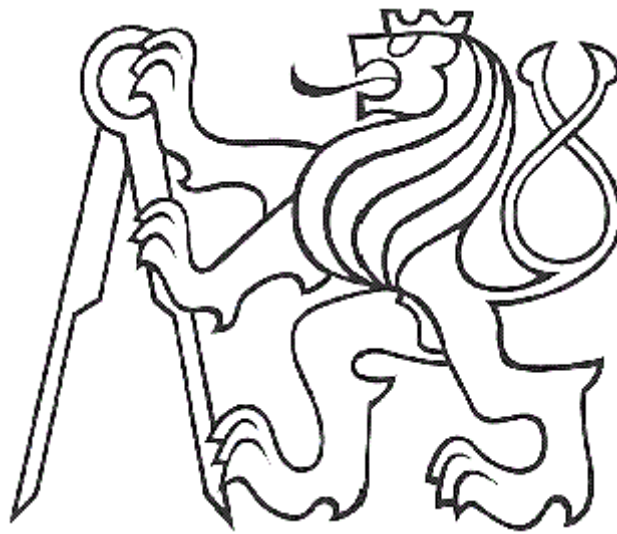


# České vysoké učení technické v Praze

Fakulta elektrotechnická  
Katedra řídicí techniky



## Bezpečnostní funkce pro Simatic S7 300 Safety function for Simatic S7 300

Vedoucí práce : Ing. Pavel Burget

Luboš Kubíček

Praha 2006

## Abstrakt

Cílem práce bylo seznámit se s programovatelnými logickými automaty(PLC) řady Simatic S7 300. Na tomto systému se seznámit s programováním PLC S7 300 pomocí software STEP 7. Dále nastudovat bezpečnostní funkce používané těmito PLC. A na základě zjištěných informací demonstrovat použití knihovny bezpečnostních funkcí na PLC S7 315F-2DP a bezpečných zařízeních připojených pomocí Profibus DP. Práce by měla čtenáři poskytnout informace o bezpečnostním systému a některých zařízeních, která tento systém využívá.

## Abstract

The object of this bachelor's work is to acquaint with programmable logical machines (PLC) Simatic S7 300. With this system to familiarize with programming PLC S7 300 with the assistance of software STEP 7. Further to study safety function, which are using by these PLC. On the basis of established information to demonstrate the using of library with safety function on PLC S7 315F-2DP and safety devices connected with the assistance of Profibus DP. This study should provide information to readers about safety system and some devices, which are using by this system.

## **Prohlášení**

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady uvedené v příloženém seznamu.

V Praze dne .....

.....

podpis

## **Poděkování**

Rád bych tímto poděkoval všem, kteří mě pomohli radou či psychickou podporou za jejich neochabující nadšení a obrovskou ochotu.

Především Ing. Pavlu Burgetovi a svým blízkým.

# Obsah

1	<b>Úvod</b> .....	1
2	<b>Požadavky na safety systém</b> .....Chyba! Zázložka není definována.	
	2.1 Konfigurační varianty I/O modulu v bezpečnostním modu.....	5
	2.2 Bezpečnostní parametry v safety modu .....	5
	2.3 Další bezpečnostní parametry v safety modu.....	6
	2.4 Adresování v bezpečnostním modu .....	7
3	<b>Vytvoření aplikace v S7 Distributed Safety</b> .....	9
4	<b>Sestava instalovaná na katedře</b> .....	17
	4.1 Zdroj PS307 – 5A.....	18
	4.2 IM153-2.....	18
	4.3 Safety protector .....	20
	4.4 Digitální moduly .....	22
5	<b>Distributed Safety F – Library</b> .....	25
	5.1 F – Application Blocks.....	25
	5.2 F – System Blocks.....	26
	5.3 F – Shared DB .....	27
6	<b>Práce na reálném zařízení</b> .....	28
	6.1 SM 326 DI SM 326 DO .....	28
	6.2 Wago .....	30
7	<b>Závěr</b> .....	32
8	<b>Seznam použité literatury</b> .....	33

# 1. Úvod

Hlavním znakem SIMATIC S7-300F je spojení standardní provozní automatizace a bezpečnostní techniky do jediného systému. To znamená, že po síti PROFIBUS DP mezi centrálním řídicím systémem a distribuovanými v/v systémy probíhá nejen „běžná“ komunikace, ale také bezpečnostně orientovaná komunikace, proto není nutná žádná samostatná bezpečnostní komunikační linka. Toto spojení standardní a bezpečnostně orientované automatizace značně snižuje výdaje na konfiguraci a návrh moderních zabezpečených provozů. SIMATIC S7-300F zajišťuje bezpečnostní funkce díky použitému F-CPU a bezpečnostním modulům, které mohou být používány jak v sestavách S7-300, tak i v distribuovaných v/v systémech ET 200M a ET 200S. Existuje softwarový balík „S7 Distributed Safety“, který usnadňuje parametrizování bezpečnostních v/v a jejich programování použitím připravených bloků.

S bezpečnostními řídicími systémy SIMATIC S7-300F může uživatel vytvářet bezpečnostní aplikace pro výrobní průmysl jak v centralizovaných, tak v distribuovaných konfiguracích.

Na tyto bezpečnostní systémy jsou samozřejmě kladeny vyšší nároky, co se týče elektromagnetické kompatibility, odolnosti vůči rušení a celkově bezchybnému chodu programu.

Základem systému je PLC osazené bezpečnostním CPU a dalšími perifériemi, které komunikují přes PROFIBUS/PROFIsafe s dalšími zařízeními, jako jsou operační panel, různé senzory a čidla, která hlídají vymezený prostor a pokud se v něm něco nebo někdo objeví, dojde k přerušení činnosti stroje. Dále jsou k síti připojena zařízení k ovládání motorů a další standardní a bezpečnostní prvky automatizační techniky.

Některé součásti SIMATIC S7-300F s distribuovanými v/v :

S7 – 300F se standardními a bezpečnostními perifériemi

ET – 200M se standardními perifériemi

ET – 200M s bezpečnostními perifériemi

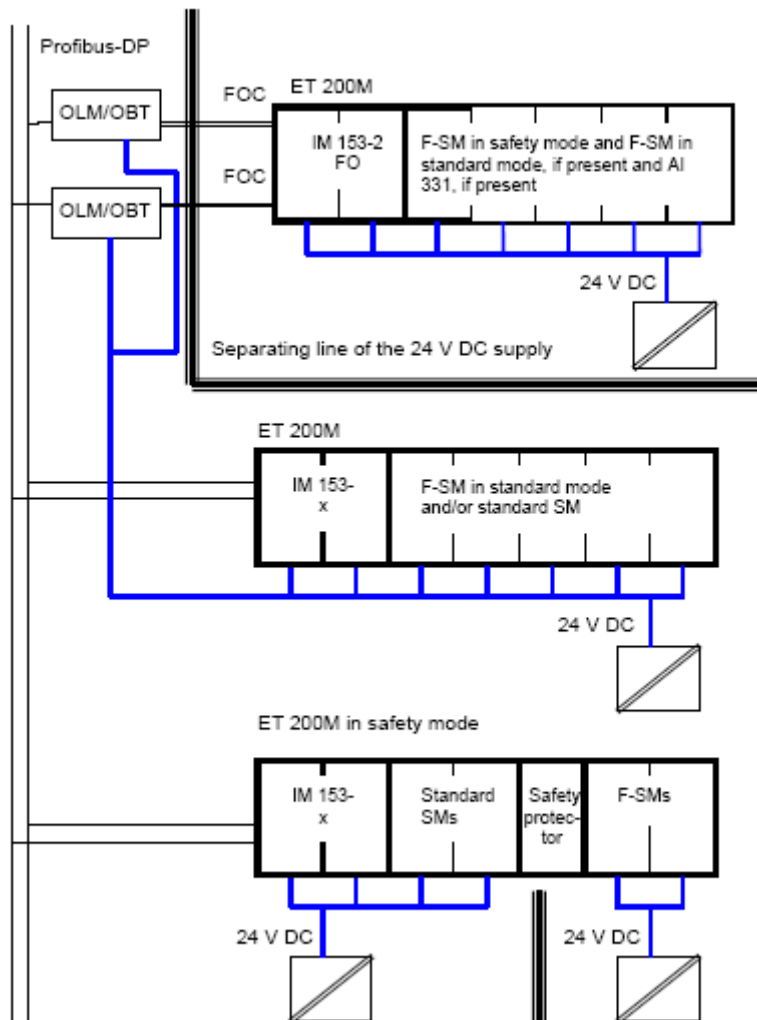
ET – 200S se standardními a bezpečnostními perifériemi a bezpečnostními startéry

Laserový scanner – snímá určitou plochu okolo strojů

Optická čidla – vysílají a přijímají světelný paprsek

## 2. Požadavky na safety systém

Bezpečnostní moduly musí umět pracovat s bezpečným napětím, které nesmí překročit hodnotu  $U_m$ . U všech bezpečnostních modulů je tato hodnota stanovena na  $U_m < 60\text{ V}$ .



Každý zdroj napětí musí být elektricky spojen, ať už se jedná o externí 24V DC zdroj, o interní 24V DC a nebo o 5V DC sběrnice napětí, aby nemohlo dojít k rozdílu potenciálu, a tím ke zvýšení napětí na nějakém zdroji nad povolenou úroveň  $U_m$ .

Komponenty v bezpečnostním systému musí být rozděleny do dvou kategorií, na které je pohlíženo z pohledu zdrojů 24V DC: všechny standardní komponenty distribuovanými vstupně výstupními jednotkami s

bezpečnostními signálními moduly v bezpečnostním modu.

Obr 2.1 Jednotlivé napájení modulů

Tyto bezpečnostní signálové moduly musí být odděleny od všech standardních modulů.

Všechny 24V DC zdroje, které jsou jak pro standardní, tak pro safety moduly, musí mít bezpečnostní elektrickou izolaci.

Na obrázku je vidět příklad takového rozdělení, kdy každá část má vlastní zdroj napájení 24V DC. Tučnou čarou je vyznačeno místo, kde je umístěn safety protector sloužící k oddělení standardních a bezpečnostních modulů.

Bezpečnostní moduly musí splňovat různá bezpečnostní kritéria, jako například elektromagnetickou kompatibilitu (EMC). Bez těchto testů by je nebylo možné používat v běžném provozu.

Tabulka ukazuje EMC bezpečnostních modulů proti impulsnímu zásahu.

Pulse-Shaped Interference	Tested With	Corresponds to Severity Level
Electrostatic discharge to IEC 61000-4-2 (DIN VDE 0843 Part 2)	8 kV	3 (Air discharge)
	6 kV	3 (Contact discharge)
Burst pulses (rapid transient interference) to IEC 61000-4-4 (DIN VDE 0843 Part 4)	2 kV (Supply line)	3
	2 kV (Signal line)	4
Surge to IEC 61000-4-5 (DIN VDE 0839 Part 10) An external suppression circuit is not required (see the chapter on lightning and overvoltage protection in the <i>S7-300 Programmable Controller, Hardware and Installation manual</i> )*		
Asymmetrical connection	1 kV (Supply line)	2*
	1 kV (Signal line/ data line)	
Symmetrical connection	0.5 kV (Supply line)	
	0.5 kV (Signal line/ data line)	



Dalšími testy EMC jsou testy na zásah sinusovým průběhem nebo například radiovým vysíláním, jak je uvedeno níže.

### Sinusoidal Interference

RF irradiation on the device to IEC 61000-4-3:

- Electromagnetic RF field, amplitude-modulated
  - From 80 to 1000 MHz
  - 10 V/m
  - 80 % AM (1 kHz)
- Electromagnetic RF field, pulse-modulated
  - $900 \pm 5$  MHz
  - 10 V/m
  - 50 % ESD
  - 200 Hz repetition frequency
- RF coupling to signal and data lines etc. to IEC 61000-4-6, high-frequency, asymmetrical, amplitude-modulated
  - From 0.15 to 80 MHz
  - 10 V effective value, unmodulated
  - 80 % AM (1 kHz)
  - 150  $\Omega$  source impedance

### Emission of Radio Interference

Emitted interference of electromagnetic fields to EN 55011: limit value class A, group 1.

From 20 to 230 MHz	< 30 dB ( $\mu$ V/m)Q
From 230 to 1000 MHz	< 37 dB ( $\mu$ V/m)Q
Measured at a distance of 30 m	

Emitted interference via system a.c. supply to EN 55011: limit value class A, group 1.

From 0.15 to 0.5 MHz	< 79 dB ( $\mu$ V)Q, < 66 dB ( $\mu$ V)M
From 0.5 to 5 MHz	< 73 dB ( $\mu$ V)Q, < 60 dB ( $\mu$ V)M
From 5 to 30 MHz	< 73 dB ( $\mu$ V)Q, < 60 dB ( $\mu$ V)M

Všechna bezpečnostní zařízení musí splňovat tyto přísná kritéria, neboť jsou na ně kladeny vysoké nároky ohledně spolehlivosti a odolnosti proti nežádoucím rušivým vlivům.

## 2.1 Konfigurační varianty I/O modulu v bezpečnostním modu

**Distribuovaná činnost v ET-200M** v bezpečnostním modu jsou vykonávány v ET-200M distribuovaném I/O zařízení. Moduly nemusí být konfigurovány v bezpečnostním modu na centrálním I/O modulu. Distribuované činnosti jsou možné pouze v ET-200M.

**Kombinace bezpečnostních I/O modulů s S7-300 standardním modulem** bezpečnostní chrániče v Et-200M může být s bezpečnostními moduly a s S7-300 standardními moduly. Zařízení chrání moduly před možným přepětím, o kterém už bylo mluveno výše, kdy Um nesmí překročit 60V. Přitom musí být všechny bezpečnostní moduly umístěny vpravo od chrániče a všechny standardní moduly vlevo od bezpečnostního chrániče.

## 2.2 Bezpečnostní parametry v safety modu

V digitálním vstupním modulu je požadovaná bezpečnostní úroveň dosažena odpovídajícím typem sensorového vyhodnocení.

Safety Level			Type of Sensor Evaluation Required
To IEC 61508	To DIN V 19250	To EN 954-1	
SIL 2	Safety level AK 4	Category 3	1oo1 Evaluation
SIL 3	AK 5, 6	Category 4	1oo2 evaluation

V analogovém vstupním modulu

Safety Level			Type of Sensor Evaluation Required
To IEC 61508	To DIN V 19250	To EN 954-1	
SIL 2	Safety level AK 4	Category 3	1oo2 evaluation, single-channel sensors
SIL 3	AK 5, 6	Category 4	1oo2 evaluation, redundant sensors

## Bezpečnostní výstupní moduly a testovací aplikace

Safety Level			Achieved by Means of Test Signal Application
To IEC 61508	To DIN V 19250	To EN 954-1	
SIL 2	Safety level AK 4	Category 3	• Dark period (< 1 ms)
SIL 3	Safety level AK 6	Category 4	• Light period (< 1 ms) and • Dark period (< 1 ms)

Tyto úrovně bezpečnosti značí, po jak dlouhé době může nastat v programu chyba

SIL 1 - jedno nebezpečné selhání během 10 let

SIL 2 - jedno nebezpečné selhání během 100 let

SIL 3 - jedno nebezpečné selhání během 1000 let

SIL 4 - jedno nebezpečné selhání během 10000 let

Převod těchto úrovní bezpečnosti mezi normami IEC a DIN

IEC	DIN
SIL 1	AK 2, AK 3
SIL 2	AK 4
SIL 3	AK 5, AK 6
SIL 4	AK 7, AK 8

## 2.3 Další bezpečnostní parametry v safety modu

### Safety Frame

V safety modu jdou data mezi CPU a fail – safe signálovými moduly přenášeny v bezpečnostním paketu, který může být dlouhý až 16 bytů.

Tento paket tvoří :

Procesní hodnoty, což jsou vlastně data uživatele

CRC testovací hodnoty

Watchdog nebo za sebou jdoucí data

Stavový byte nebo kontrolní byte (koordináční data pro safety mod)

## **CRC testovací hodnota**

Platnost procesních hodnot v safety modu, platnost přiřazených adresových odkazů a bezpečnostně souvisejících parametrů jsou chráněny prostředky CRC testovacích hodnot obsažených v bezpečnostním paketu.

Když při komunikaci mezi CPU a modulem nastane chyba (např. dočasný elektromagnetický zásah), diagnostická zpráva indikuje v testovací hodnotě chybu. V takovém případě jsou výstupy na výstupních modulech okamžitě vypnuty.

## **Monitoring Time and Consecutive Number**

Základní monitorovací čas v aktualizovaném paketu v PROFISafe protokolu vezme prostor jako výsledek z CPU, vydávající za sebou jdoucí čísla do fail – safe signálových modulů.

Platný současný paket musí přijít do CPU s platným po sobě jdoucím číslem. Když toto číslo není detekováno během monitorovacího času, diagnostická zpráva indikuje, že monitorovací čas v safety programu byl překročen. V takovém případě jsou výstupy na výstupních modulech okamžitě vypnuty.

## **2.4 Adresování v bezpečnostním modu**

**Při adresování se rozhoduje mezi :**

- logickou modulovou adresou
- číslem kanálu

**Logická modulová adresa :** Je konfigurována jako vstupní parametr bezpečnostních signálových modulů

- k nastavení bezpečnostního signálového modulu je používán adresový přepínač
- tyto bezpečnostní moduly zabírají 16 bytů ve vstupní a výstupní oblasti
- přípustný adresový rozsah je 8 až 8191 v bloku po osmi

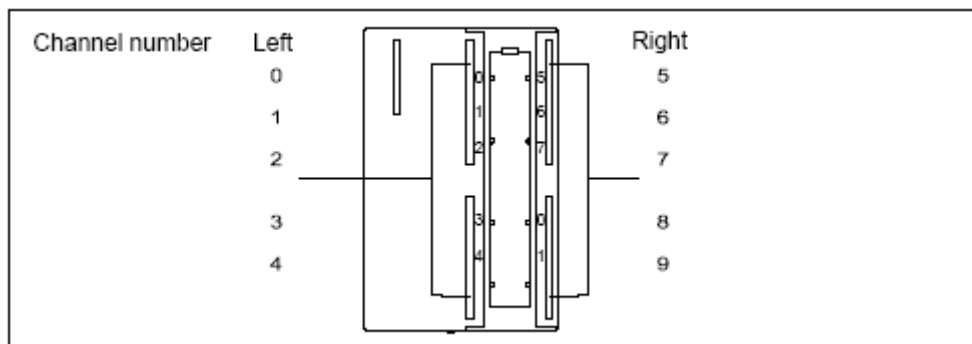
**Číslo kanálu :** Vstupy a výstupy jsou adresovány uvnitř bezpečnostních funkcí přes číslo kanálu

Číslo kanálu je za sebou jdoucí číslo, začínající "0"

Číslo kanálu v bezpečnostních signalových modulech - je konfigurováno jako vstupní nebo výstupní parametr v bezpečnostních jednotkových blocích

Jsou zmíněny v kanálu – specifické diagnostické zprávy

Příklad: Následující obrázek ukazuje převod z čísla kanálu na vstupy/výstupy použité například u SM 326; DO 10x24V DC/2A s diagnostikou přerušení



Obr 2.2 Číslování kanálů

### Požadavky analogových senzorů a akčních členů

Analogové senzory

Následující zpravidla platí :

- uspokojující požadavek je SIL 2 a jednokanálový senzor je dostačující
- uspokojující požadavek je SIL 3, pak už musí být dvoukanálový senzor

Akční členy : jsou bezpečnostní výstupní moduly testující výstupy v pravidelných intervalech. A to tak, že modul krátce odpojí aktivní výstupy, když je to nezbytné a krátce zapne výstupy, které byly předtím vypnuté.

Tyto testovací pulsy mají následující dobu trvání : temná perioda < 1 ms

světlá perioda < 1 ms

Akční členy, které odpoví rychle, mohou být deaktivovány nebo aktivovány krátce během testu. Když proces nemůže tolerovat toto, pak akční členy jsou dostatečně pomalé (> 1 ms)

### 3. Vytvoření aplikace v S7 Distributed Safety

Tvorba produktu je následující : Konfigurovat hardware

F-Call do cyklického OBxx

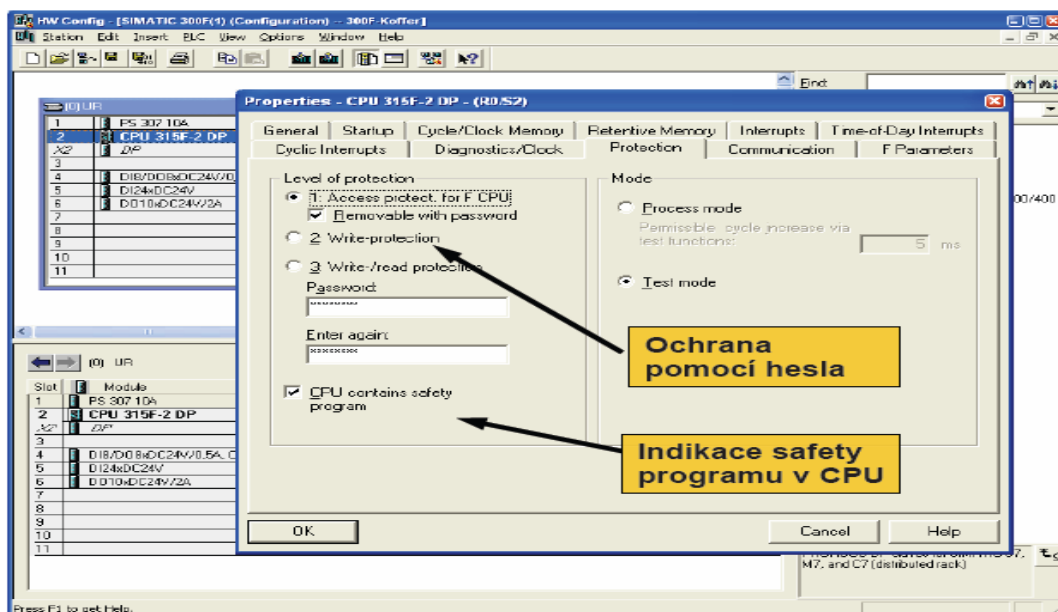
Sestavit strukturu programu vložit F - FB/F - FC

Definovat F - runtime pravidla

Generovat a download fail-safe programu

Konfigurace hardware : je stejná jako při vytváření standardního projektu pomocí programu STEP7. To znamená, že zvolíme příslušný „RACK“ a do něj poté umístíme hardware, který máme k dispozici. Přidáme Profibus a k němu připojíme IMxxx jednotku a k ní přidáme I/O zařízení, která používáme pro naše řízení.

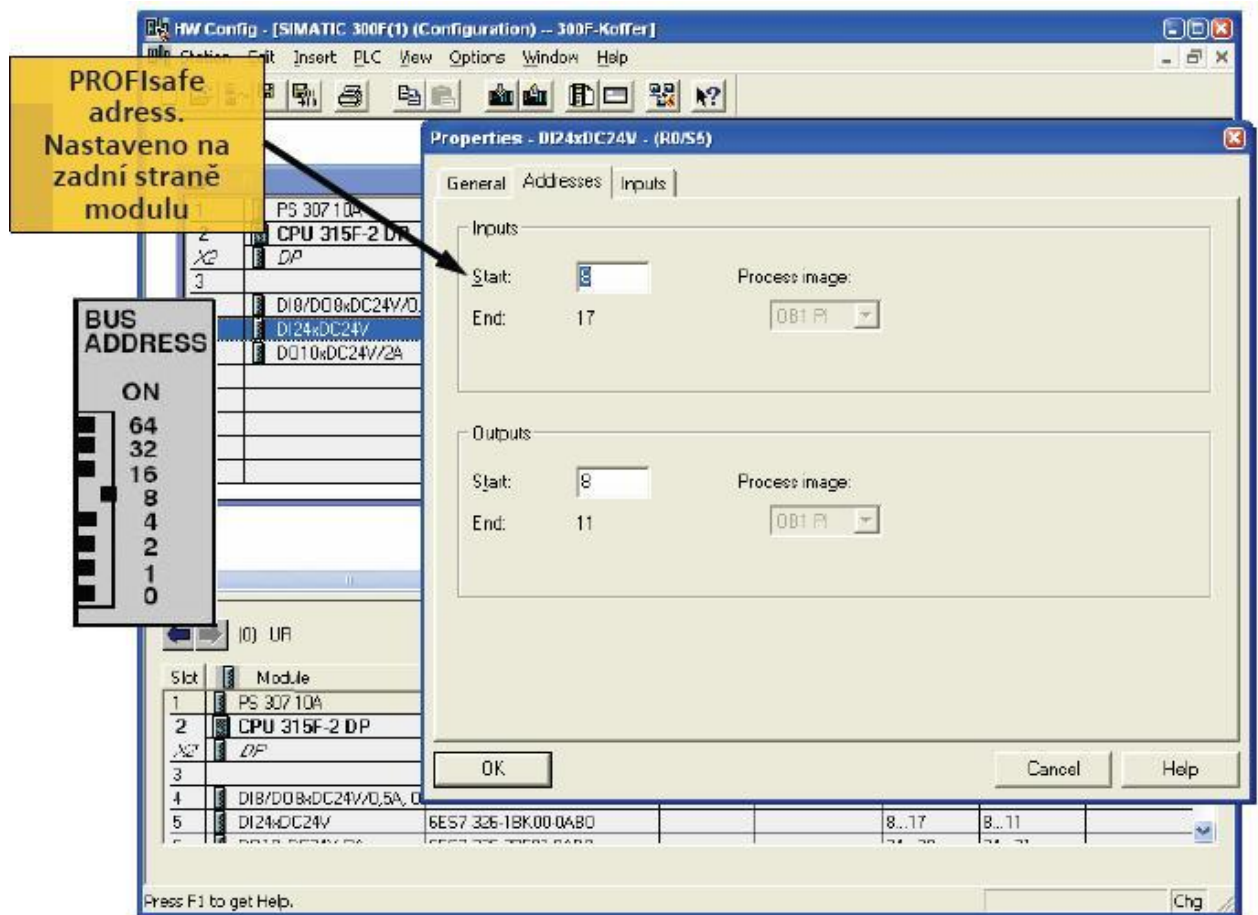
Následuje nastavení CPU, aby pracovalo v safety modu: dvojklikem na CPU se nám objeví dialogové okno, kde po zvolení záložky „Protection“ zaškrtneme „Removable with password“, což nám umožní zabezpečit CPU heslem, aby nemohlo dojít k nežádoucímu změnění uživatelského programu. Poté je samozřejmě nutné zadat do příslušných políček námi zvolené heslo a ještě zaškrtnout „CPU contains safety program“, což nám bude indikovat safety program v CPU.



Obr 3.1 Properties v CPU 315F – 2 DP

U modulu IMxxx nastavíme Profibus DP adresu.

Dále pokračujeme nastavením příslušných parametrů I/O modulů: dvojklikem otevřeme dialogové okno příslušného modulu a v záložce „Addresses“ nastavíme adresu, kterou jsme nastavili na zadním panelu daného modulu ještě předtím, než jsme ho nainstalovali do RACKu.



Obr 3.2 Nastavení adres I/O modulů

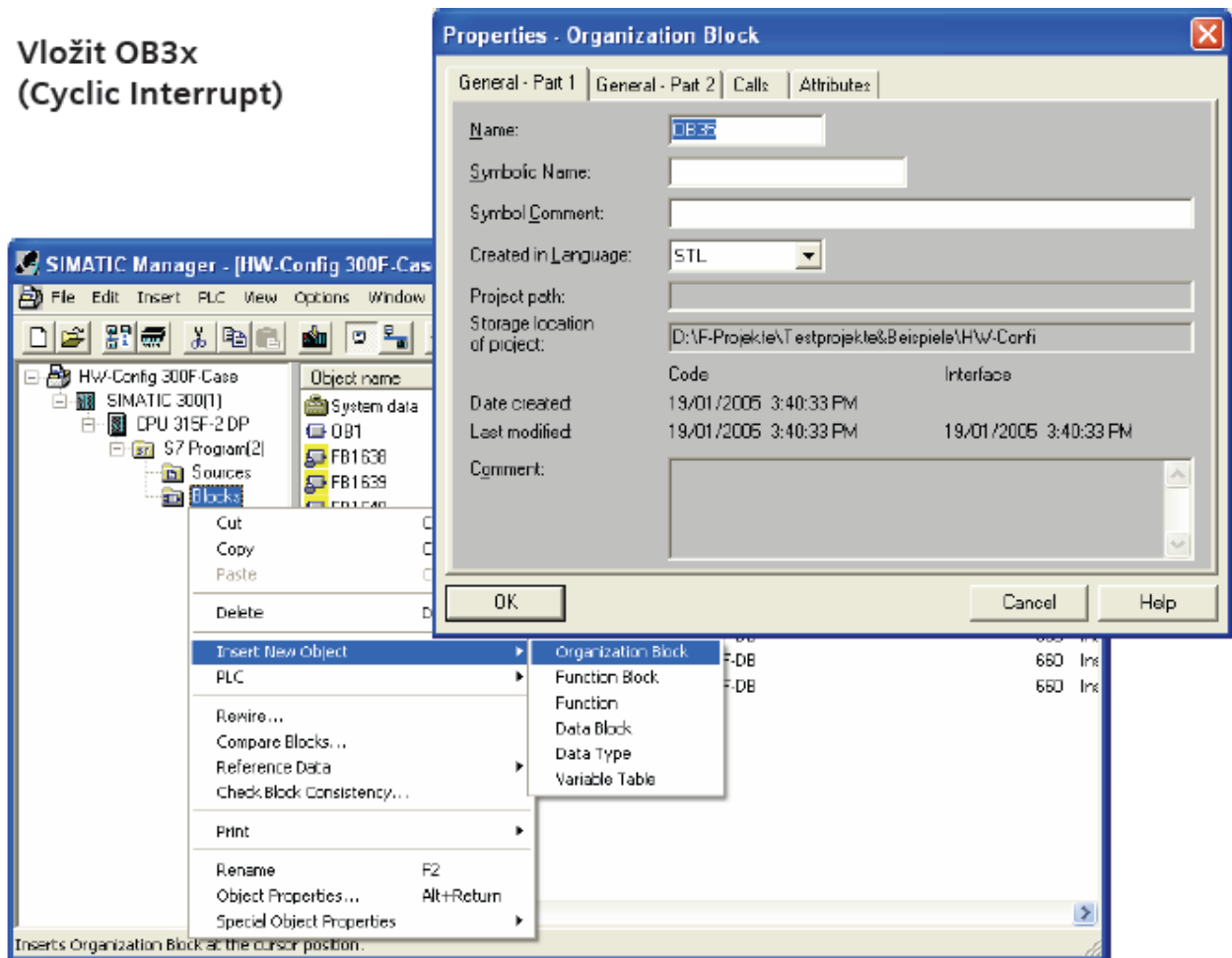
Zde je nutné, aby moduly měly odlišné adresy. Toto nastavení provedeme u všech I/O modulů, které využíváme. Dále u všech modulů deaktivujeme nepoužívané I/O kanály a vhodně upravíme PROFIsafe monitoring time.

Nyní už stačí takto vytvořenou HW – konfiguraci uložit a zkompilovat.

## F – CALL do cyklického Obxx

Vložení OB3x : v Simatic Manager otevřeme naši HW – konfiguraci a vytvoříme nový organizační blok OB – vyplníme jeho jméno a v nabídce „Created in Language“ zvolíme možnost STL.

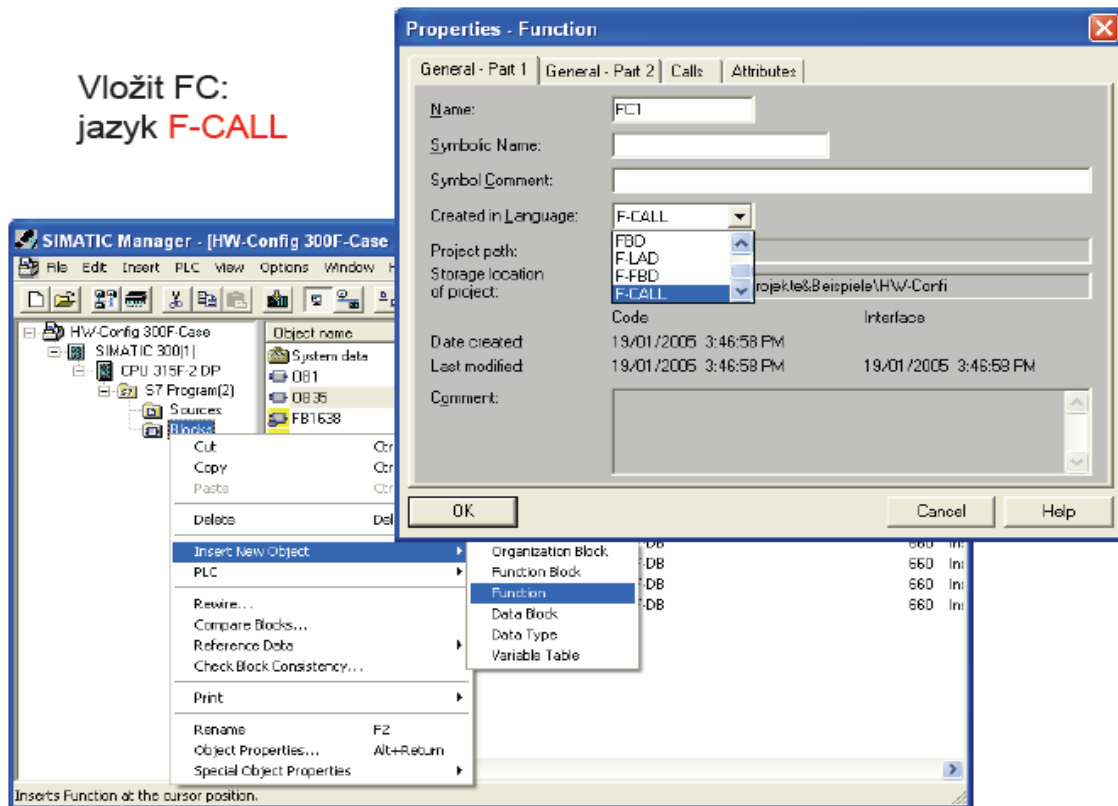
### Vložit OB3x (Cyclic Interrupt)



Obr 3.3 Vytvoření OB35



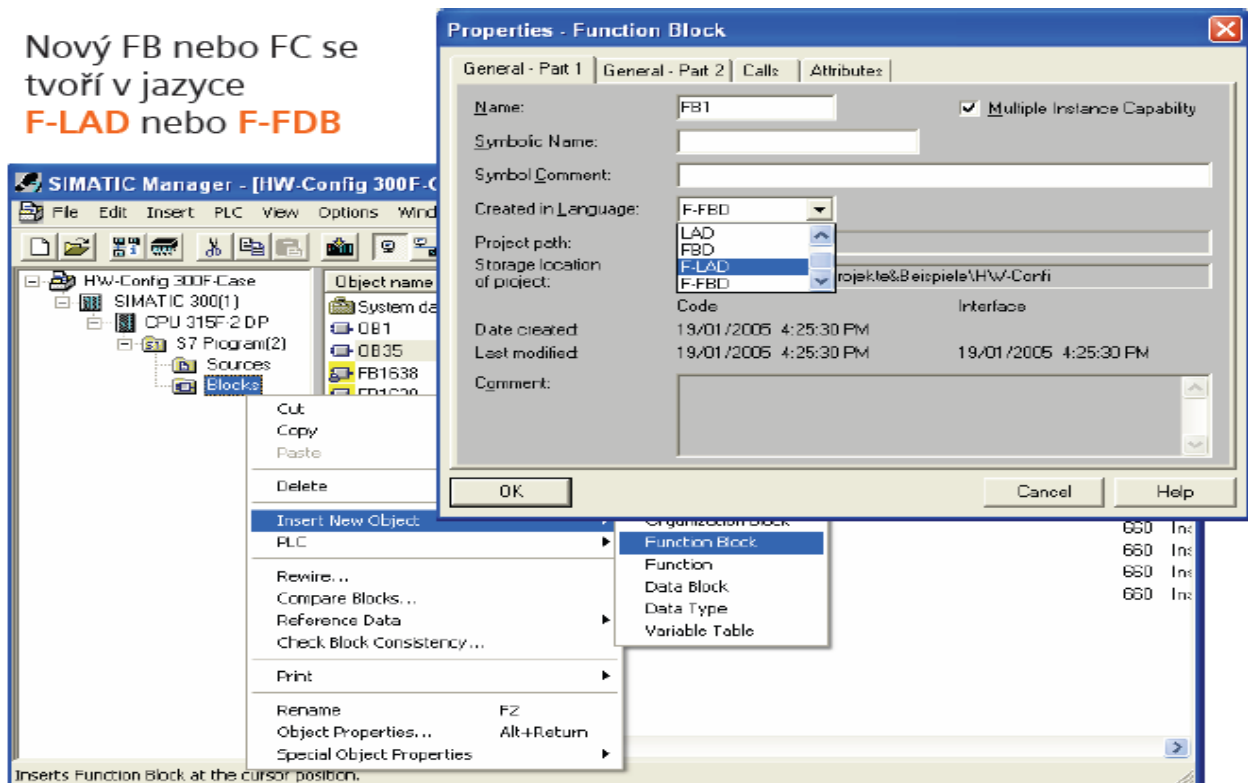
Dále vytvoříme funkci FC1, u které zvolíme možnost F-CALL.



Obr 3.4 Vytvoření FC1

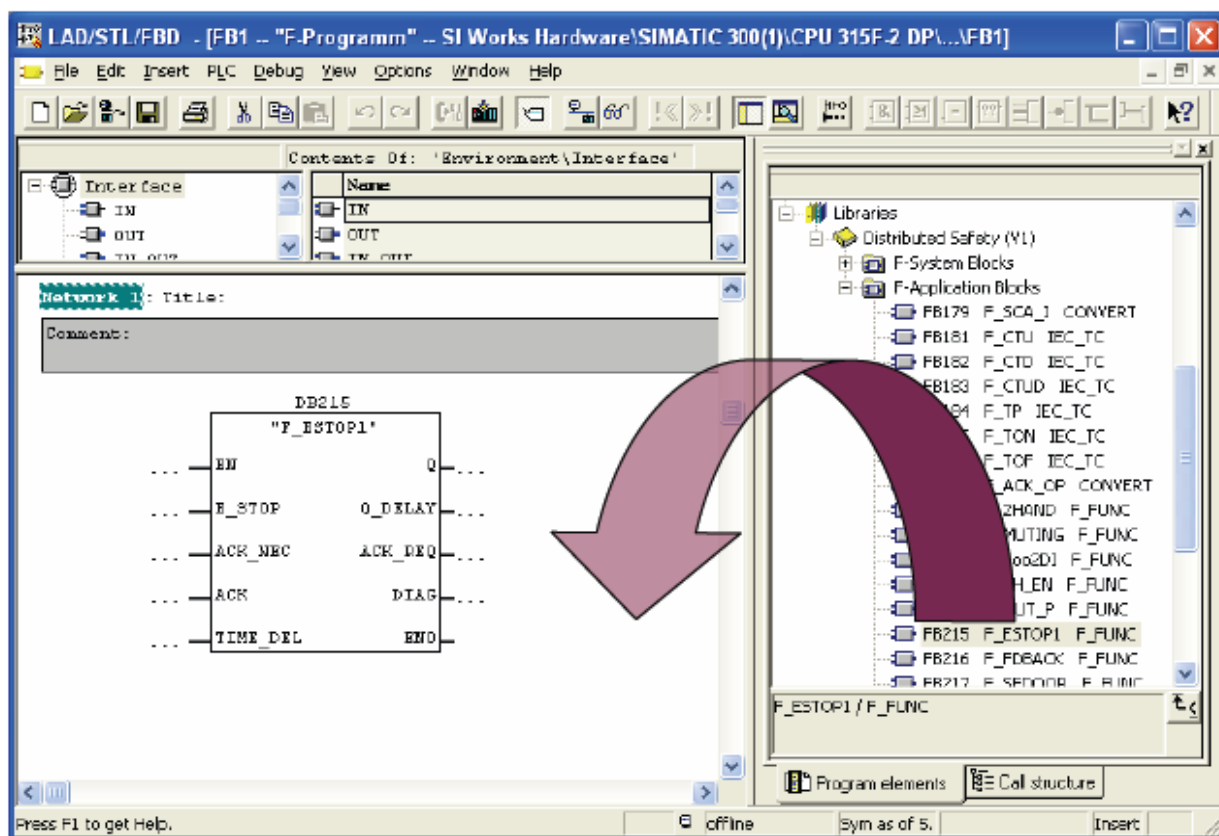
Poté dvojklikem na již vytvořený blok OB3x se otevře program, který umožňuje provádět úpravy jednotlivých bloků. My zde vytvoříme rozhraní mezi standardní a fail-safe částí programu tím, že do bloku OB3x přidáme volání bloku FC1. V levé části okna je strom, ve kterém si najdeme naši funkci FC1 a dvojklikem na ni se objeví daný příkaz volání. Změny uložíme.

Sestavit strukturu programu vložit F - FB/F – FC : v Simatic Manager vytvoříme tentokrát funkční blok (např. FB1) a zvolíme u něj v nabídce „Created in Language“ F – LAD



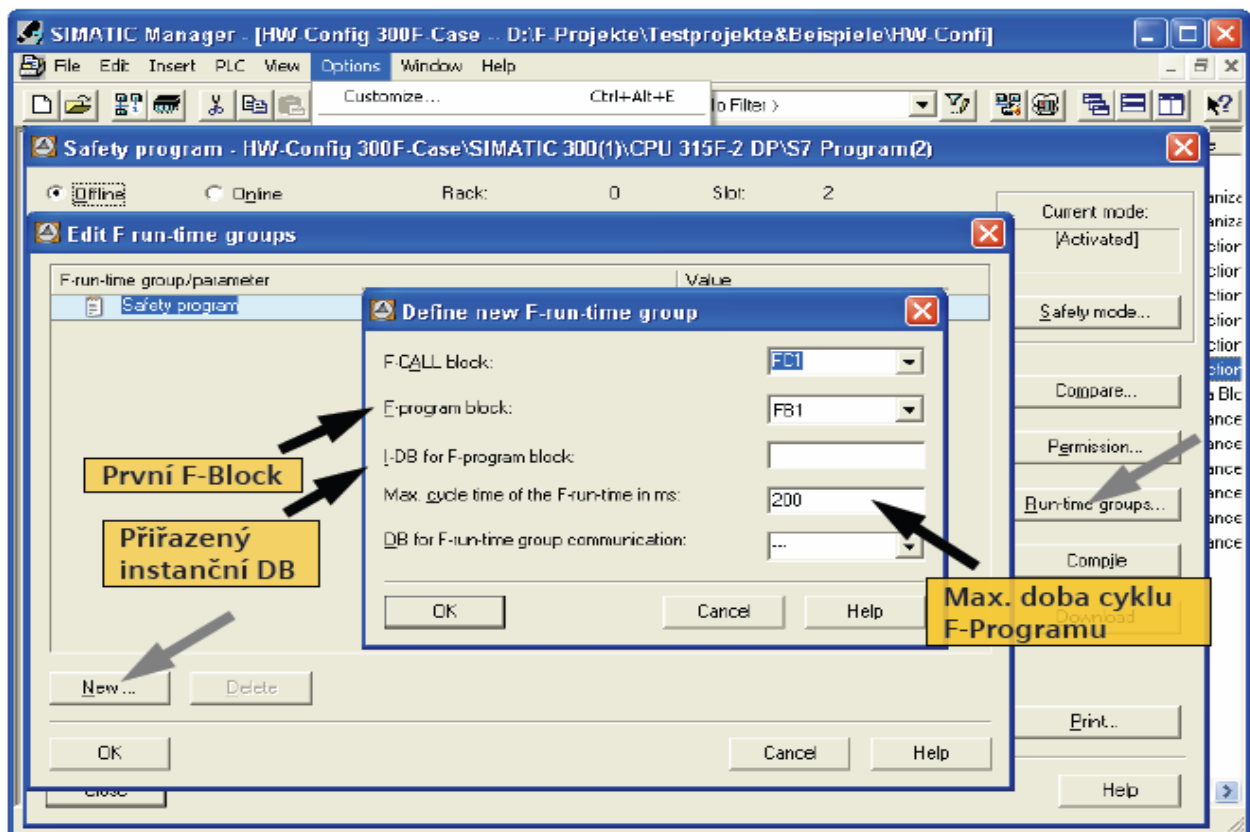
Obr 3.5 Vytvoření funkčního bloku

Dvojklikem na tento blok se opět dostaneme do LAD/STL/FBD programu a do otevřeného bloku vložíme jeden libovolný aplikační blok z naší Distributed Safety Library a tento blok pojmenujeme.



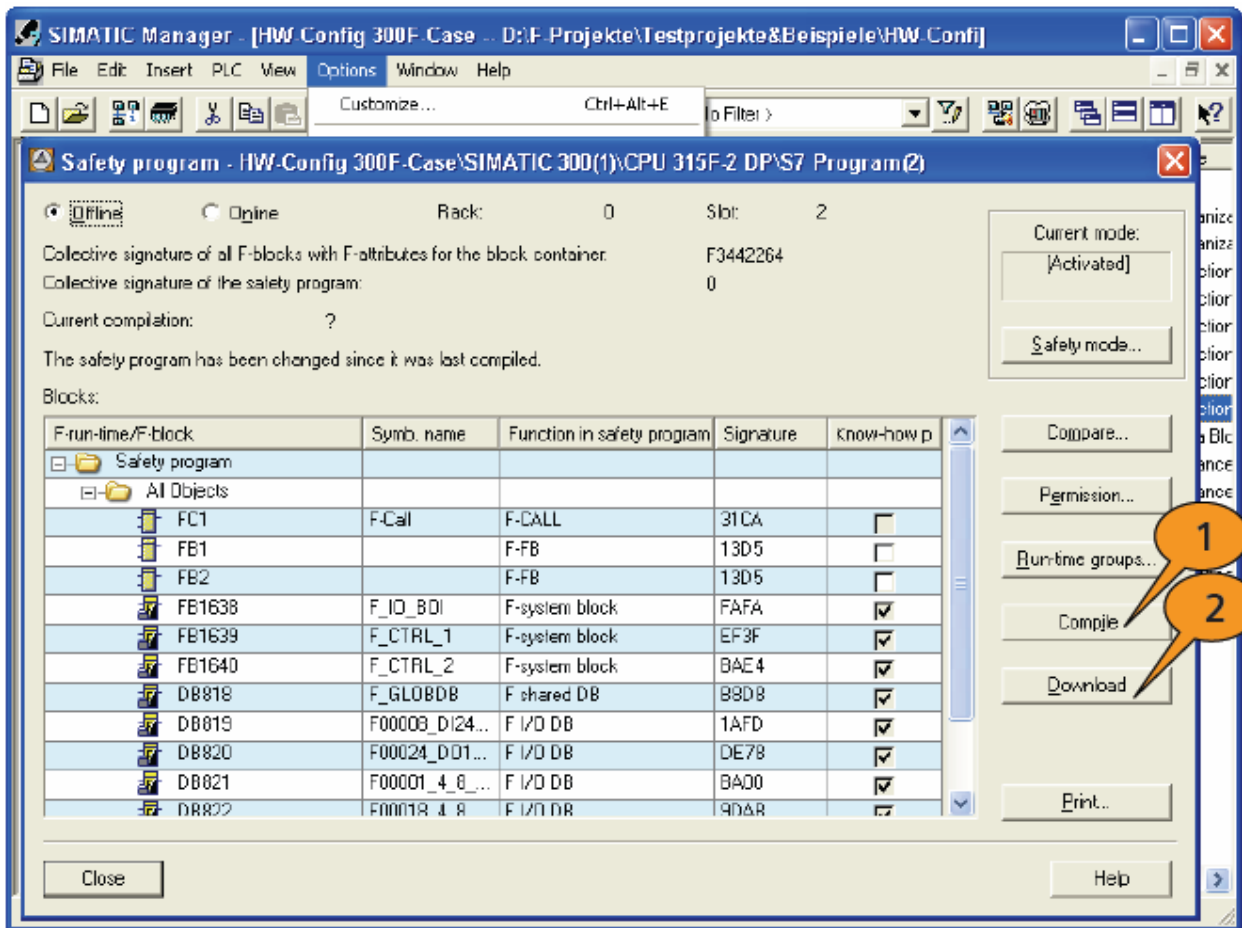
Obr 3.6 Vložení aplikačního bloku do FB

Následuje definování F – runtime pravidel : v Simatic Manager Options vybereme z nabídky Edit Safety program. Objeví se dialogové okno, ve kterém klikneme na tlačítko „Run – Time Groups“. Otevře se nám další okno, kde klikneme na „New“ a poté se nám ukáže poslední okno, ve kterém už můžeme definovat runtime pravidla.



Obr 3.7 Nastavení runtime pravidel

Generování a download failsafe programu : v Simatic Manager Options vybereme z nabídky Edit Safety program, otevře se nám dialogové okno, ve kterém klikneme na Compile. Pokud vše proběhne bez problémů, je možné takto vytvořený program již nahrát do CPU pomocí tlačítka „Download“ .



Obr 3.8 Kompilace a download safety programu

## 4. Sestava instalovaná na katedře

„Hluboká“ lišta s bezpečnostní sběrnici

zdroj PS307-5A

CPU315F-2DP (315-6FF01-0AB0)

IM153-2 (153-2BA00-0XB0)

Safety protector (195-7KF00-0XA0)

I/O modul SM326 DI24xDC24V (326-1BK00-0AB0)

I/O modul SM326 DO10xDC24V/2A (326-2BF01-0AB0)

Zdroj a CPU jsou samostatně a ostatní zařízení jsou umístěna na bezpečnostní sběrnici.

Komunikace mezi počítačem a CPU je zajištěna pomocí CP5611(MPI) a komunikace mezi CPU a IM 153-2 probíhá pomocí CP5611(Profibus). Komunikace mezi dalšími moduly je již zajišťována pomocí bezpečnostní sběrnice, na které jsou umístěny společně IM 153 – 2 a I/O moduly.

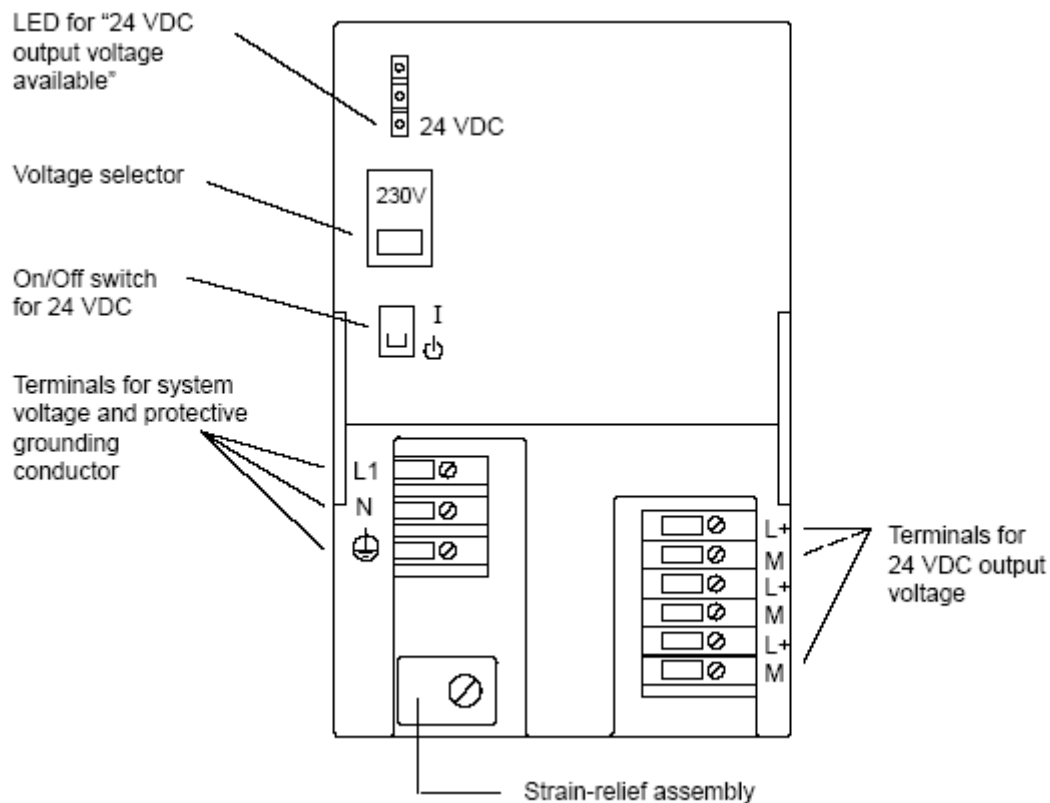
U I/O modulů je nutno přivést ještě externí napájení samotných vstupů a výstupů. Správné zapojení bude signalizováno rozsvícením příslušných LED diod a používáme-li moduly v safety modu bude svítit i LED dioda SAFE. Bez tohoto externího napájení, i když máme nastaven safety mod, tato dioda svítit nebude.

## 4.1 Zdroj PS307 – 5A

Výstupní proud – 5A

Výstupní napětí – 24V DC

Vstupní napětí – 120/230V AC 50/60 Hz



Obr 4.1 Přední strana PS307 – 5A

**4.2 IM153-2** je zařízení z modulové řady ET 200M, patřící mezi standardní moduly, které slouží ke spojení standardních modulů s bezpečnostními.

Přední panel vlevo se zavřenými a vpravo s otevřenými dvířky, pod kterými je vidět konektor pro připojení PROFIBUSu. Dále se tam nalézá napájení modulu 24V DC a přepínač sloužící k nastavení PROFIBUS adresy.

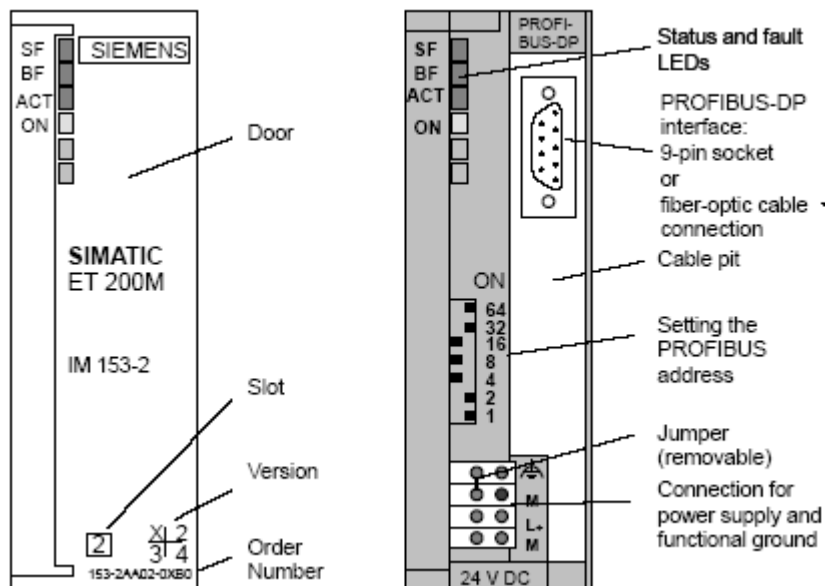
Signalizační LED diody:

SF – systémová chyba

BF – chyba v komunikaci

ACT – modul je aktivní v redundantním modu

ON – modul je připojen ke zdroji 24V DC



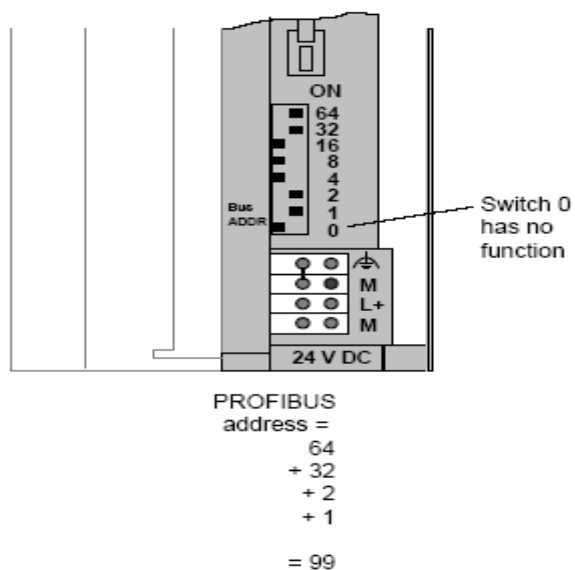
Obr 4.2 IM 153 - 2

Nastavení PROFIBUS adresy : tuto adresu je možno volit v rozsahu 1 – 125, kdy 125 je nastaveno v okamžiku, když všechny části přepínače jsou přepnuty vpravo.

Požadovaná adresa se nastaví kombinací jednotlivých přepínačů, kdy například na obrázku je nastavena adresa na „99“.

Přepínač „0“ nemá žádnou funkci, protože adresa „0“ neexistuje.



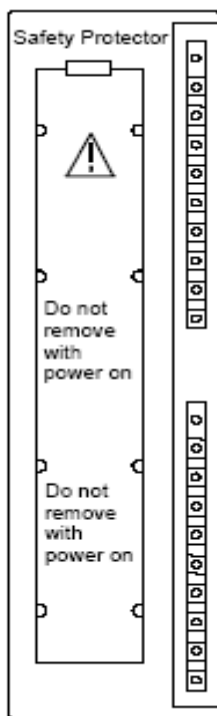


Obr 4.3 Přepínač na zadní straně I/O modulů

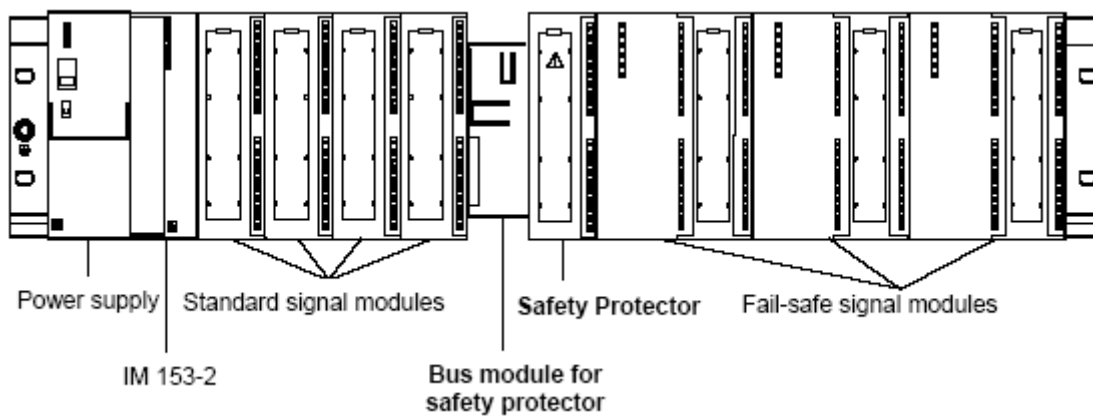
### 4.3 Safety protector slouží k hlídání přepětí mezi standardními a fail-safe moduly

K zajištění přepět'ové ochrany v safety modu je potřeba zajistit následující :

- všechny standardní signálové moduly umístit vlevo a všechny fail-safe signálové moduly umístit vpravo od safety protectoru.
- uzemnit RACK
- spojit safety protector s funkční zemí. To tak, že spojíme piny 19 a 20 safety protectoru s uzemněným RACKem pomocí co nejkratšího kabelu o průřezu  $1.5\text{mm}^2$ .



Obr 4.4 Přední panel safety protektoru



Obr 4.5 Umístění standardních a fail-safe modulů

Obrázek 4.5 ukazuje možnost zapojení signálových modulů na bezpečnostní sběrnici, kdy všechny standardní moduly jsou umístěny vlevo od safety protektoru a bezpečnostní moduly jsou vpravo, čímž je zajištěna správná funkce safety protektoru, který tak může řádně plnit svoji funkci.

## 4.4 Digitální moduly

Tři bezpečnostní, digitální moduly z S7-300 modulové řady jsou k dispozici pro spojení s digitálními senzory/kodéry.

Tři digitální moduly jsou : SM 326 – DI 24 x 24 V DC s diagnostikou přerušení

SM 326 – DI 8 x NAMUR s diagnostikou přerušení

SM 326 – DO 10 x 24 V DC/2A s diagnostikou přerušení

**SM326 DI24xDC24V :** 24 vstupů rozdělených do skupin po 12-ti

Napájení je 24V DC

Nutné externí napájení vstupů

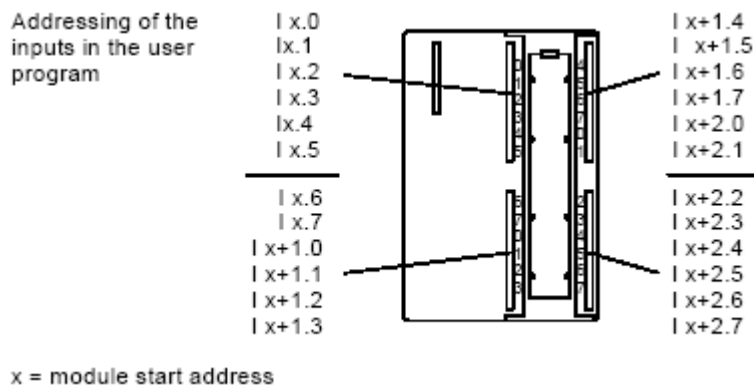
Safety mód signalizován rozsvícenou LED diodou „SAFE“

Chyba na zařízení signalizována rozsvícenou LED diodou „SF“

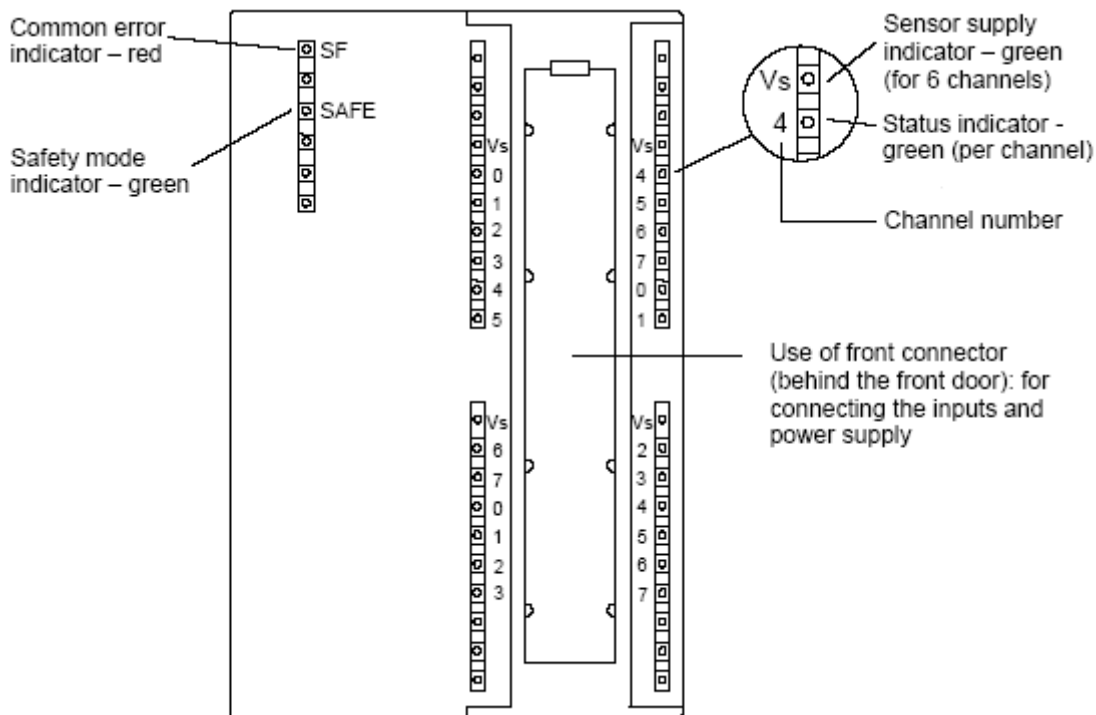
Umožňuje práci ve standardním i safety modu

Připojení vstupů je možno jedno- a nebo dvou- vodičově

Rekonfigurace při běhu pouze ve standardním módu



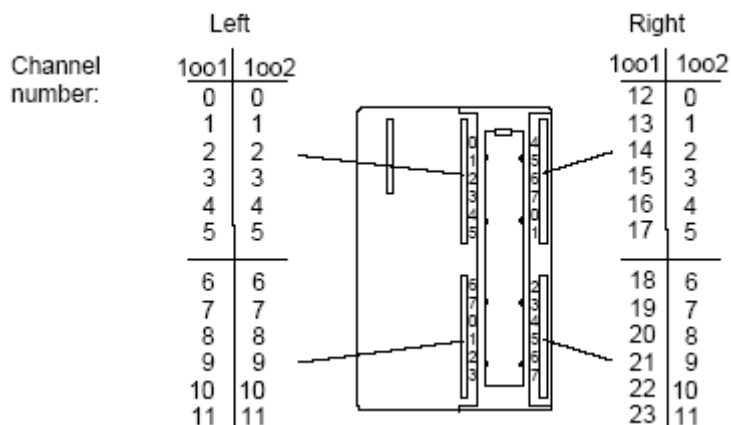
Obr 4.6 Adresování vstupů u SM 326 DI



Obr 4.7 Přední panel SM 326 DI

Je-li modul v safety modu a nevyskytují se na něm žádné chyby, jsou rozsvíceny zelené LED diody SAFE a všechny Vs, které signalizují připojené externí napájení vstupů.

Číslování kanálů podle zvoleného způsobu připojení senzorů : levé sloupce s označením 1001 představují jednovodičové zapojení a pravé sloupce s označením 1002 představují dvou vodičové zapojení vstupů tohoto modulu.



Obr 4.8 Značení vstupů při jedno a dvou vodičovém zapojení

**SM326 DO10xDC24V/2A** : 10 výstupů rozdělených do dvou skupin po 5-ti

Výstupní proud 2A

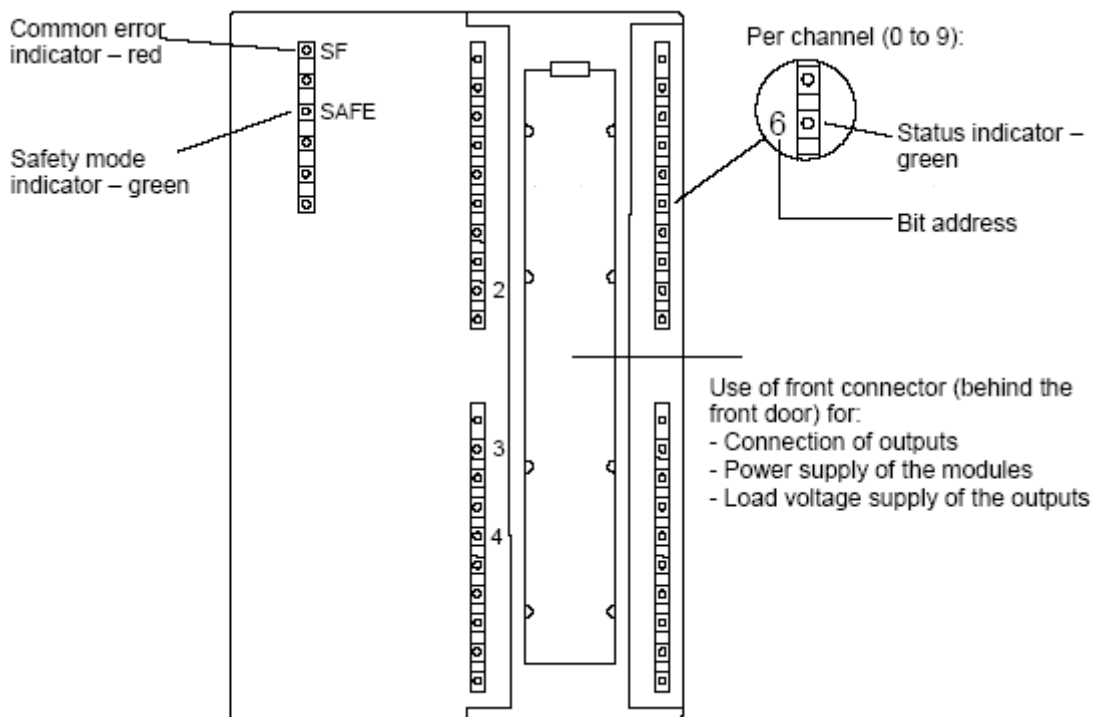
Napětí je 24V DC

Nutné externí napájení výstupů

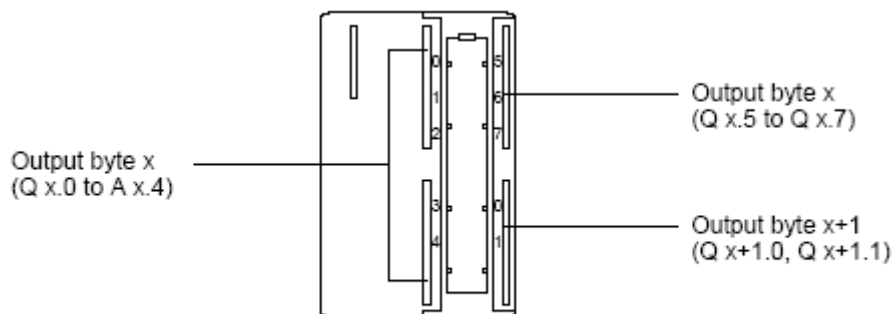
Safety mód signalizován rozsvícenou LED diodou „SAFE“

Chyba na zařízení signalizována rozsvícenou LED diodou „SF“

Umožňuje práci ve standardním i safety modu



Obr 4.9 Přední panel SM326 DO



x = Modules start address

Obr 4.10 Umístění kanálů podle adres

## 5. Distributed Safety F – Library

Obsahuje : F – aplikační bloky jsou obsažené v F – Application Blocks

F – systémové bloky a F – sdílené DB jsou obsažené v F – System Block

### 5.1 F – Application Blocks

Přehled :	FB 179	F_SCA_I	poměr hodnot datového typu INT
	FB 181	F_CTU	vzestupné čítání
	FB 182	F_CTD	sestupné čítání
	FB 183	F_CTUD	obousměrné čítání
	FB 184	F_TP	vytvoření pulsu
	FB 185	F_TON	spouštění časové prodlevy
	FB 186	F_TOF	ukončování časové prodlevy
	FB 187	F_ACK_OP	fail-safe potvrzení
	FB 188	F_2HAND	obouruční monitorování
	FB 189	F_MUTING	potlačení
	FB 190	F_1oo2DI	dvouvodičové připojení vstupů
	FB 211	F_2H_EN	obouruční monitorování s povolením
	FB 212	F_MUT_P	paralelní potlačení
	FB 215	F_ESTOP1	záchranné tlačítko STOP
	FB 216	F_FDBBACK	monitorování odezvy
	FB 217	F_SFDOOR	monitorování bezpečnostních dveří
	FB 223	F_SENDDP	posílání dat přes PROFIBUS DP
	FB 224	F_RCVDP	přijímání dat přes PROFIBUS DP
	FB 225	F_SENDS7	pro CPU 4xxF, posílání dat přes S7 spojení
	FB 226	F_RCVS7	pro CPU 4xxF, přijímání dat přes S7 spojení
	FC 174	F_SHL_W	posun o 16 bitů doleva
	FC 175	F_SHR_W	posun o 16 bitů doprava
	FC 176	F_BO_W	převod z dat.typu BOOL do dat.typu WORD
	FC 177	F_W_BO	převod z dat.typu WORD do dat.typu BOOL
	FC 178	F_INT_WR	zápis hodnoty dat.typu INT nepřímo do F-DB
	FC 179	F_INT_RD	čtení hodnoty dat.typu INT nepřímo z F-DB

Tyto bloky slouží k vytváření vlastního uživatelského programu. S jejich pomocí a s použitím standardních prvků lze vytvořit bezpečnostní program dle požadavků.

## 5.2 F – System Blocks

Přehled :

- F\_CTRL\_1
- F\_CTRL\_2
- F\_IO\_BOI
- FSIO\_BOI
- F\_RTGCO2
- FISCA\_I
- FICTU
- FICTD
- FICTUD
- FITP
- FITON
- FITOF
- FI2HAND
- FIMUTING
- FI1oo2DI
- FI2H\_EN
- FIMUT\_P
- FIACK\_OP
- FISHL\_W
- FISHR\_W
- FIBO\_W
- FIW\_BO
- FIINT\_WR
- FIINT\_RD

Tyto bloky jsou automaticky přidávány, když je safety program kompilován k vytvoření vykonatelného safety programu.

**5.3 F – Shared DB** jsou bezpečnostní bloky, které sdílí veškerá data z bezpečnostního programu a navíc informace potřebné F – systémem. V okamžiku, kdy v HW Config uložíme a zkompilujeme konfiguraci, jsou F – Shared DB automaticky vloženy.

Pro S7 Distributed Safety je také možno si vytvořit vlastní bezpečnostní knihovnu.

Postup vytvoření vlastní F – knihovny : - v Simatic Manager zvolíme File -> New

- v „Libraries“ zvolíme „F - Library“ z nabídky „Type“.

- této knihovně zvolíme jméno, specifikujeme cestu, kde budou soubory.

- zavřeme dialogové okno stiskem tlačítka“OK“ a bezpečnostní knihovna by měla být vytvořena.



## 6. Práce na reálném zařízení

### 6.1 SM 326 DI a SM 326 DO

Při demonstrování použití bezpečnostní knihovny se v laboratoři vyskytl problém, který se bohužel nepodařilo odstranit.

K realizaci bylo použito následujícího hardwaru :

PS 307 – 5A

CPU 315F-2DP (315-6FF01-0AB0)

IM 153-2 (153-2BA00-0XB0) bez paměťové karty

Safety protector (195-7KF00-0XA0)

I/O modul SM326 DI24xDC24V (326-1BK00-0AB0)

I/O modul SM326 DO10xDC24V/2A (326-2BF01-0AB0)

CPU nebylo umístěno na safety sběrnici, ale zvlášť a s IM153 - 2 bylo spojeno přes PROFIBUS . Ostatní moduly byly umístěny na společné safety sběrnici. Piny 19 a 20 na safety protectoru byly uzemněny a u I/O modulů bylo zapojeno externí napájení přivedené na příslušné konektory.

Pokud se systém používal ve standardním modu, tak i přes chybovou hlášku uvedenou níže I/O moduly žádnou systémovou chybu pomocí LED diod nesignalizovaly.

Problém nastal v okamžiku, kdy se I/O moduly přepnuly ze standardního do safety modu. Před přechodem do safety modu je nutné vyjmout I/O moduly a na zadní straně pomocí DIL přepínače nastavit adresu. Na každém modulu musí být jiná adresa. Poté je možné vrátit moduly do svých pozic a pokračovat v nastavování softwarově.

Když se pustilo CPU do RUN modu bylo bez chyb. Také modul IM153 - 2 byl po startu bez chyb a svítily na něm ON a ACT LED diody , žádné chybové diody. Ale I/O moduly nepracovaly a svítily na nich chybové SF LED diody, které značily nějakou systémovou chybu.

Poté co se program HW Config přepnul z offline do online režimu, bylo možné se podívat na I/O moduly a najít informace týkající se nefunkčnosti modulů.

V „modulu information“ v „diagnostic buffer“ pro obě I/O karty byly viděny následující chybové hlášky :

V safety modu:

Event 1 of 3: Event ID 16# F980:8031

Loss of Communication

External error, Incoming event

Event 2 of 3: Event ID 16# F980:0201

Monitoring time for data message frame exceeded

External error, Incoming event

Event 3 of 3: Event ID 16# F580:8006

Module not Assigned Parameters

Internal error, Incoming event

Ve standardním modu se objevovala pouze jedna chybová hláška:

Event 1 of 1: Event ID 16# F580:8006

Module not Assigned Parameters

Internal error, Incoming event

Tento problém byl nejprve řešen pomocí helpů dostupných u jednotlivých programů v kombinaci s manuály. Když toto nevedlo k řešení, dalším krokem byla technická podpora od výrobce, tedy u Siemensu. Nejprve českého a poté i zahraničního, kdy v obou případech jim byly dodány veškeré možné informace týkající se problému. Bohužel ani tato cesta se neukázala být tou správnou, a tak řešení problému, kdy I/O moduly nepracují v safety modu, nebylo nalezeno.

## 6.2 Wago

Poté, co se nepodařilo provést demonstraci bezpečnostních funkcí na zařízení od firmy Siemens, byly I/O moduly od Siemensu nahrazeny zařízením od firmy Wago. Pomocí Profibusu byla tato zařízení propojena s CPU 315F – 2 DP.

Postup při vytváření aplikace v S7 Distributed Safety pro moduly Wago je stejný, jako v předchozím případě pro moduly Simatic.

Moduly Wago byly sestaveny do následující konfigurace :

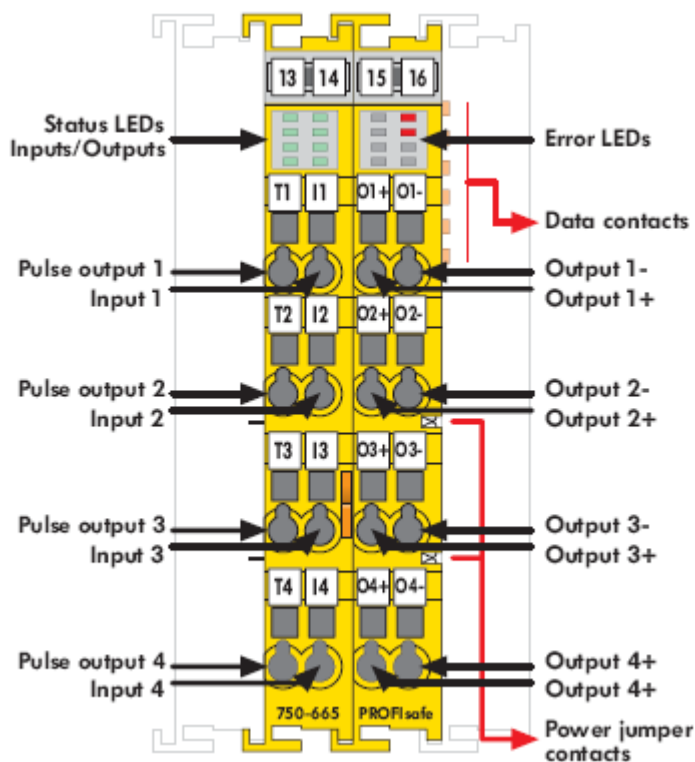
- 750 – 833 programovatelný komunikační modul
- 750 – 400 2-kanálový binární vstupní modul DC 24V 3ms
- 750 – 402 4-kanálový binární vstupní modul DC 24V 3ms
- 750 – 512 2-kanálový výstupní reléový modul AC 230V, DC 30V
- 750 – 665 digitální bezpečnostní modul pro ProfiSafe
- 750 – 600 zakončovací modul

U těchto modulů bylo nutné také přivést napájení 24V DC, které se připojilo na programovatelný komunikační modul k příslušným kanálům.

V programu HW Config byla tato sestava umístěna místo SM 326 I/O modulů. Bylo nutné v tomto programu nastavit Profibus adresu a zvolit ji stejnou, jaká byla nastavena na modulu 750 – 833 pomocí dvou přepínačů. Tyto přepínače umožňují nastavení adresy v rozmezí od 1 do 99, protože na jednom přepínači se nastavují jednotky a na druhém desítky, proto je možné s jejich pomocí dosáhnout až adresy 99. Z katalogového listu byla vytvořena sestava totožná s tou reálnou. Ale poté se objevily opět stejné problémy jako v případě zařízení Sikativ. Po nahrání konfigurace do CPU se objevily stejné potíže jako s předchozím zařízením. I v případě Wago modulů docházelo k chybě při komunikaci, která byla signalizována rozsvícenou chybovou diodou na 750 – 665 failsafe modulu.

**Modul 750 – 665** - jedná se o failsafe modul od společnosti Wago, obsahující 4 digitální vstupy a 4 digitální výstupy.

U tohoto modulu je také nutné nastavit PROFIsafe adresu, kterou je možné nastavit na přepínači umístěném na boku modulu. Proto je nutné ji nastavit ještě než spojíme moduly v jeden celek, abychom se vyhnuli pozdější demontáži a nastavování adresy.



Obr 6.1 Modul 750 – 665

PROFIsafe parametry u modulu 750 – 665 umožňují provést některá nezbytná nastavení modulu.

Jedná se například o parametr  $F\_Sil$ , u kterého je možno nastavit úroveň SIL2 nebo SIL3, které říkají kolik poruch a v jakém časovém období je přípustných u daného systému. Dalším parametrem, který je možno u tohoto modulu nastavit je parametr  $F\_Par\_Version$ . U tohoto parametru se nastavuje použitá verze PROFIsafe.

Další parametry :

- $F\_Check\_SeqNr$
- $F\_CRC\_Length$
- $F\_WD\_Time$

## 7. Závěr

Programovatelné logické automaty se stále více uplatňují v řízení a ovládání různých systémů, tím dochází k zautomatizování výrobního procesu. Při práci jsou kladeny vysoké nároky na bezpečnost provozu zejména s ohledem na lidské zdraví a zde právě nacházejí uplatnění bezpečnostní funkce PLC, jejichž úkolem je, aby nedocházelo k zraněním obsluhujícího personálu, a aby nedocházelo k přerušení výroby.

Při demonstraci použití knihovny bezpečnostních funkcí na PLC S7 315F – 2DP se vyskytl problém, který se nepodařilo odstranit ani s pomocí technické podpory výrobce modulů. O pomoc jsem žádal, jak zastoupení výrobce v České republice, tak přímo výrobce v Německu. Ani v jednom případě se nepodařilo získat informace vedoucí k odstranění daného problému a splnění zadaného úkolu. Pak jsem vyměnil moduly od Siemensu a nahradil je moduly od Waga, ale i s těmito moduly se objevoval podobný problém.

Budoucnost těchto systémů je zajištěna díky požadavkům a zpřísnování pravidel pro bezpečnost obsluhy, okolního prostředí a technologií.

## 8. Seznam použité literatury

Tyto manuály jsou volně stažitelné ze stránek [www.siemens.com](http://www.siemens.com) , [www.siemens.cz](http://www.siemens.cz)

s7300f\_d.pdf

s7300f\_e.pdf

S7 Distributed Safety Configuring and Programming.pdf

S7 Distributed Safety Getting Started.pdf

Distributed\_Safety.pdf

Distributed Safety - priklad.pdf

Safety Integrated – uvod.pdf

Safety Integrated – prehled.pdf

ET200M\_e.pdf

Manuály z <http://dce.felk.cvut.cz/rs/>

STEP7Strucne.pdf

Rychly\_nastup\_do\_simatic\_manageru.pdf

Online katalog na [www.wago.com](http://www.wago.com)

Manuál v technické dokumentaci na [www.wago.cz](http://www.wago.cz)

m066500e.pdf