno, nejlépe použít tlačítko ovládané klíčem. Poslední z funkcí, které musíme splnit, je vlastní kontrola funkce stykače pomocí pomocných kontaktů stykače tzv. EDM. K rozepnutí příslušných stykačů dojde i při vyhodnocení závady na Safety PLC nebo jeho příslušenství. V tomto případě je karta výstupů automaticky pasivována. Tlačítko Reintegrace slouží k obnovení funkce bezpečnostních karet po odstranění závady tzv. reintegraci. Tato reintegrace musí být součástí bezpečnostního programu.



Obrázek 24: Princip safety programu

Na obrázcích (Obrázek 44, Obrázek 45, Příloha 7) jsou zobrazeny varianty navrženého bezpečnostního opatření obsluhy. Jednotlivé varianty mají své výhody a nevýhody. Společnou nevýhodou je snížení průchodnosti učebny a snížení počtu pracovních míst. U varianty s oplocením je problém vlastní instalace, kdy dle mne není možné instalovat oplocení na lavici s dostatečnou pevností, aby nedošlo při nárazu robota do oplocení k jeho zborcení a následném možném riziku úrazu osoby za oplocením. Proto jsem se přiklonil k variantě s využitím optického plotu. Kdy v době nečinnosti robota je možnost využít, jinak zablokované pracovní místo. Vzdálenost bezpečnostních prvků určíme až po zjištění doby doběhu robota. Při pro nás nepříznivém výsledku a následném zjištění nemožnosti instalace těchto opatření, bude nutné omezit výkon a tím pádem i rychlost robota na bezpečnou mez a signalizovat, že robot je v běhu. Nejvhodnějším řešením by však bylo přemístění robota do jiné části učebny.

Závěr

Zabezpečení strojního zařízení a jeho obsluhy je v průmyslu obvyklý a nutný požadavek. Využívají se k tomu dostupné bezpečnostní komponenty, které jsou dnes již běžně k dostání u různých výrobců. Výrobci zaručují, při dodržení jejich podmínek, splnění určité bezpečnostní kategorie. Problematika bezpečnosti je poměrně složitá záležitost, a aby se člověk stal odborníkem v této problematice, znamená to nepřetržité a dlouhé studium především norem a požadavků na bezpečnost. Jedná se o práci, která s sebou nese velkou zodpovědnost za správnost návrhu a provedení bezpečnostních opatření.

Cílem této diplomové práce bylo zorientování se v problematice bezpečnosti a poté navrhnout bezpečnostní opatření pro robotické pracoviště v učebně K09 na katedře řídicí techniky s využitím Safety PLC, které je k dispozici na této katedře. A toto PLC zprovoznit.

Návrh bezpečnostního opatření robotického pracoviště je prováděn v souladu s normou ČSN EN ISO 13849–1: Bezpečnost strojních zařízení. Která udává požadavky na přídavný bezpečnostní systém, v tomto případě na použité Safety PLC firmy Siemens. V práci je navrženo bezpečnostní opatření zobrazené na obrázku (Obrázek 44) přílohy 7. Toto opatření má i své nedostatky, a to především ve snížení průchodnosti a snížení počtu pracovních míst v učebně. Problematická se jeví i instalace kvůli blízkosti dveří k lavicím. Proto bych se přikláněl k přemístění robota do jiné části učebny. Pokud to nebude možné a nebude možná ani instalace oplocení nebo světelného závěsu, je nutné omezit hardwarově pohyb robota, aby se nedostal do situace, která je zobrazena na obrázku (Obrázek 44, Příloha 7). Současně omezit výkon, rychlost robota a jeho pohyb signalizovat zvukově i pomocí signalizačního majáku.

Pro správnou realizaci bezpečnostních funkcí je však potřeba provést i úpravu řídicí jednotky tak, aby obsahovala bezpečnostní vstupy pro externí bezpečnostní systém a splňovala bezpečnostní požadavky normy ČSN EN 62061, případně konstrukční požadavky na správnou realizaci bezpečnostních funkcí dle normy ČSN EN ISO 13849–1 alespoň do úrovně PL = d.

Pro další práci na robotu bych doporučil nejprve provést výměnu všech kabelů a zastaralých součástí, například jako součást semestrálního projektu. Následně po úpravě řídicí jednotky provést důkladnou identifikaci robota a především zjištění jeho dynamických parametrů. Poté po vhodném umístění robota pomocí této práce realizovat bezpečnostní funkce na zajištění bezpečnosti obsluhy tohoto robota.

Literatura

[1]Profibus International: http://www.profisafe.net

[2] PROFIsafe: PROFIBUS for Functional Safety: http://www.profibus.com/pb/profibus/safety/

[3] PROFIsafe Technology and Application - System Description: http://www.profibus.com/pall/meta/downloads/article/02232/

[4]Seznam technických norem: http://seznam.normy.biz/

[5] Siemens, Safety Integrated System Manual, 5.Edition, Order No. 6ZB5 000-0AA02-0BA1

[6] ČSN EN ISO 13849-1, Část 1: Všeobecné zásady pro konstrukci, 2007

[7] IEC 60812, Analysis Techniques for System Reliability, 2006

[8] ČSN EN 62061, 2005

[9] Siemens, Safety Engineering in SIMATIC S7 System Manual, 04/2006, A5E00109529-05

[10] Siemens, Automation System S7-300 Fail-Safe Signal Modules Manual, A5E00085586-08

[11] Siemens, S7-300 CPU 31xC and CPU 31x, Technical Specifications Manual, 12/2006

A5E00105475-07

[12] Siemens, Prezentace Safety Integrated TIA na dosah

[13] Siemens, Short Catalog Safety Integrated 2007, Order No. E86060-K1005-B101-A2-7600

[14] Siemens, S7 Distributed Safety - Configuring and Programming Manual, A5E00747650-03

[15] Šiška M.: Průmyslový robot RSP 01 – nadřazené řízení, Bakalářská práce 2007, ČVUT

[16] Sedláček V.: Průmyslový robot RSP 01 – základní řízení, Bakalářská práce 2007, ČVUT

[17] Paleček M., et al.: Postupy a metodiky analýz a hodnocení rizik pro účely zákona č. 353/1999 Sb., o prevenci závažných havárií, VÚBP Praha 2000

[18] Kubíček L.: Bezpečnostní funkce pro Simatic S7 300, Bakalářská práce 2007, ČVUT

[19] ČSN EN 1050, 2001

[20] ČSN EN ISO 10218-1, Část 1: Robot, 2007

[21] SICK, Guidelines Safe Machinery Six steps to a safe machine, 8007988/2008-06-26

[22] Dieterle G., Pelikán F.: Prezentace Bezpečnostní management dle ČSN EN ISO 13849-1:2006, SICK 2007

[23] Dieterle G., Pelikán F.: Bezpečnostní management dle ČSN EN 62061:2005, SICK 2007

[24] Dieterle G., Pelikán F.: Porovnání / Použití / FAQ's ČSN EN ISO13849-1 vs. ČSN EN 62061, SICK 2007

[25] Nařízení vlády ze dne 21. dubna 2008 o technických požadavcích na strojní zařízení, Sbírka zákonů č. 176 / 2008

[26] Nařízení vlády ze dne 9. prosince 2002, kterým se stanový technické požadavky na strojní zařízení, Sbírka zákonů č. 24 / 2003

Příloha 1 – Příklady diagnostických pokrytí DC

Originální tabulky lze nalézt ve zdroji: [6]

Tabulka 13: Odhad diagnostického pokrytí pro vstupní zařízení

Opatření	DC [%]
Vstupní zařízení	
Stimulace cyklické zkoušky dynamickou změnou vstupních signálů	90
Věrohodná kontrola, např. použití nuceně mechanicky vedených vypínacích a zapínacích kontaktů	99
Křížové monitorování vstupních signálů bez dynamické zkoušky	0 – 99[19]
Křížové monitorování vstupních signálů s dynamickou zkouškou tehdy, pokud zkraty nejsou detekovatelné (při násobném I/O)	90
Křížové monitorování vstupních signálů a mezivýsledků uvnitř logiky a časové a logické softwarové monitorování chodu programu a detekce statických závad a zkratů (při násobném I/O)	99
Nepřímé monitorování (např. monitorování tlakovým spínačem, elektrické monitorování polohy pohonů)	0 – 99[20]
Přímé monitorování (např. elektrické monitorování polohy řídicích ventilů, monitorování elektromechanických zařízení nuceně mechanicky vedenými prvky)	99
Detekce závady procesem	0 – 99[21]
Monitorování některých charakteristik senzoru (reakční doba, rozsah analogových signálů, odpor, kapacita atd.)	60

[19] Záleží na frekvenci změny signálu během použití
[20] Závisející na použití
[21] Závisející na aplikaci, není samostatně dostatečné pro úroveň vlastností PL = e

Tabulka 14: Odhad diagnostického pokrytí Logika

Opatření	DC [%]
Logika	
Nepřímé monitorování (např. monitorování tlakovým spínačem, elektrické monitorování polohy pohonů)	90 – 99[22]
Přímé monitorování (např. elektrické monitorování polohy řídicích ventilů, monitorování elektromechanických zařízení nuceně mechanicky vedenými prvky)	99
Monitorování jednoduché dočasné logiky (např. čítač času jako časovací jednotka, kde jsou spouštěcí body v programu logiky)	60
Časové a logické monitorování logiky časovací jednotkou, kde zkušební zařízení provádí kontroly věrohodnosti chování logiky	90
Samočinné zkoušky spuštění k detekci latentních závad v částech logiky (např. paměť programu, údajů, vstupních/výstupních bran, rozhraní)	90[23]
Kontrola reakční schopnosti monitorovacího zařízení (např. časovací jednotky) hlavním kanálem při spuštění nebo kdykoliv je požadována bezpečnostní funkce nebo kdykoliv to vnější signál vyžaduje pomocí vstupních zařízení	90
Dynamický princip (všechny součásti logiky jsou požadovány ke změně stavu ZAPNUTO-VYPNUTO-ZAPNUTO v době, kdy je požadována bezpečnostní funkce, např. blokovací obvod realizovaný pomocí relé)	99
Neproměnná paměť: označení jednoho slova (8 bitů)	90
Neproměnná paměť: označení jednoho slova o dvojnásobné délce (16 bitů)	99
Proměnná paměť: Zkouška RAM použitím zálohovaných údajů, např. příznaků, značek, konstant, časovačů a křížového porovnávání těchto údajů	60
Proměnná paměť: kontrola čitelnosti a psací schopnosti použitých paměťových buněk údajů	60
Proměnná paměť: monitorování RAM modifikovaným Hammingovým kódem nebo samočinnou zkouškou RAM (např. Abraham)	99
Jednotka zpracování: samočinná zkouška pomocí software	60 – 90
Jednotka zpracování: kódované zpracování	90 – 99
Detekce závady procesem	0 – 99[24]

[22] Závisející na aplikaci.
[23] Závisející na zkušební technice.
[24] Závisející na aplikaci, samostatně toto opatření není dostatečné pro úroveň vlastností PL = e.

Tabulka 15: Odhad diagnostického pokrytí pro výstupní zařízení

Opatření	DC [%]
Výstupní zařízení	
Monitorování výstupu jedním kanálem bez dynamické zkoušky	0 – 99[25]
Křížové monitorování výstupů bez dynamické zkoušky	0 – 99[26]
Křížové monitorování vstupních signálů s dynamickou zkouškou bez detekce zkratů (pro násobné I/O)	90
Křížové monitorování vstupních signálů a mezivýsledků uvnitř logiky a časové a logické softwarové monitorování chodu programu a detekce statických závad a zkratů (při násobném I/O)	99
Zálohovaná zastavovací dráha bez monitorování pohonu	0
Zálohovaná zastavovací dráha s monitorováním jednoho z pohonů buď logikou, nebo zkušebním zařízením	90
Zálohovaná zastavovací dráha s monitorováním pohonů buď logikou, nebo zkušebním zařízením	99
Nepřímé monitorování (např. monitorování tlakovým spínačem, elektrické monitorování polohy pohonů)	90 – 99[27]
Detekce závady procesem	0 – 99[28]
Přímé monitorování (např. elektrické monitorování polohy řídicích ventilů, monitorování elektromechanických zařízení nuceně mechanicky vedenými prvky)	99

Další odhady diagnostického pokrytí jsou k dispozici v IEC 61508–2.

[25] Závisí na tom, jak často je aplikací měněn signál.
[26] Závisí na tom, jak často je aplikací měněn signál.
[27] Závisející na aplikaci.
[28] Závisející na aplikaci, samostatně toto opatření není dostatečné pro úroveň vlastností PL = e.

Příloha 2 – Formulář opatření proti poruchám CCF

Číslo	Opatření proti CCF	Počet bodů
1	Oddělení/segregace	
	Fyzické oddělení mezi jednotlivými dráhami signálu: - Oddělení u vodičů/potrubí; - Dostatečné vzduchové a povrchové vzdálenosti na deskách s plošnými spoji	15
2	Diverzita	
	Jsou použity různé technologie/konstrukce nebo fyzikální principy, například: - První kanál programovatelná elektronika a druhý kanál pevně spojen; - Druh iniciace; - Tlak a teplota; Měření vzdálenosti a tlaku: - Digitálně a analogově; Součásti různých výrobců;	20
3	Konstrukce/použití/zkušenosti	
	Ochrana proti přetlaku, přepětí, nadproudu atd.	15
	Jsou použity osvědčené součásti.	5
4	Posouzení/analýza	
	Jsou k vyloučení CCF v konstrukci uvažovány výsledky režimu poruchy a analýzy účinku.	5
5	Způsobilost/zácvik	
	Byli konstruktéři/údržbáři zacvičeni k pochopení příčin a následků poruch CCF	5
6	Prostředí	
	Zamezení kontaminace a elektromagnetická kompatibilita (EMC) proti CCF podle příslušných norem.	25
	Ostatní vlivy – odolnost proti relevantním vlivům prostředí (teplota, vibrace, rázy, vlhkost).	10
	Opatření pro vyloučení CCF, která nejsou uvedená ve formuláři[29]	
	Celkový počet dosažených bodů – více jak 65b včetně = splněno	

[29] Lze obodovat opatření, která nejsou uvedena ve formuláři, ale jsou využívána. Nutno dopsat tato opatření do dokumentace.

Příloha 3 – Přehled kategorií

Tabulka 16: Přehled kategorií a jejich požadavků

Kat.	Požadavky kategorie	Systém chování	Zásada používaná k dosažení bezpečnosti	$MTTF_d$ každého kanálu	DC_{avg}	CCF
B	SRP/CS a/nebo jejich ochranná zařízení, stejně jako jejich součásti, musí být navrženy, vyrobeny, voleny, namontovány a kombinovány podle relevantních norem tak, že mohou odolávat očekávaným vlivům. Musí být použity základní bezpečnostní zásady.	Výskyt závady může vést ke ztrátě bezpečnostní funkce	Hlavně charakterizována volbou součásti	Krátká až Střední	žádné	-
1	Musí být splněny požadavky kategorie B a použity osvědčené bezpečnostní součásti a osvědčené bezpečnostní zásady.	Výskyt závady může vést ke ztrátě bezpečnostní funkce, ale pravděpodobnost výskytu je menší než v kategorii B	Hlavně charakterizována volbou součásti	Dlouhá	žádné	-
2	Musí být splněny požadavky kat. B a musí být použity osvědčené bezpečnostní zásady. Bezpečnostní funkce musí být kontrolována ve vhodných intervalech ovládacím systémem stroje.	Výskyt závady může vést ke ztrátě bezpečnostní funkce mezi kontrolami. Ztráta bezpečnostní funkce je detekována kontrolou.	Hlavně charakterizována strukturou	Krátká až Dlouhá	Nízké až Střední	≥ 65b
3	Musí být splněny požadavky kat. B a musí být použity osvědčené bezpečnostní zásady. Bezpečnostní části musí být navrženy tak, aby jednotlivá závada v jakékoliv části nevedla ke ztrátě bezpečnostní funkce. A pokud to bude „rozumně“ možné byla jednotlivá závada detekována.	Vyskytne-li se jednotlivá závada, bezpečnostní funkce je vždy zachována. Některé ale ne všechny závady jsou detekovány. Nahromadění nedetekovaných závad může vést ke ztrátě bezpečnostní funkce	Hlavně charakterizována strukturou	Krátká až Dlouhá	Nízké až Střední	≥ 65b
4	Musí být splněny požadavky kat. B a musí být použity osvědčené bezpečnostní zásady. Bezpečnostní části musí být navrženy tak, aby jednotlivá závada v jakékoliv části nevedla ke ztrátě bezpečnostní funkce a jednotlivá závada byla detekována při nebo před nejbližší bezpečnostní funkcí, ale pokud není tato detekce možná, pak nahromadění nedetekovaných závad nesmí vést ke ztrátě bezpečnostní funkce.	Vyskytne-li se jednotlivá závada, bezpečnostní funkce je vždy zachována. Detekce nahromaděných závad snižuje pravděpodobnost ztráty bezpečnostní funkce (vysoké DC) Závady budou detekovány dostatečně včas, aby bylo zamezeno ztrátě bezpečnostní funkce	Hlavně charakterizována strukturou	Dlouhá	Vysoké, včetně nahromadění závad	≥ 65b

Zdroj: [6], vlastní úprava

Příloha 4 – příklad formuláře pro odhad SIL

Tabulka 17: Formulář pro odhad SIL

Odhad rizika a bezpečnostní opatření

Produkt: _____
Vydal: _____
Datum: _____

Černá oblast = Požadovaná bezpečnostní opatření
Šedá oblast = Doporučená bezpečnostní opatření

Č. dokumentu
Část:

☐ Předběžný odhad rizika
☐ Mezilehlý odhad rizika
☐ Následný odhad rizika

Následky	Závažnost Se	Class CI 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Četnost a doba, Fr		Pravděpodobnost výskytu nebezp., Pr		Vyvarování se Av	
Smrt, ztráta oka nebo paže	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hodina	5	Velmi vysoká	5		
Trvalé, ztráta prstů	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <= den	5	Pravděpodobná	4		
Přechodné, lékařská péče	2			OM	SIL 1	SIL 2	>1den - <= 2týd	4	Možná	3	Nemožné	5
Přechodné, první pomoc	1				OM	SIL 1	> 2týd. - <= 1rok	3	Výjimečná	2	Možné	3
							> 1rok	2	Zanedbatelná	1	Pravděpodobné	1

Poř. č.	Č. neb.	Nebezpečí	Se	Fr	Pr	Av	CI	Bezpečnostní opatření	Bezp.

Poznámky

Zdroj: [8]

Příloha 5 – Normy zabývající se bezpečnostní strojního zařízení

Normy vztahující se k bezpečnosti strojních zařízení[30]:

- **ČSN EN ISO 12100**: Bezpečnost strojních zařízení – Základní pojmy, všeobecné zásady pro konstrukci.

Tato norma je rozdělena na dvě části, kdy první část popisuje základní terminologii a metodologii pro konstrukci bezpečného stroje a druhá část definuje technické zásady pro konstrukci bezpečného stroje. Norma je vhodná pro konstruktéry.

- **ČSN EN ISO 14121–1:** Bezpečnost strojních zařízení – Posouzení rizika.

Norma uvádí postupy k identifikaci nebezpečí, odhadu a zhodnocení rizika a také požadavky na dokumentaci k ověření provedení posouzení rizika. Norma neplatí pro rizika, kterým jsou vystavena domácí zvířata, majetek a okolní prostředí. Norma nahrazuje normu ČSN EN 1050: Bezpečnost strojních zařízení – Zásady pro posouzení rizika.

- **ČSN EN 60204–1:** Bezpečnost strojních zařízení – Elektrická zařízení strojů.

Tato část normy popisuje předpisy pro zařízení pracující do 1000 V AC a 1500 V DC a se jmenovitým kmitočtem nepřesahující 200 Hz. Popisují se zde požadavky na elektrická zařízení a jsou zde poznamenány národnostní rozdíly v požadavcích.

- **ČSN EN 61508**: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností.

Norma se skládá ze sedmi částí: všeobecné požadavky, požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností, požadavky na software, definice zkratky, příklady metod určování úrovní integrity bezpečnosti, metodické pokyny po použití IEC 61508–2,3, přehled technik a opatření. Jedná se o všeobecnou normu, která definuje požadavky na bezpečnostní systémy elektronického charakteru. Například pro návrh bezpečnostního opatření strojních zařízení existují příslušné normy ČSN EN ISO 13849–1 a ČSN EN 62061.

- **ČSN EN ISO 13857**: Bezpečnost strojních zařízení – Bezpečné vzdálenosti k zamezení dosahu k nebezpečným místům horními a dolními končetinami.

[30] Uvádím výčet několika dle mne důležitých norem, norem týkajících se bezpečnosti strojních zařízení je samozřejmě více.

- **ČSN EN 954–1:** Bezpečnost strojních zařízení – Bezpečnostní části řídicích systémů.

Tato norma je v současné době již zrušena a nahrazena normou ČSN EN ISO 13849–1 případně normou ČSN EN 62061.

- **ČSN EN 999**: Bezpečnost strojních zařízení – Umístění ochranných zařízení vzhledem k rychlosti přibližování částí lidského těla.

  Platnost této normy končí k 1. 1. 2009, nahrazena ČSN EN 999 + A1

- **ČSN EN ISO 13850**: Bezpečnost strojních zařízení – Nouzové zastavení – Zásady pro konstrukci.
- **ČSN EN ISO 10218–1:** Roboty pro výrobní prostředí – Požadavky na bezpečnost.

Norma stanovuje požadavky pro bezpečnou konstrukci, ochranná opatření a informace pro použití průmyslových robotů. Popisuje základní nebezpečí související s roboty a rizika související s těmito nebezpečími. Mezi průmyslové roboty nespadají například podmořské roboty, roboty pro vojenské a kosmické použití, mikroroboty, roboty využívané ve zdravotnictví. Tato norma nahrazuje normu ČSN EN 775 Průmyslové roboty – Bezpečnost.

- **ČSN EN ISO 13849–1:** Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů.

V normě jsou uvedeny bezpečnostní požadavky a pokyny pro zásady konstrukce a začlenění bezpečnostních částí ovládacích systémů pro strojní zařízení. Norma platí pro všechny typy strojních zařízení a umožňuje návrh bezpečnostního opatření s různou použitou technologií (pneumatické, hydraulické, elektrické atd.). Pracujeme zde s úrovní vlastností PL, která popisuje úroveň bezpečnostní funkce. Tato norma je nástupcem ČSN EN 954-1. Návrh elektronických programovatelných ovládacích systémů je kompatibilní s postupy uvedenými v normě ČSN EN 62061, proto záleží na našem výběru, kterou normu použijeme.

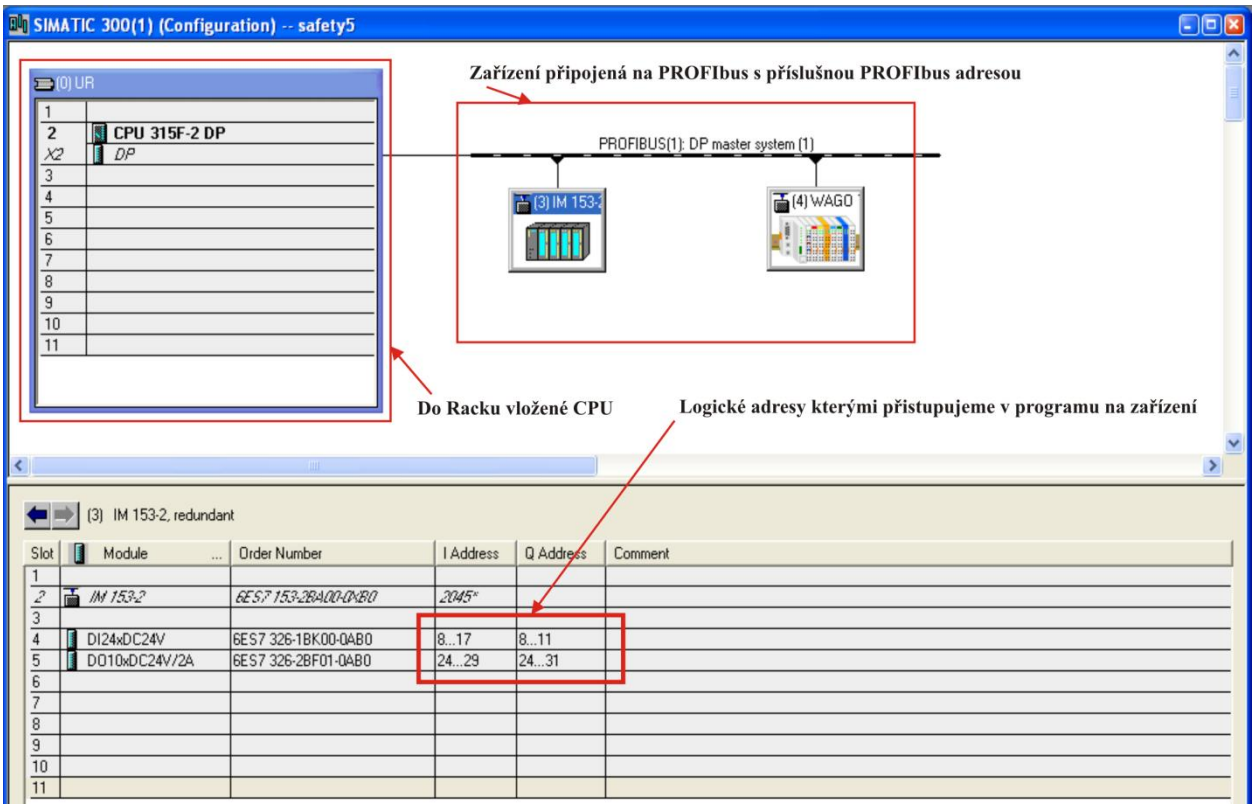
- **ČSN EN 62061:** Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností.

Norma je určena pro konstruktéry strojního zařízení a výrobce řídicích systémů a patří do podskupiny norem normy IEC 61508. Stanovuje požadavky a postupy pro dosažení požadované bezpečnostní funkce strojního zařízení. Pracujeme zde s úrovní bezpečnostní integrity SIL a předpokládané použití je pro elektronické a elektromechanické systémy.

Příloha 6 – Příklad nastavení HW konfigurace a ukázka bezpečnostního programu

Postup vytvoření bezpečnostní aplikace s využitím systému S7 Distributed Safety firmy Siemens je uveden na příkladu distribuovaného řízení s využitím Safety PLC 315F-2DP firmy Siemens a vzdálených I/O Siemens (ET200M) a Wago.

Začneme HW konfigurací, kdy, stejně jako u standardních PLC, stylem „drag and drop“ umístíme příslušné komponenty do svých pozic (Obrázek 25).

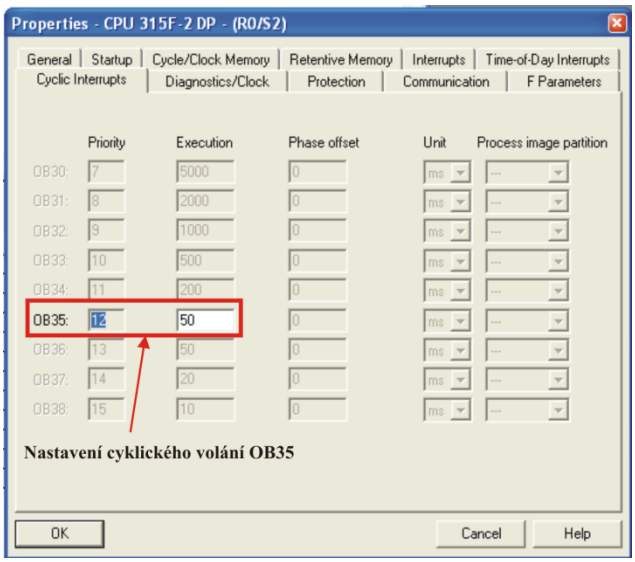


Obrázek 25: HW konfigurace ukázkového příkladu

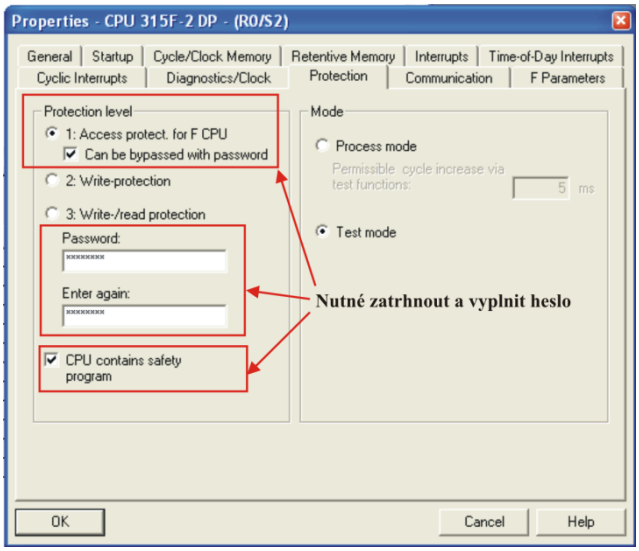
Dvojklikem na příslušný modul se dostaneme do karet nastavení parametrů. Postupně zde uvádím jednotlivá nastavení pro všechny moduly z Obrázku 23.

CPU:

Na kartě vlastností CPU musíme nastavit hodnotu cyklického volání OB35 (Obrázek 26). Jedná se o organizační blok, ve kterém se volá bezpečnostní program. Následuje záložka Protection. Zde musíme zaškrtnout několik políček, viz obrázek (Obrázek 27). Bez tohoto nastavení nám není umožněno vytvořit bezpečnostní program. Heslem zajišťujeme, že případnou změnu HW konfigurace nebo nahrání HW konfigurace či programu do PLC provede osoba s příslušným oprávněním.



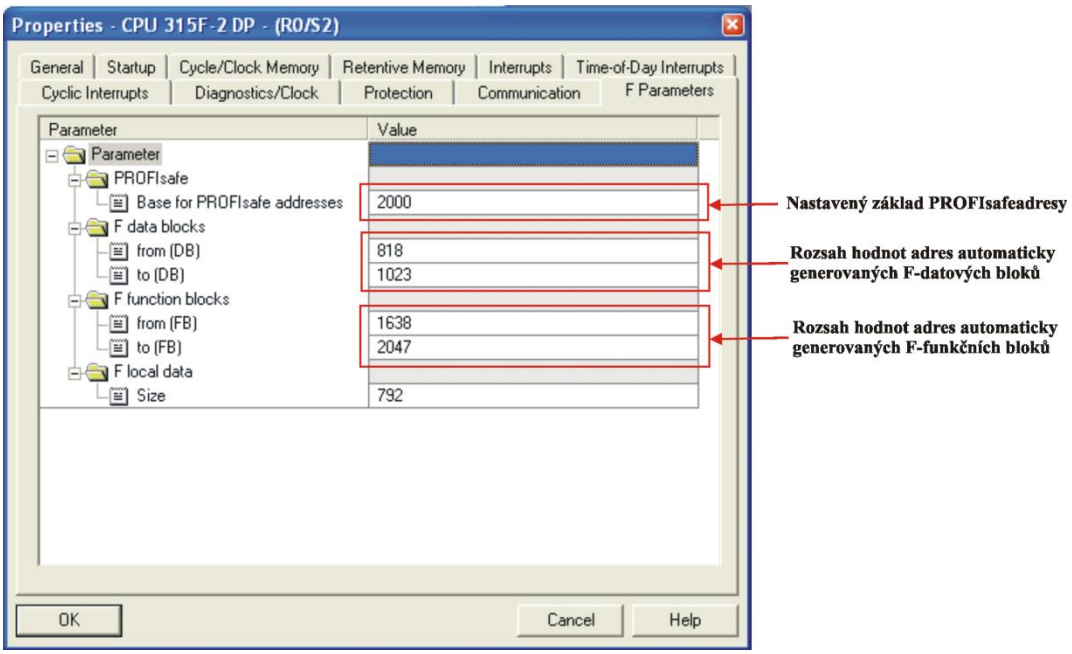
Obrázek 26: Cyklické volání OB35



Obrázek 27: Nastavení záložky Protection

Záložka F Parameters udává základní nastavení rozsahu adres datových a funkčních bezpečnostních bloků. Položka PROFIsafe adresa udává základ PROFIsafe adresy zařízení

připojených pomocí sběrnice PROFIbus. U jednotlivých zařízení je poté tento základ automaticky generován a není možnost změny.



Obrázek 28: Záložka F parametry

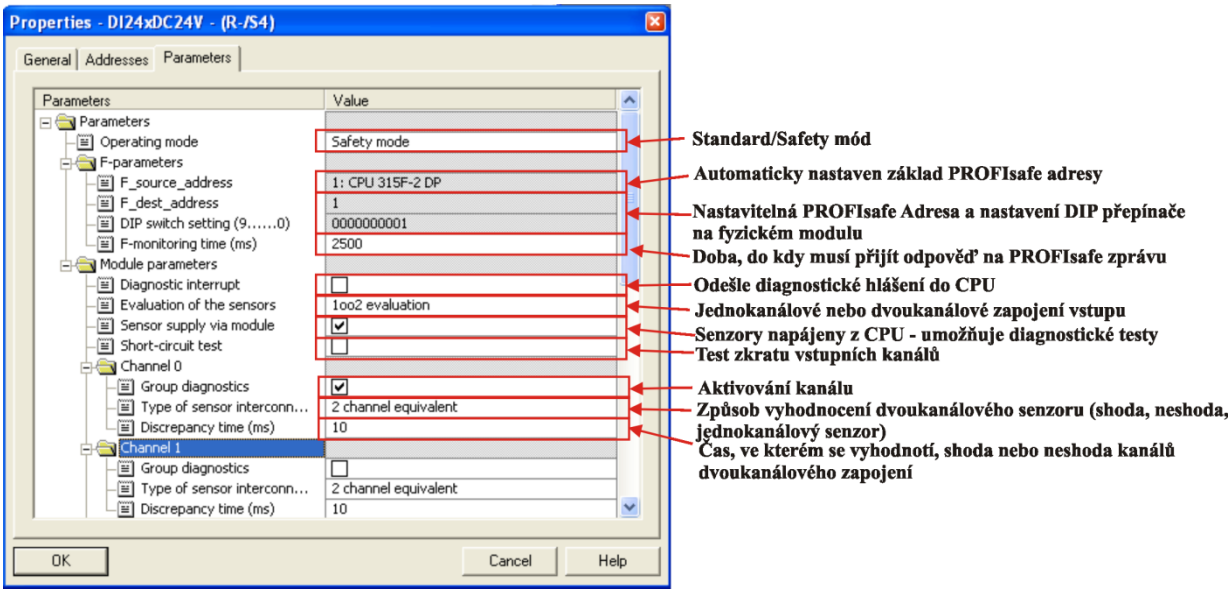
Po nastavení modulu CPU provedeme nastavení vzdálených I/O karet připojených pomocí ET200M přes PROFIbus.

Na kartě bezpečnostních vstupů provádíme tato nastavení (Obrázek 29):

Pokud karty chceme používat v Safety režimu, nastavíme příslušný operační mód. Jelikož se jedná o starou vstupní kartu, nedochází k přidělení PROFIsafe základní adresy (F_source_address). Tato položka je však generována automaticky. Více nás zajímá nastavení F_dest_address. Jedná se o adresu, kterou musíme nastavit na přepínači příslušného zařízení. Nastavení přepínače je zobrazeno hned v další kolonce – DIP Switch Setting. Pokud toto nastavíme špatně, nebude fungovat PROFIsafe komunikace a bude generována chyba. Jedná se o častý zdroj chyb. F-monitoring time je položka, která udává dobu, ve které musí proběhnout komunikace mezi příslušnou kartou a PLC, jinak je hlášena chyba komunikace. Diagnostic Interrupt slouží k odeslání diagnostických informací do CPU. Pokud není zaškrtnuta chyba, je signalizována pouze na příslušné kartě. Další položkou v nastavení je způsob zapojení senzorů, zda karta bude očekávat připojení jednokanálových nebo dvoukanálových senzorů. Při výběru dvoukanálových senzorů, jsou odpovídající kanály umístěny naproti sobě. Napájení senzoru z modulu je vhodné pro zvýšení diagnostického pokrytí. PLC pak provádí různé diagnostické testy, při nichž může odhalit poškození senzoru nebo sama sebe. Pokud používáme kartu

s dvoukanálovým zapojením, lze připojit i jednokanálový senzor, ale doporučuji pak vypnout diagnostiku zkratu. Každá sada kanálů má totiž své napájení, se kterým provádí příslušné diagnostické testy a pokud připojíme jednokanálový senzor dvoukanálově, dostává se napájecí napětí s nevhodnou diagnostikou do špatného kanálu a je to vyhodnoceno jako chyba.

U vlastních kanálů nastavujeme jejich aktivaci. U těchto starších karet je to řešeno pomocí Group diagnostics příslušného kanálu, u novějších karet je již přidána samostatná položka aktivace. Je-li položka zaškrtnuta, vstup bude očekávat připojené zařízení. V případě, kdy nic nepřipojíme, bude hlásit chybu. Pokud používáme dvoukanálové zapojení, můžeme si zvolit, zda příslušný kanál má vyhodnocovat shodu nebo neshodu připojených dvou kanálů anebo zda je tam připojen jednokanálový senzor dvoukanálově. Poslední položkou je časový údaj, do kdy musí dojít ke změně obou kanálů dvoukanálového zapojení, jinak je vyhodnocena chyba.

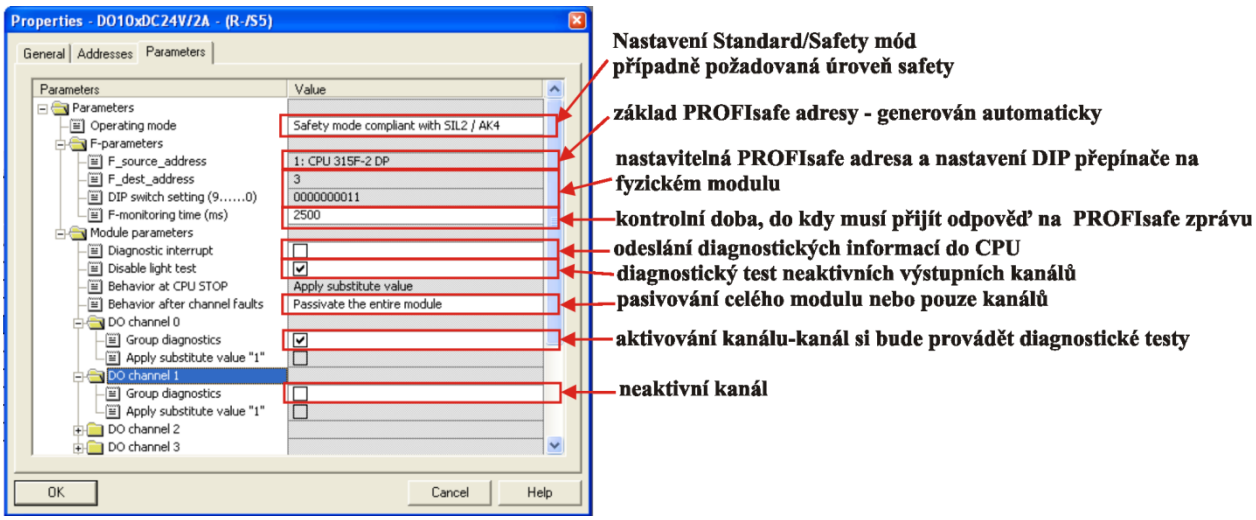


Obrázek 29: Nastavení parametrů karty F-DI

Nastavení parametrů karty bezpečnostních výstupů (Obrázek 30):

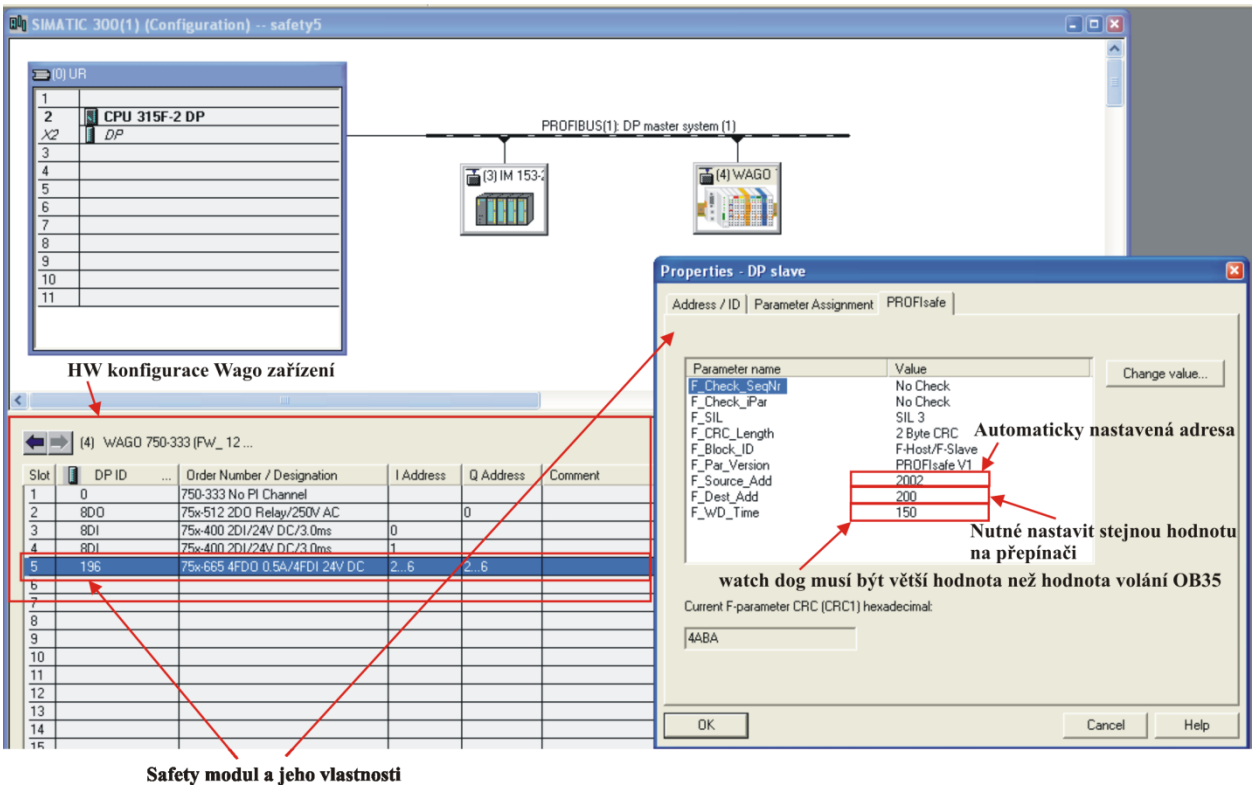
Zde uvedu jen položky, u kterých se karta liší od vstupních karet. U operačního módu máme možnost výběru úrovně bezpečnostní kategorie, kterou chceme splnit. Výběr má vliv na četnost provádění diagnostických testů. Další položkou, kterou se karty odlišují, je Disable light test. Jedná se o test, kdy deaktivované výstupy jsou na krátký čas sepnuty a tím dochází ke kontrole jejich funkčnosti. Pokud okénko zaškrtneme, provádí se pouze tzv. „dark period“ test, kdy nastane odpojení aktivních výstupů na dobu kratší 1 ms. Ve standardním módu máme možnost

nastavit výchozí hodnotu na výstupech, jestliže se přepne CPU do režimu STOP. V Safety módu je nastavena vždy hodnota log. 0. U této karty výstupů si můžeme zvolit, zda se při chybě má pasivovat celá karta nebo pouze příslušný kanál.

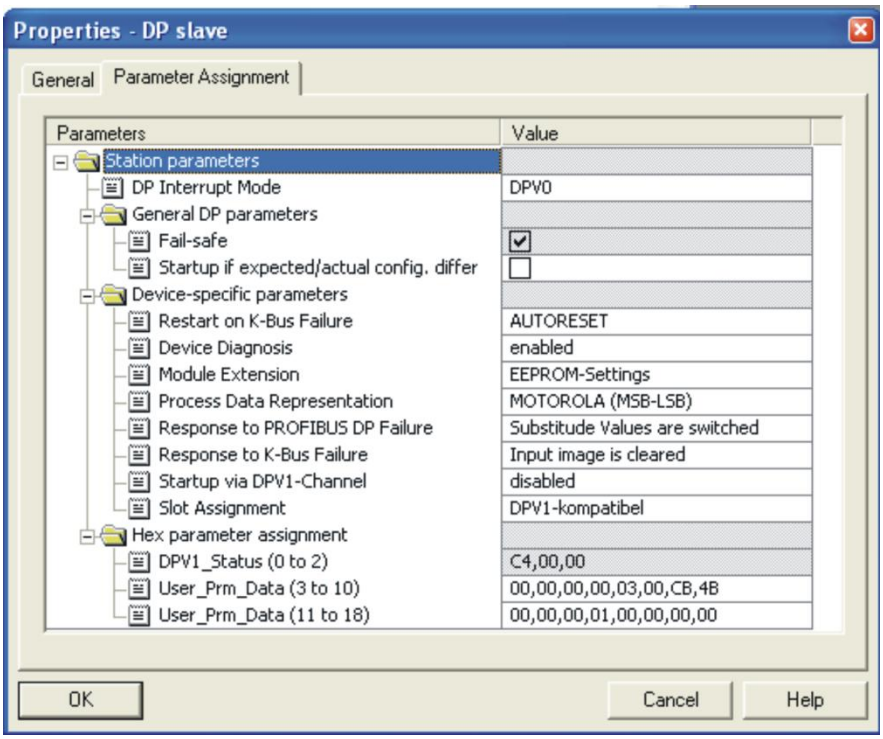


Obrázek 30: Nastavení parametrů karty F-DO

Na následujícím obrázku (Obrázek 31) je naznačena konfigurace zařízení Wago. Jedná se o komunikační kartu, ke které jsou připojeny karty standardních výstupů 2D0, 2x karta standardních vstupů 2DI (celkem 4DI) a bezpečnostní karta F-4DI/F-4DO. Je důležité zkontrolovat a případně, za pomoci přepínače umístěného na dané kartě, nastavit PROFIsafe_dest_address. Dále překontrolujeme, zda u hodnoty watch dog je větší časový údaj, než při volání OB35. Nastavení komunikační karty se mi osvědčilo dle obrázku (Obrázek 32). Zde musíme především deaktivovat DPV1 kanál v položce „Startup via DPV1-Channel “.

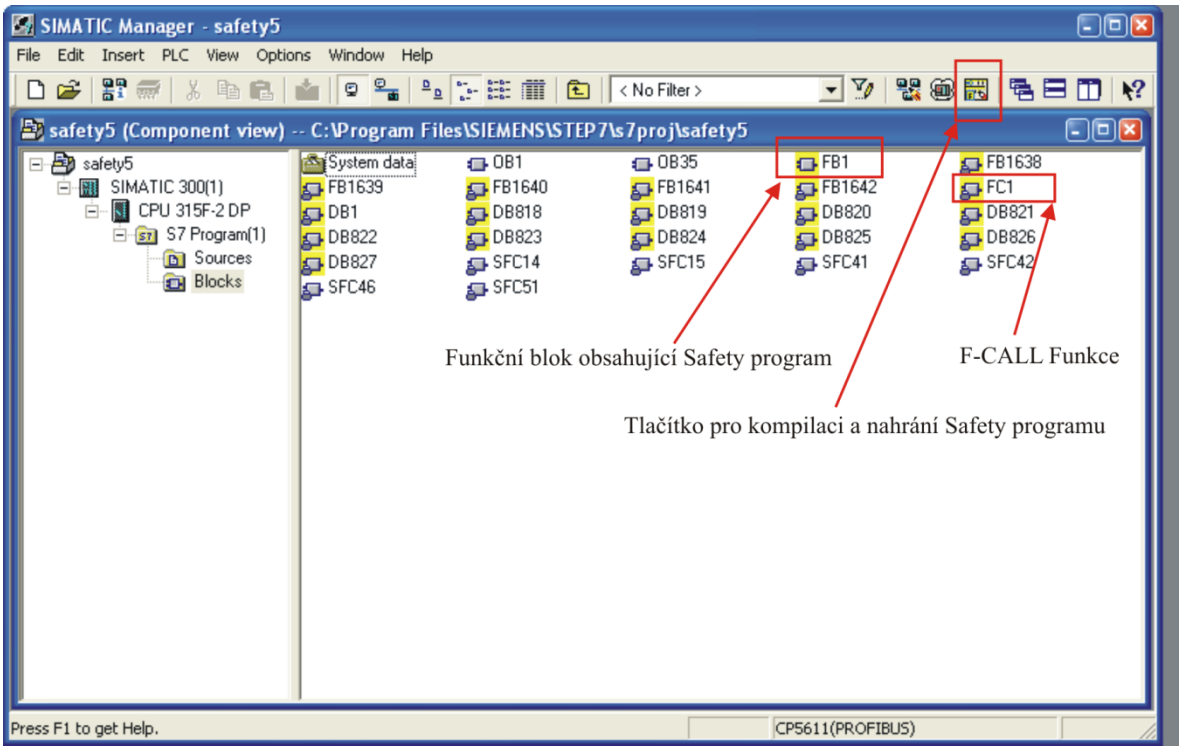


Obrázek 31: HW konfigurace Wago zařízení a parametry F-DI/DO karty



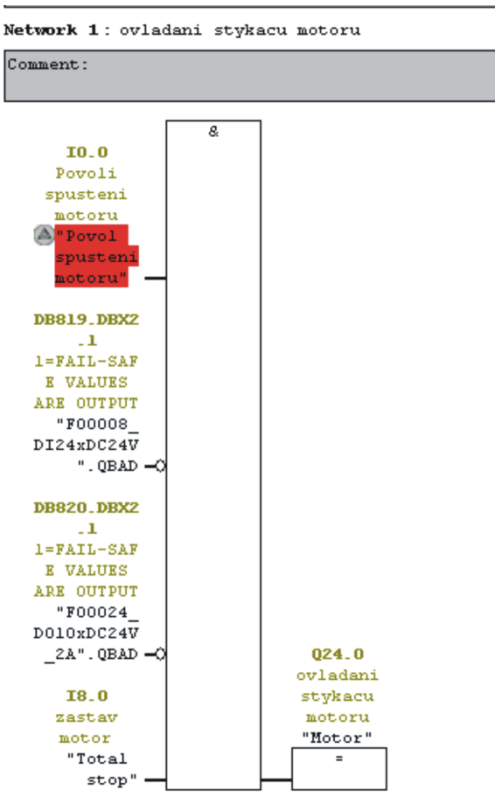
Obrázek 32: Parametry komunikační karty Wago

Po provedení konfigurace je nutné ji uložit, zkompilovat a nahrát do PLC. Po zkompilování se nám v projektu vygeneruje řada bezpečnostních funkčních a datových bloků dle příslušných zařízení (Obrázek 33). Bezpečnostní funkční a datové bloky jsou označeny žlutou barvou. Na fyzickém zařízení by měly LED diody signalizovat nastavení Safety režimu.



Obrázek 33: Ukázka projektu s F-datovými a F-funkčními bloky

Pro vytvoření bezpečnostního programu musíme dodržet následující postup, kdy nejprve vytvoříme organizační blok OB35 a funkci FC1. U funkce FC1 nastavíme parametr „Creative in Language“ na F-CALL. Poté tuto funkci v OB35 zavoláme pomocí funkce CALL. Tímto máme hotové rozhraní pro bezpečnostní program. Nyní je na našem rozhodnutí, zda použijeme pro vlastní bezpečnostní program bezpečnostní funkční blok F-FB nebo bezpečnostní funkci F-FC. V našem příkladu je použit F-FB1. Při vytváření F-FB nebo F-FC máme na výběr ze dvou programovacích jazyků, a to jazyk bezpečnostních funkčních bloků F-FBD a jazyk bezpečnostní žebříčková schémata F-LAD. Jeden z nich zvolíme. Na následujících obrázcích je ukázka programu ovládání motoru se zapojeným tlačítkem nouzového zastavení na vzdálených I/O systému Siemens a ovládání světla na zařízení Wago.

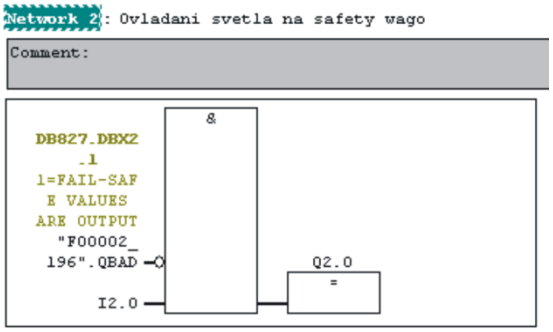


Obrázek 34: Network 1 ovládání motoru na Siemens zařízení

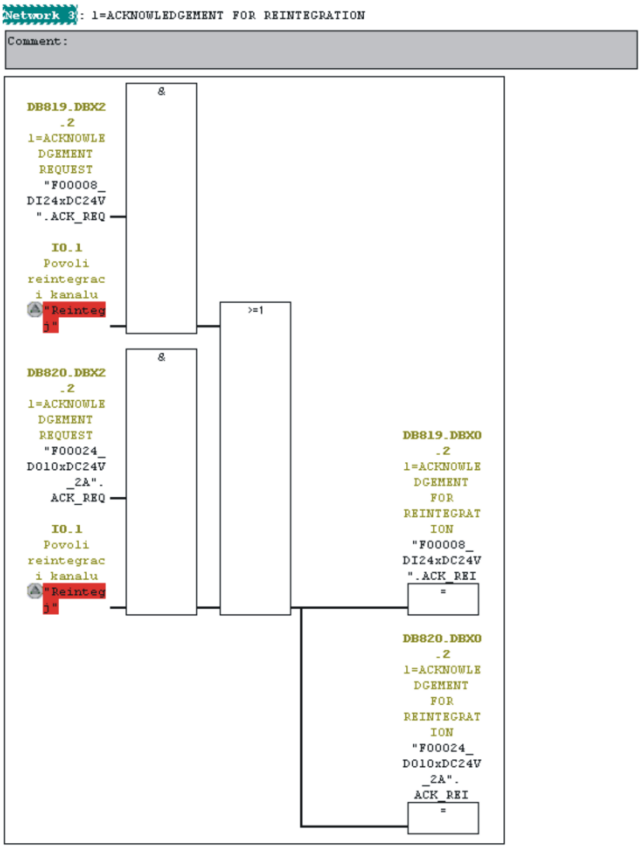
Na obrázku (Obrázek 34) provádíme obsluhu motoru. Motor smí být spuštěn, pokud se na I/O bezpečnostních kartách neobjeví chyba, není stisknuto tlačítko total stop nebo přijde signál z povolovacího tlačítka. Signály QBAD jednotlivých karet se nastaví, zjistí-li karta nějakou závadu. Dojde k její pasivaci a uvedení do bezpečného stavu. Z bezpečného stavu lze, po odstranění závady, kartu dostat tzv. reintegrací (povolením obnovení). Karta si sama detekuje, že závada je již odstraněna a v tomto případě vydá požadavek ACK_REQ. Pokud poté provedeme nastavení ACK_REI příslušné karty, dojde k její reintegraci. Automatické reintegrování lze provést vyresetováním bitu ACK_NEC v datovém bloku příslušné karty. Detekce nepřítomnosti závady trvá zhruba 30 s. Červeně označená položka znamená, že příslušná proměnná není bezpečnostní. Barvu této signalizace lze nastavit ve vlastnostech nastavení. Povolení spuštění motoru je připojeno na standardní vstup zařízení Wago. K tomuto řešení přistupujeme, protože potřebujeme potvrdit reintegraci a spuštění motoru a použitá karta bezpečných vstupů Siemens umí pouze pasivovat celou kartu vstupů.

Na obrázku (Obrázek 35) pouze ovládáme bezpečnostním vstupem zařízení Wago bezpečnostní výstup toho samého zařízení. U tohoto zařízení je také nutná reintegrace. Dále je potřeba provést, po odstranění chyby, zapnutí/vypnutí napájení a uvedení CPU Siemens z režimu run do stop a

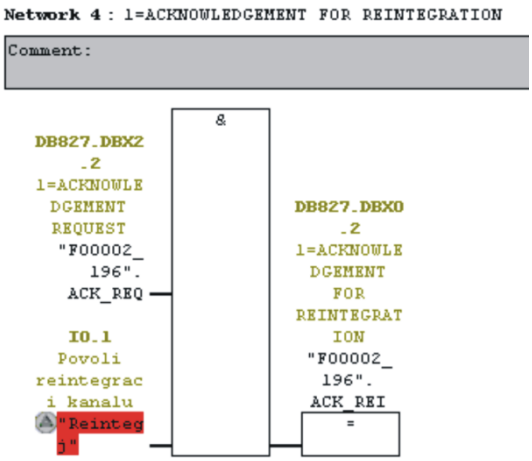
zpět. Přepnutím režimu CPU z run do stop a zpět se reintegruje i samotné zařízení Siemens, musí však být odstraněn zdroj závady. Na následujících obrázcích je pak uvedeno vlastní provedení reintegrace a signalizace a který ze systémů je v chybě na standardních výstupech Wago karty.



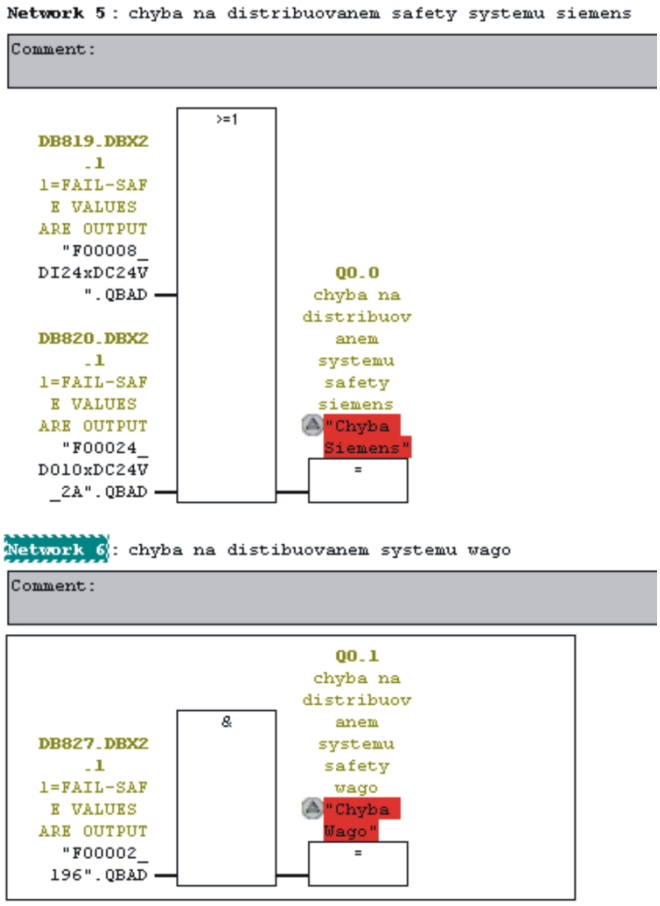
Obrázek 35: Network 2 ovládání světla na Wago zařízení



Obrázek 36: Reintegrace Siemens zařízení

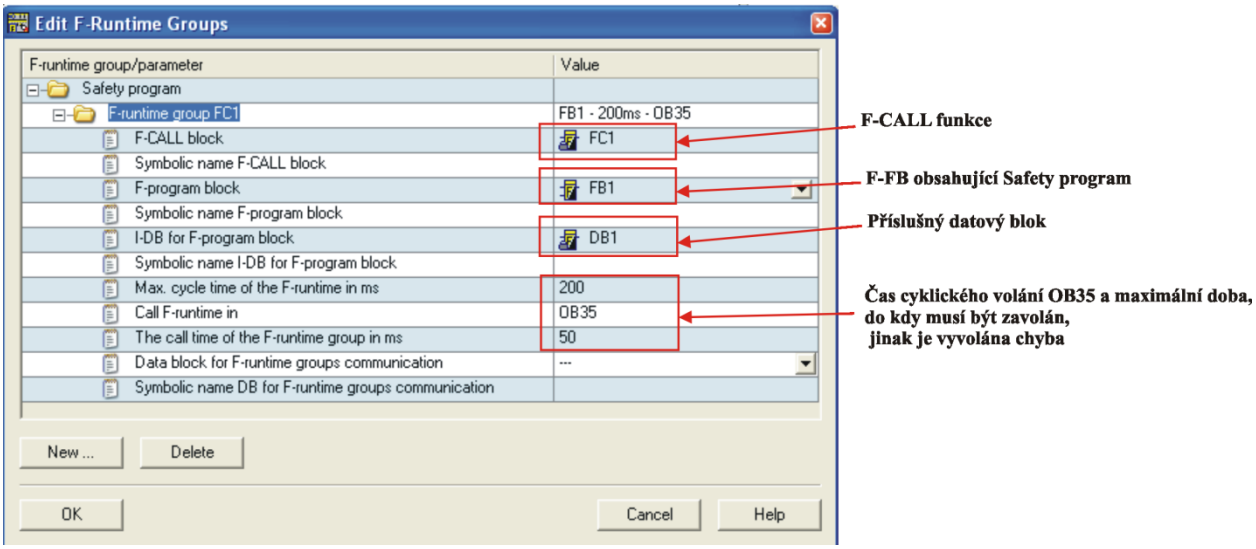


Obrázek 37: Reintegrace Wago zařízení

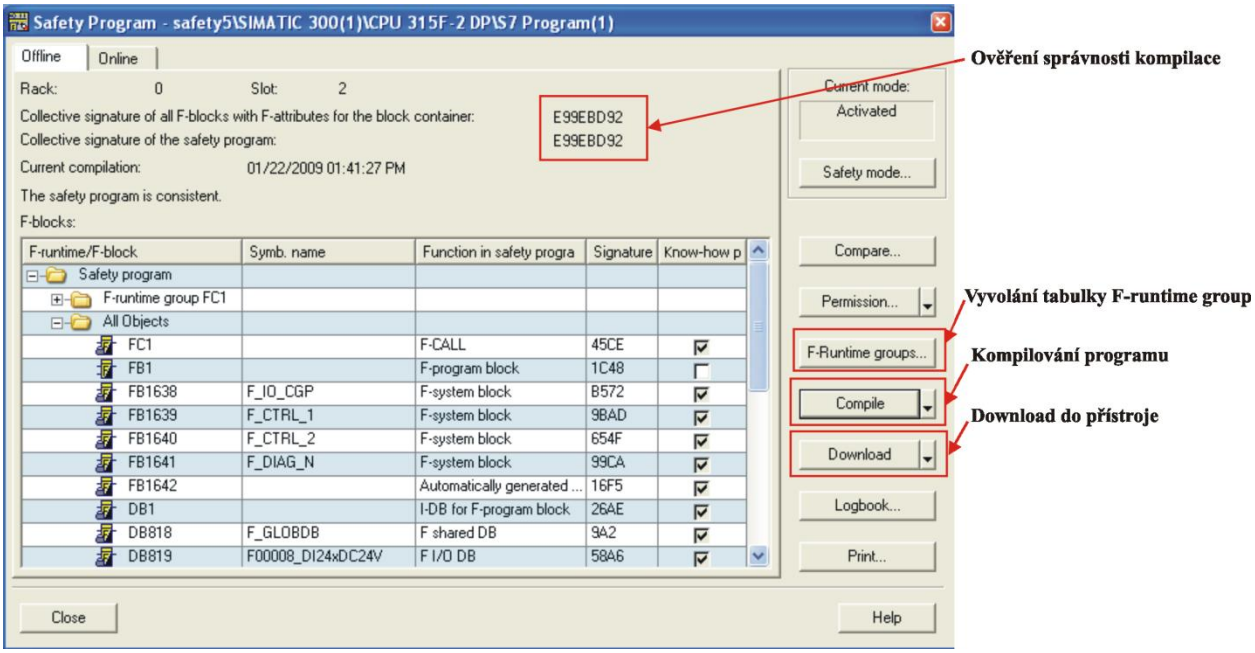


Obrázek 38: Signalizace chyby příslušného zařízení

Po vytvoření programu je potřeba jej uložit a provést správný postup kompilace a nahrání programu do zařízení. Ke kompilaci nám slouží tlačítko na obrázku (Obrázek 33). Jeho stisknutím se vyvolají následující tabulky (Obrázek 39, Obrázek 40). V první z tabulek nastavíme datový blok bezpečnostního programu (v tomto příkladě DB1). Pokud není vytvořen, po stisknutí OK se nás software dotáže, zda ho má vytvořit. To potvrdíme. Dále zde zkontrolujeme, zda čas cyklu F-runtime skupiny je větší než čas volání OB35. Tato tabulka by se měla automaticky vyvolat při první kompilaci bezpečnostního programu. Pokud ne, lze ji otevřít kliknutím na tlačítko F-Runtime Groups v druhé tabulce. Druhá tabulka (Obrázek 40) nám podává souhrn všech bezpečnostních bloků, které program využívá. Program zde musíme nejprve zkompilovat. Pokud proběhne kompilace úspěšně, je vytvořen „podpis“. Naznačeno na obrázku (Obrázek 40). Jestli program není ještě zkompilován nebo pokud v něm byla provedena změna, je „podpis“ nastaven na nulu. Po úspěšné kompilaci provedeme download do zařízení.



Obrázek 39: Edit F-runtime group



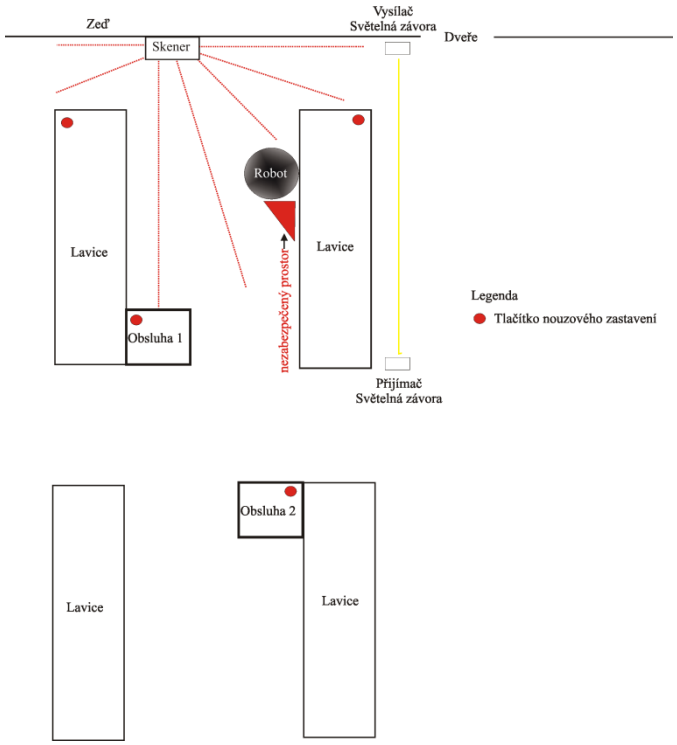
Obrázek 40: Složení Safety programu

Příloha 7 – Možná řešení umístění bezpečnostních prvků a dosah robota

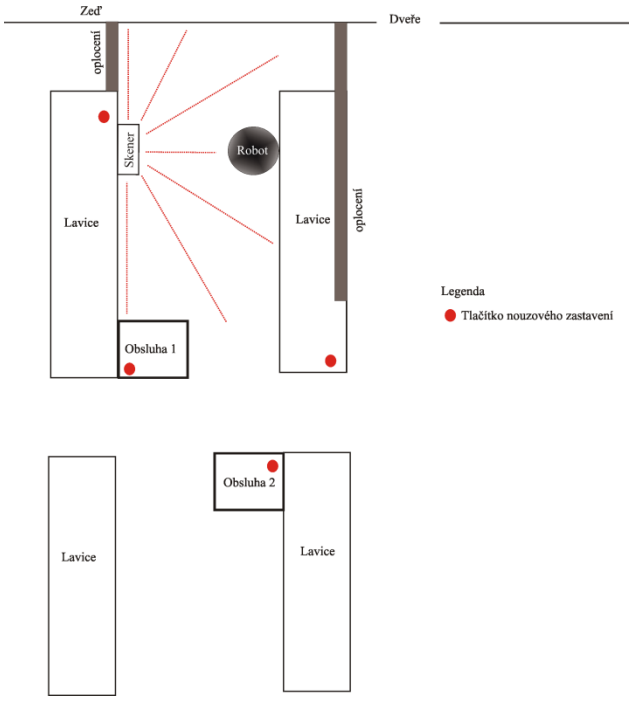
Obrázek 41: Dosah robota 1

Obrázek 42: Dosah robota 2

Obrázek 43: Dosah robota 3



Obrázek 44: Umístění bezpečnostních prvků 1



Obrázek 45: Umístění bezpečnostních prvků 2

Příloha 8 – Vyplněný formulář CCF

Příloha 2 – Formulář opatření proti poruchám CCF

Číslo	Opatření proti CCF	Počet bodů
1	Oddělení/segregace	
	Fyzické oddělení mezi jednotlivými dráhami signálu: - Oddělení u vodičů/potrubí; - Dostatečné vzduchové a povrchové vzdálenosti na deskách s plošnými spoji	15
2	Diverzita	
	Jsou použity různé technologie/konstrukce nebo fyzikální principy, například: - První kanál programovatelná elektronika a druhý kanál pevně spojen; - Druh iniciace; - Tlak a teplota; Měření vzdálenosti a tlaku: - Digitálně a analogicky; Součásti různých výrobců;	20
3	Konstrukce/použití/zkušenosti	
	Ochrana proti přetlaku, přepětí, nadproudu atd.	15
	Jsou použity osvědčené součásti.	5
4	Posouzení/analýza	
	Jsou k vyloučení CCF v konstrukci uvažovány výsledky režimu poruchy a analýzy účinku.	5
5	Způsobilost/zácvik	
	Byli konstruktéři/údržbáři zacvičeni k pochopení příčin a následků poruch CCF	5
6	Prostředí	
	Zamezení kontaminace a elektromagnetická kompatibilita (EMC) proti CCF podle příslušných norem.	25
	Ostatní vlivy – odolnost proti relevantním vlivům prostředí (teplota, vibrace, rázy, vlhkost).	10
	Opatření pro vyloučení CCF, která nejsou uvedená ve formuláři[27]	
	Celkový počet dosažených bodů – více jak 65b včetně = splněno	75b

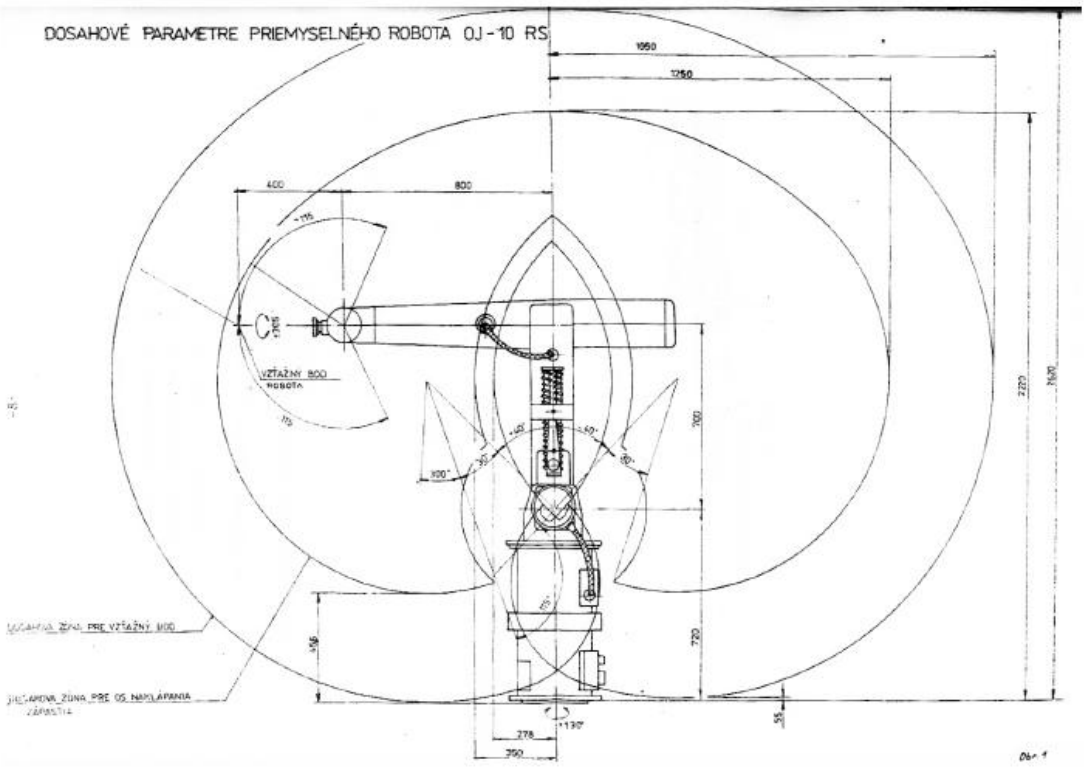
Obrázek 46: Vyplněný formulář CCF pro vstupní zařízení

Příloha 2 – Formulář opatření proti poruchám CCF

Číslo	Opatření proti CCF	Počet bodů
1	Oddělení/segregace	
	Fyzické oddělení mezi jednotlivými dráhami signálu: - Oddělení u vodičů/potrubí; - Dostatečné vzduchové a povrchové vzdálenosti na deskách s plošnými spoji	15
2	Diverzita	
	Jsou použity různé technologie/konstrukce nebo fyzikální principy, například: - První kanál programovatelná elektronika a druhý kanál pevně spojen; - Druh iniciace; - Tlak a teplota; Měření vzdálenosti a tlaku: - Digitálně a analogicky; Součásti různých výrobců;	20
3	Konstrukce/použití/zkušenosti	
	Ochrana proti přetlaku, přepětí, nadproudu atd.	15
	Jsou použity osvědčené součásti.	5
4	Posouzení/analýza	
	Jsou k vyloučení CCF v konstrukci uvažovány výsledky režimu poruchy a analýzy účinku.	5
5	Způsobilost/zácvik	
	Byli konstruktéři/údržbáři zacvičeni k pochopení příčin a následků poruch CCF	5
6	Prostředí	
	Zamezení kontaminace a elektromagnetická kompatibilita (EMC) proti CCF podle příslušných norem.	25
	Ostatní vlivy – odolnost proti relevantním vlivům prostředí (teplota, vibrace, rázy, vlhkost).	10
	Opatření pro vyloučení CCF, která nejsou uvedená ve formuláři[27]	
	Celkový počet dosažených bodů – více jak 65b včetně = splněno	70b

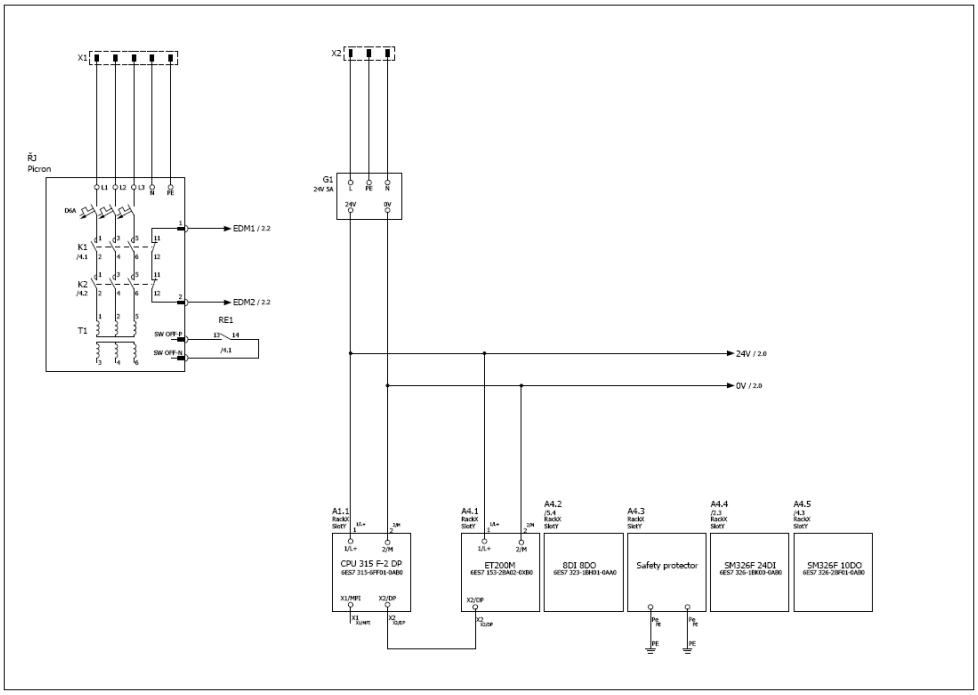
Obrázek 47: Vyplněný formulář CCF pro výstupní kombinaci stykačů

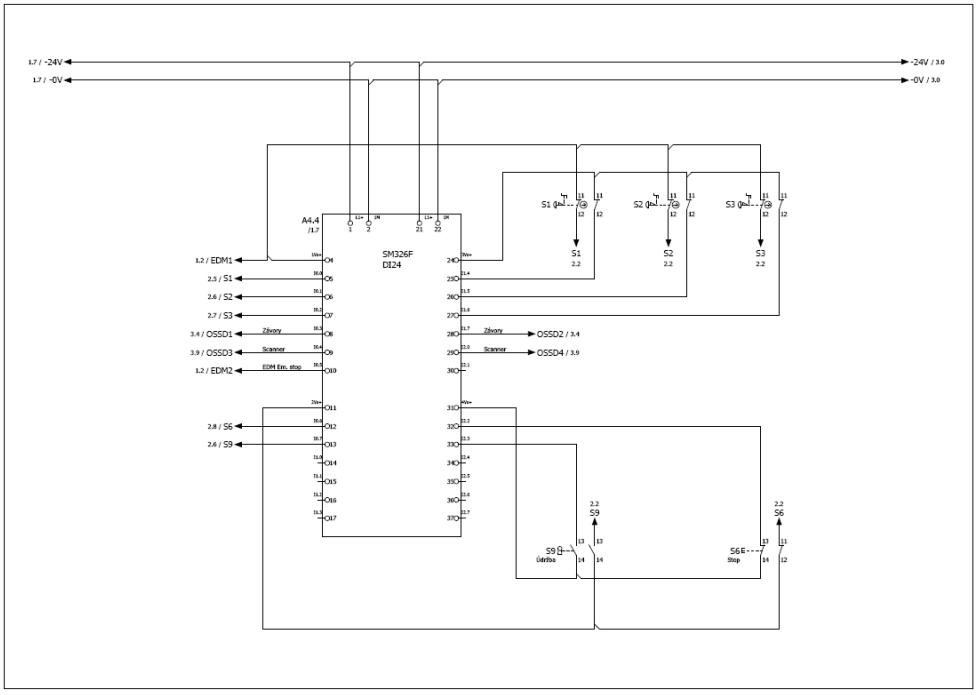
Příloha 9 – Dosahové parametry robota

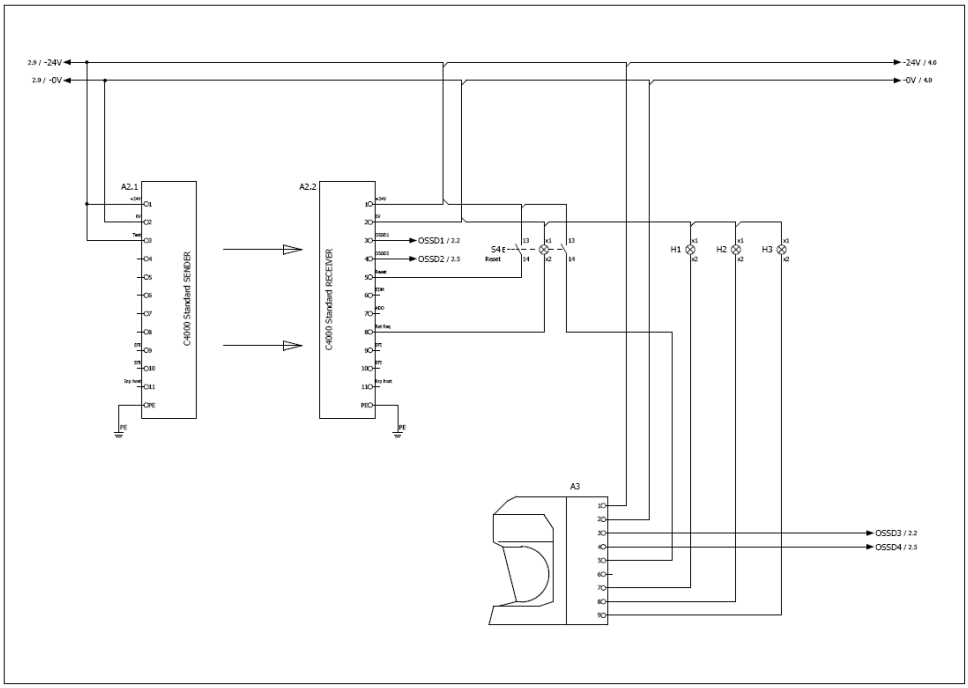


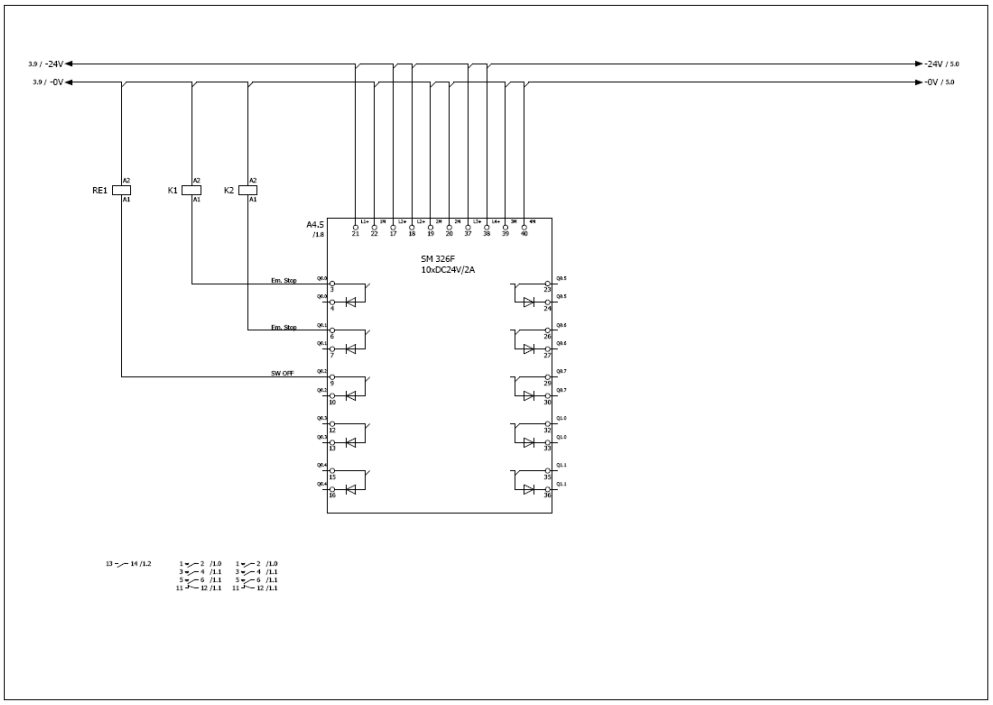
Obrázek 48: Dosahové parametry robota

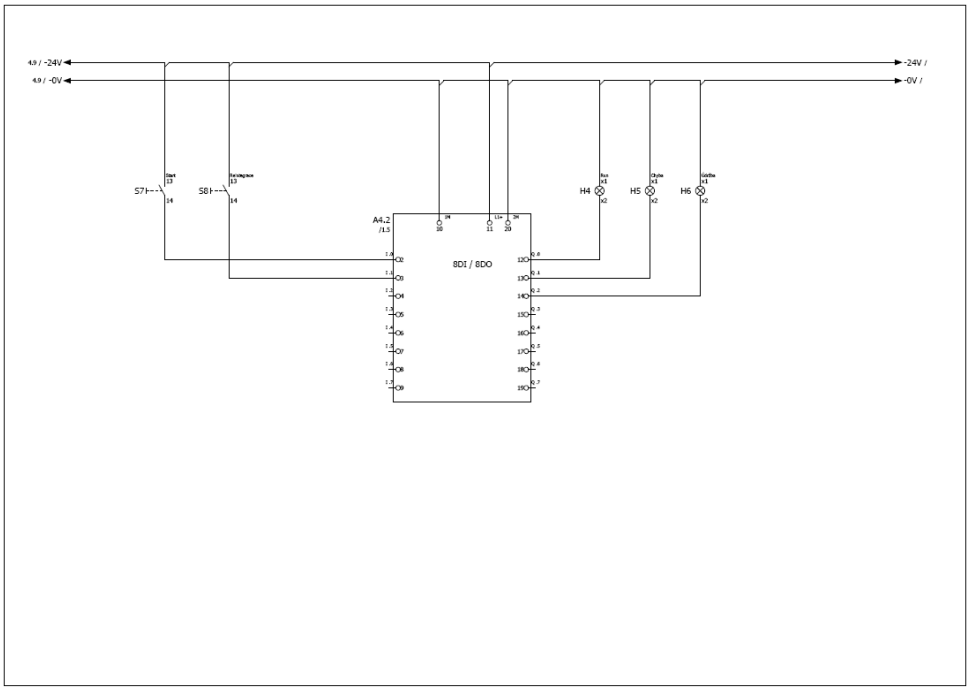
Příloha 10 – Schéma zapojení Safety PLC






2.9 / -24V
2.9 / -0V
-24V / 4.0
-0V / 4.0
A2.1
C4000 Standard SENDER
A2.2
C4000 Standard RECEIVER
OSSD1 / 2.2
OSSD2 / 2.5
S4
Reset
H1
H2
H3
A3
OSSD3 / 2.2
OSSD4 / 2.5
PE


3.9 / -24V
3.9 / -0V
-24V / 5.0
-0V / 5.0
RE1
K1
K2
A4.5
/1.8
SM 326F
10xDC24V/2A
Em. Stop
Em. Stop
SW OFF


4.9 / -24V
4.9 / -0V
-24V /
-0V /
S7
S8
H4
H5
H6
A4.2
/1.5
8DI / 8DO

Příloha 11 – Struktura přiloženého CD

- Obsah CD – ObsahCD.pdf
- Diplomová práce – dp_polak_petr_2009.docx
- Diplomová práce – dp_polak_petr_2009.pdf
- Prohlášení
- Adresář s obrázky
- Ukázkový projekt