



**Rockwell
Automation**

Innovation & Technology Forum

Session title: T70 – Introduction to the Allen-Bradley® Integrated Safety System

Karel Stibor

Solution Architect Safety

Agenda

1

PŘEHLED HW
SYSTÉMY S INTEGROVANOU BEZPEČNOSTÍ

2

RYCHLÉ PŘEDSTAVENÍ STUDIO 5000

3

NEJČASTĚJŠÍ SW BLOKY

4

JAK VÁM MŮŽEME POMOCI

Bezpečnostní HW – vstupy

Snímání přítomnosti



Prostředky pro zjišťování přítomnosti osob

- Optoelektronické prvky
- optické bariéry (více paprsků)
- optické závory (jednopaprskové)
- laserový scanner
- Nášlapné rohože
- Bezpečnostní hrany

Bezpečnostní zámky a spínače



Spínače:

- Koncové spínače
- plastové
- kovové
- mini-spínače
- Spínače bezpečnostních krytů
- mechanické
- mechanické s uzamykáním
- magnetické
- obyčejné
- s kódováním
- RFID
- bez kódování
- s kódováním
- Klíčové pasti

Tlačítka nouzového zastavení a vypínací zařízení



Zařízení používaná k zastavení procesu v případě nebezpečí:

- tlačítka nouzového zastavení
- lankové spínače

Operátorská rozhraní



Rozhraní operátor - stroj:

- Tlačítka dvouručního ovládání
- povelové a povolovací spínače

Bezpečnostní HW – logické jednotky

Bezpečnostní relé



Jedno/dvojkanálové monitorování zařízení pro bezpečnostní aplikace

Dvě základní platformy:

- Jednoduchá bezpečnostní relé/moduly MSR
- Rozsiritelná multifunkční relé / moduly GSR

SW konfigurovatelné



Konfigurovatelné bezpečnostní zařízení až do PLe/SIL3 může být konfigurováno přes CCW nebo Studio5000 přes vestavěný USB nebo rozšiřitelný EtherNet port.

Integrované systémy



Integrovaný systém GuardLogix použitelný až do SIL3/PLe z rodiny ControlLogix & CompactLogix. Standardní a bezp. řízení na jedné platformě, s jedním softwarem, jednou sítí a jednoduchou komunikací a diagnostikou.

IO moduly



Bezpečnostní I/O na síti nebo lokální pro použití s různými platformami

Bezpečnostní HW – aktuátory

Stykače



Nuceně vedené kontakty pro připojení zpětné vazby. Široké spektrum a typů přesně pro vaši aplikaci s jednou z nejlepších hodnot B10d na trhu.

100S, 700S a 109S bezpečnostní stykače, 700 HPS paticová relé

Měniče PowerFlex



Pohony PowerFlex s volitelnou a rozšiřitelnou základní nebo pokročilou bezpečností pro rychlejší, jednodušší, více efektivní a spolehlivé aplikace

- Řada Powerflex 5
- Řada Powerflex 7

Motion Kinetix



Integrované řízení pohybů Kinetix s volitelnou a rozšiřitelnou základní nebo pokročilou bezpečností pro rychlejší, jednodušší, více efektivní a spolehlivé aplikace

- Kinetix 6000
- Kinetix 6200
- Kinetix 6500
- Kinetix 5500
- Kinetix 350 and 300

Hlavní body platformy GuardLogix®

GuardLogix® je systém s vysokým výkonem pro multidisciplinární řízení, které zahrnuje vše z nebezpečnostní řady ControlLogix®, ale rovněž zahrnuje schopnosti řídit bezpečnostní smyčky aplikace.

- Až do SIL 3, Plc při CAT 4
- Standardní, bezpečnostní, motion a další řízení v jednom CPU
- CIP Safety přes EtherNet/IP (DeviceNet)
- Certifikované bezpečnostní instrukce
- High Integrity Add-On Instrukce (bezpečnostní add-on)



5580 GuardLogix & 5380 Compact GuardLogix

Jeden systém pro standardní a bezpečnostní řízení

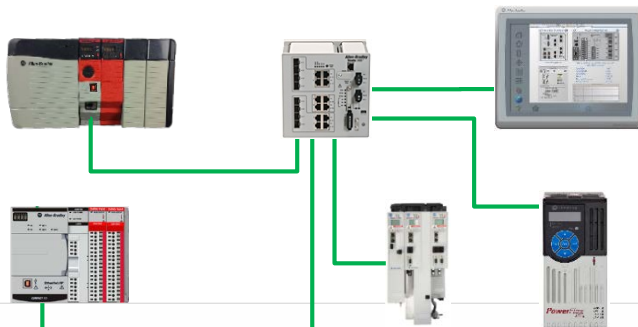
- Žádný dodatečný čas potřebný pro integraci
- Lepší, rychlejší a jednodušší diagnostika
- Nejjednodušší možné poskytování dat pro HMI

Name	Usage
CIP_Safety_Acting	Public
Reset	Local

Parameter Connections {2:0}	
Connection	\\UN01_ExampleMachine.CIP_Safe_Off_Demand
Connection	\\UN01_ExampleMachine.CIP_Safety_Demand

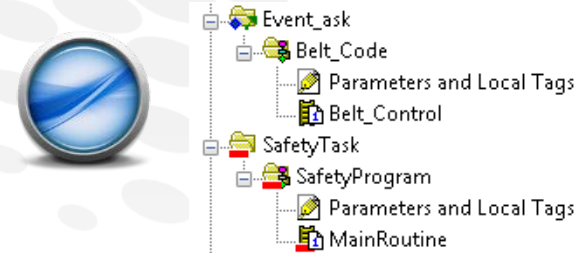
Jedna síť pro standardní a bezpečnostní řízení

- Žádná další síť nebo rozhraní pro I/O
- Schopnost kombinovat se standardními I/O



Jeden software pro standardní a bezpečnostní řízení

- Stejný vzhled a ovládání urychluje vytváření aplikace
- Flexibilita systému šetří čas



Kompatibilní a flexibilní

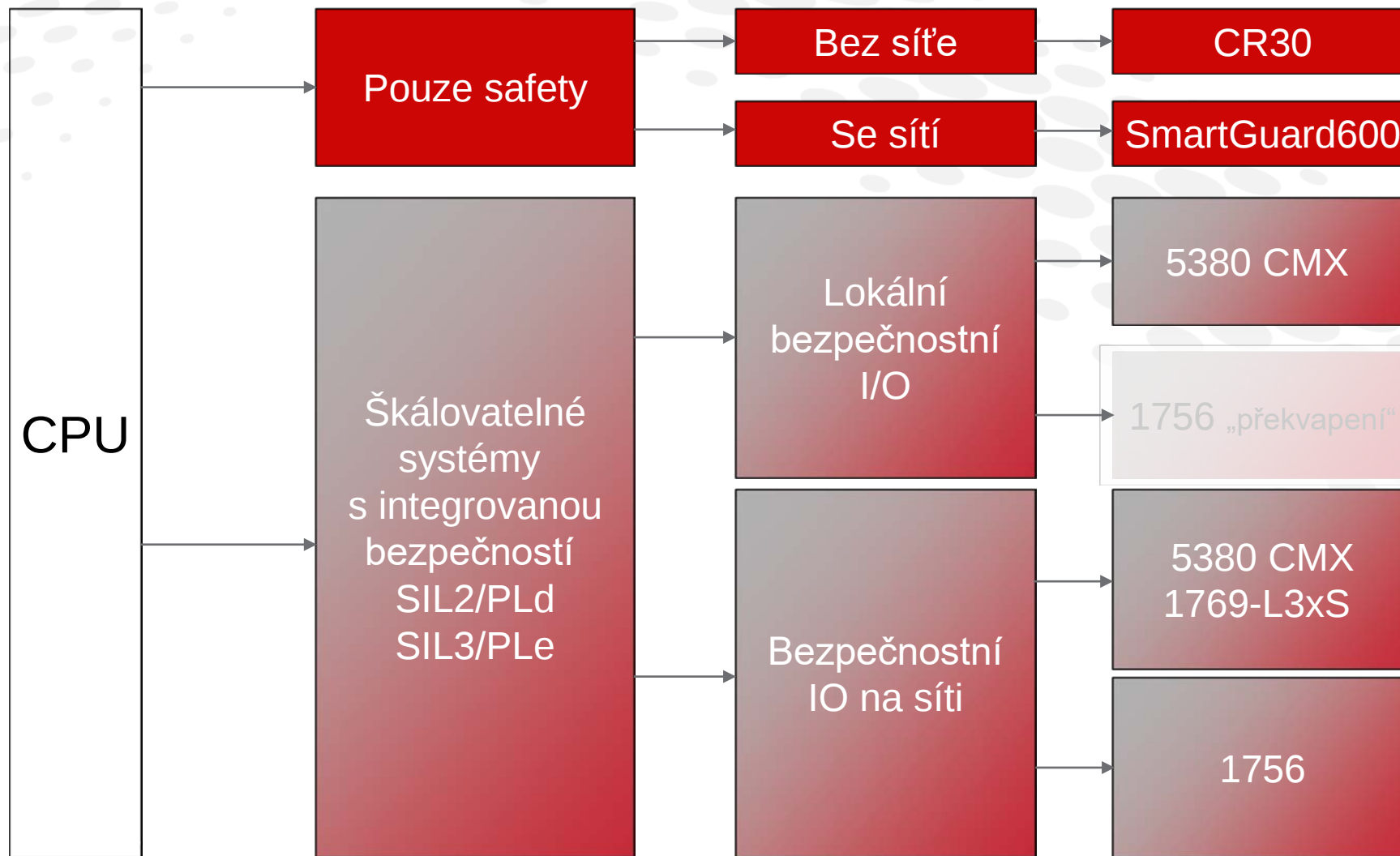
- Certifikované bezpečnostní instrukce (přes 100)
- Možnost vytvářet vlastní (HI Add-On instrukce)

Dual-channel Input Start (DCSRT)



Dual Channel Input Start (DCSRT)	
DCSRT	Safety_5
Safety Function	ENABLE PENDANT
Input Type	EQUIVALENT - ACTIVE HIGH
Discrepancy Time (Msec)	20
Enable	Safety_Enable
Channel A	Safety_Block_A1:P100Data
Channel B	Safety_Block_A1:P101Data
Input Status	Safety_Block_A1:CombinedStatus
Reset	Safety_Reset_PB

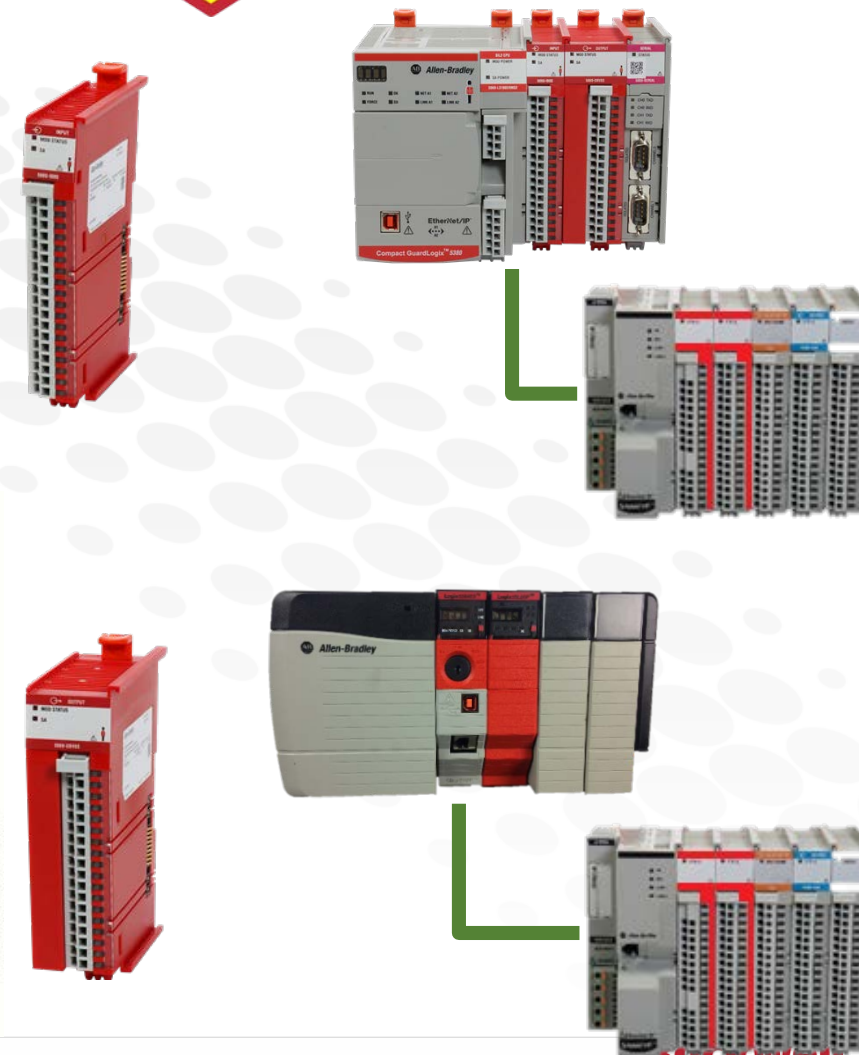
Procesory s bezpečnostním řízením



5069 Compact I/O

AFC od
06.05. 2019

- Bezpečnostní lokální karty
- Lokální I/O & distribuované I/O pro Compact GuardLogix 5380
- Distribuované I/O pro GuardLogix 5580 (brzy více...)
- Karta bezpečnostních digitálních vstupů 5069-IB8S
 - 8 jednokanálových vstupů PL d nebo
 - 4 dvojkanálové vstupy PL e
- Karta bezpečnostních digitálních výstupů 5069-OBV8S
 - Mód „Sourcing“
 - 8 jednokanálových výstupů PL d nebo
 - 4 dvojkanálové výstupy PL e
 - 4 bipolární výstupy PL e
- Obsaženo ve Studio5000 Logix Designer V32, pro nižší verze dostupné AOP ke stažení



FLEX 5000™ digitální bezpečnostní I/O



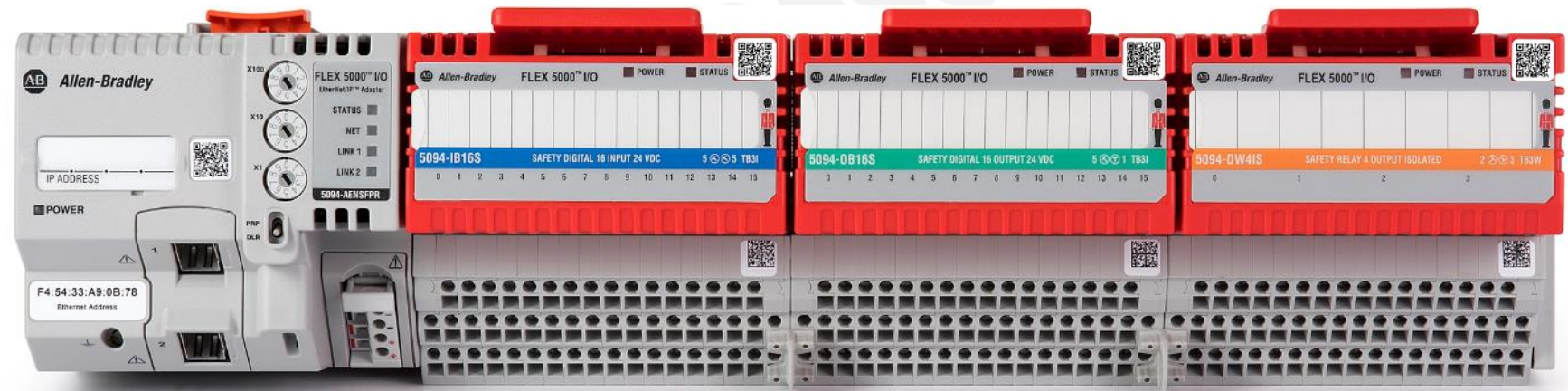
Bezpečnostní digitální výstupy

Bezpečnostní digitální vstupy

Bezpečnostní reléové výstupy

Safety Integrity Level

SIL 3, PL e, kat. 4



Distribovaná bezpečnostní aplikace
Vzdálený reset chyb
Konfigurovatelný bezpečný stav

Rozšířená diagnostika
Detekce přerušného vodiče,
kontrola teploty ...

Fail-safe aplikace
Režim nízkého, vysokého a
stálého vyžádání

Agenda

1

PŘEHLED HW
SYSTÉMY S INTEGROVANOU BEZPEČNOSTÍ

2

RYCHLÉ PŘEDSTAVENÍ STUDIO 5000

3

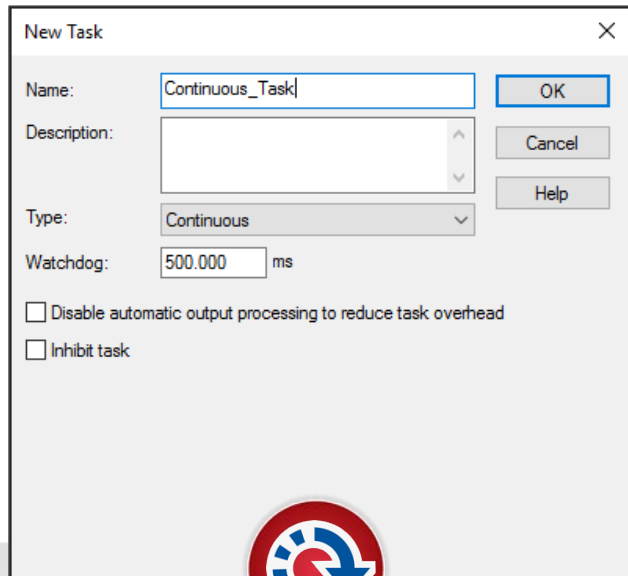
NEJČASTĚJŠÍ SW BLOKY

4

JAK VÁM MŮŽEME POMOCI

Flexibilní spoštění úloh

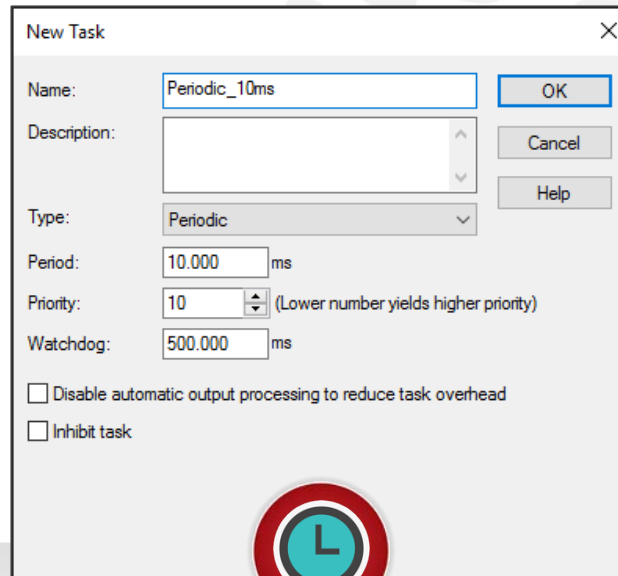
- Tři typy



The 'New Task' dialog box for a Continuous Task. The 'Name' field contains 'Continuous_Task'. The 'Type' dropdown is set to 'Continuous'. The 'Watchdog' field is set to '500.000 ms'. There are checkboxes for 'Disable automatic output processing to reduce task overhead' and 'Inhibit task', both of which are currently unchecked. The 'OK', 'Cancel', and 'Help' buttons are visible on the right.



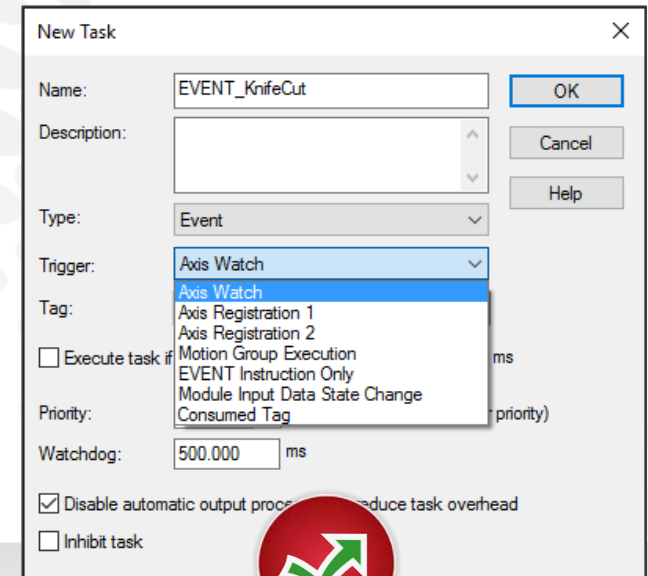
Continuous Task



The 'New Task' dialog box for a Periodic Task. The 'Name' field contains 'Periodic_10ms'. The 'Type' dropdown is set to 'Periodic'. The 'Period' field is set to '10.000 ms'. The 'Priority' field is set to '10' with a note '(Lower number yields higher priority)'. The 'Watchdog' field is set to '500.000 ms'. There are checkboxes for 'Disable automatic output processing to reduce task overhead' and 'Inhibit task', both of which are currently unchecked. The 'OK', 'Cancel', and 'Help' buttons are visible on the right.



Periodic Tasks



The 'New Task' dialog box for an Event Task. The 'Name' field contains 'EVENT_KnifeCut'. The 'Type' dropdown is set to 'Event'. The 'Trigger' dropdown is set to 'Axis Watch', and a list of options is displayed: 'Axis Watch', 'Axis Registration 1', 'Axis Registration 2', 'Motion Group Execution', 'EVENT Instruction Only', 'Module Input Data State Change', and 'Consumed Tag'. The 'Tag' field is empty. There are checkboxes for 'Execute task if', 'Disable automatic output processing to reduce task overhead', and 'Inhibit task'. The 'OK', 'Cancel', and 'Help' buttons are visible on the right.



Event Tasks

BEZPEČNOST

POHONY

Rockwell Software
Studio 5000

PROCES

DISKRÉTNÍ

BATCH

MOTION

Prostředí Studio 5000

[illegible]

Prostředí Studio 5000

Paleta instrukcí (i běžné standardní instrukce mohou použít v safety části)

Safety instrukce mohou použít POUZE v safety části, jako např. LC, DCS, SMAT, DCA, ROUT apod.

Použití bloků není limitováno počtem použití, nic se nemusí doinstalovávat, nebo přikupovat.

Prostředí Studio 5000

The screenshot displays the Rockwell Studio 5000 Logix Designer interface. On the left, the **Controller Organizer** pane shows a hierarchical tree of the project structure. Key elements are circled in red: **Controller GuardLogix**, **Controller Tags**, **Controller Fault Handler**, **Power-Up Handler**, **MainTask**, **MainProgram**, **SafetyTask**, **SafetyProgram**, **Parameters and Local Tags**, and **MainRoutine**. The main workspace shows a ladder logic diagram for **Rung 0 of 8**. The diagram includes inputs like **Zone1_LC_O1**, **Sts_Zone1_ESTOP_InputOK**, **Sts_Zone1_LC_InputOK**, **Sts_Zone1_InputsOK**, and **Cmd_Zone1_SafetyReset**. It also features a **Cmd_Zone1_OutputEnable** output. A table on the right lists channel data for **AENT_01:1.I.PIO5Data** and **AENT_01:2.I.CombinedInputStatus**. The status bar at the bottom indicates the communication software is **RSLink Classic**.

Zobrazení „tagů“ (proměnných), ne-bezpečnostní a bezpečnostní části programů.

Prostředí Studio 5000

Hlavní část okna se zobrazí logikou vybraného programu

Pokud jsem v safety-části, zobrazuje se mi vodoznak loga „GuardMaster“ – bezpečnostní HW naší firmy.

Prostředí Studio 5000

The screenshot displays the Rockwell Studio 5000 Logix Designer interface. The main window shows a ladder logic program for a safety routine, titled "SafetyProgram - MainRoutine". The program is organized into rungs, with the first rung labeled "Zone1_ESTOP.01". The interface includes a "Controller Organizer" on the left, a "Safety" tab in the top right, and a "Move/Logical" element group selected. A red circle highlights the "I/O Configuration" section in the Controller Organizer, showing the hardware structure of the system, including the 1756 Backplane, 1756-A4, and various modules like the 1756-L81ES GuardLogix, 1756-L8SP GuardLogixPart, 1756-EN2T Ethernet, and 1734-AENT/A AENT_01. The ladder logic program shows various safety-related logic, including inputs like "Zone1_ESTOP.01", "Zone1_LC.01", and "Cmd_Zone1_SafetyReset", and outputs like "Cmd_Zone1_OutputEnable".

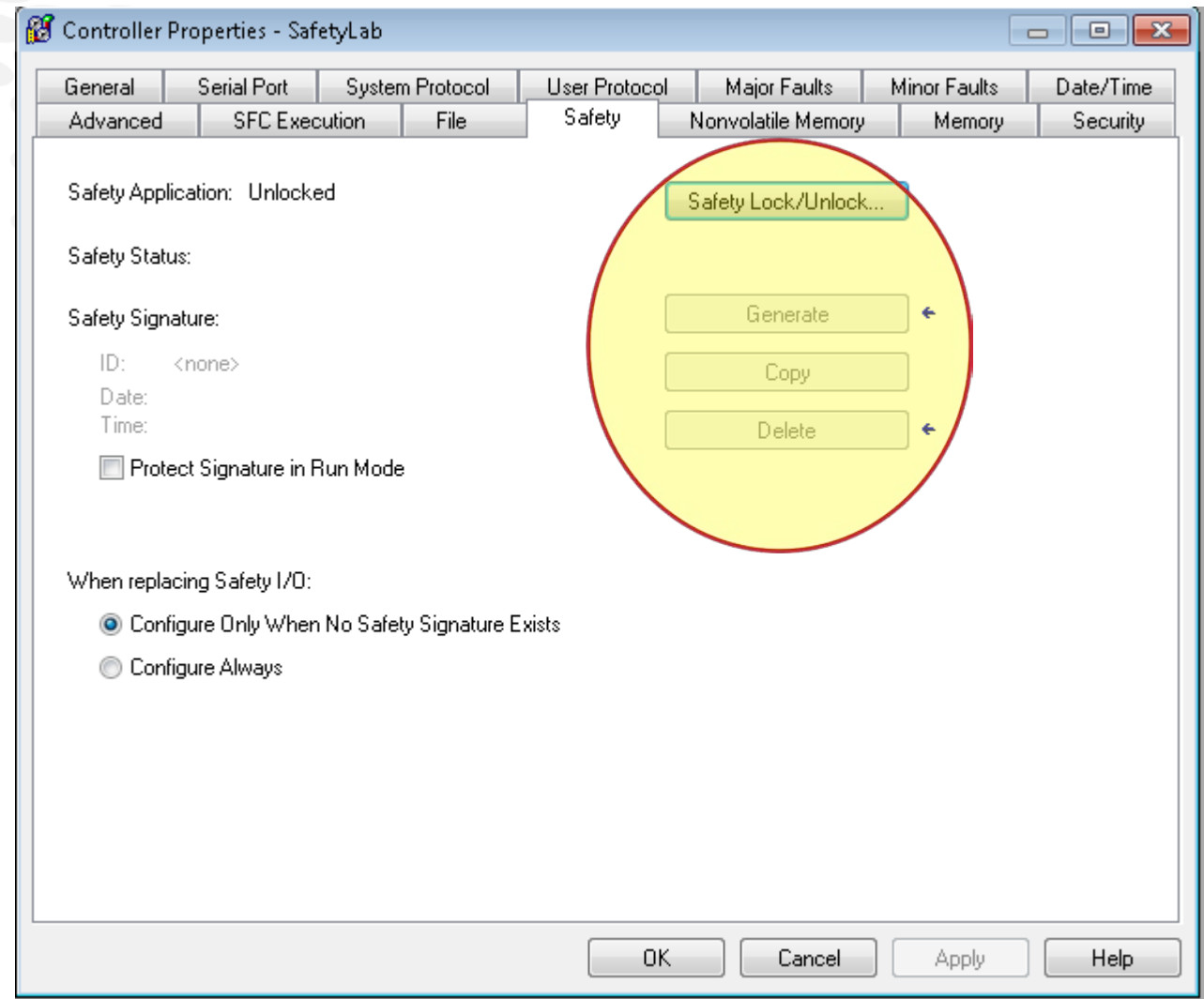
Zobrazení struktury HW v aplikaci
(jak ne-bezpečnostní, tak bezpečnostní)

Prostředí Studio 5000

Možnost zobrazit standardní zobrazení (viz. obrázek) nebo Logický organizér, kde mohu upravovat zobrazení podle logických vazeb (například IO, měnič a safety řešící zásobník materiálu bude ve stejné skupině jako standardní a safety program, které jej řídí, další část stroje v další skupině atd.)

Postup konfigurace a programování

- Nezapomeňte, že požadavky na zabezpečení aplikací je součástí legislativy již od prvních měsíců roku 2018!
- Záměrná, nebo náhodná změna SW například nesmí vést k nárůstu nebezpečí, nebo ke vzniku nových rizik na strojích...
- Aplikujte ISO TR22100-4, IEC TR 63074 a skupinu norem IEC 62443 do vašich aplikací!



Agenda

1

PŘEHLED HW
SYSTÉMY S INTEGROVANOU BEZPEČNOSTÍ

2

RYCHLÉ PŘEDSTAVENÍ STUDIO 5000

3

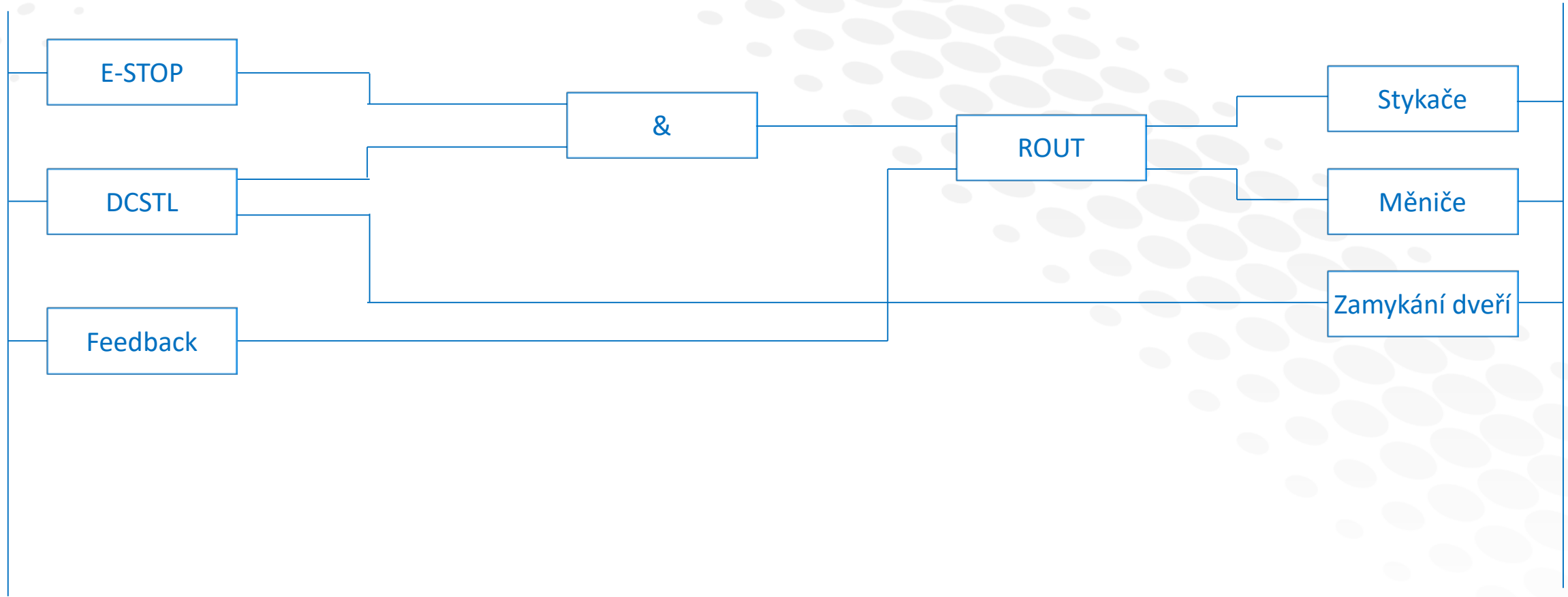
NEJČASTĚJŠÍ SW BLOKY

4

JAK VÁM MŮŽEME POMOCI

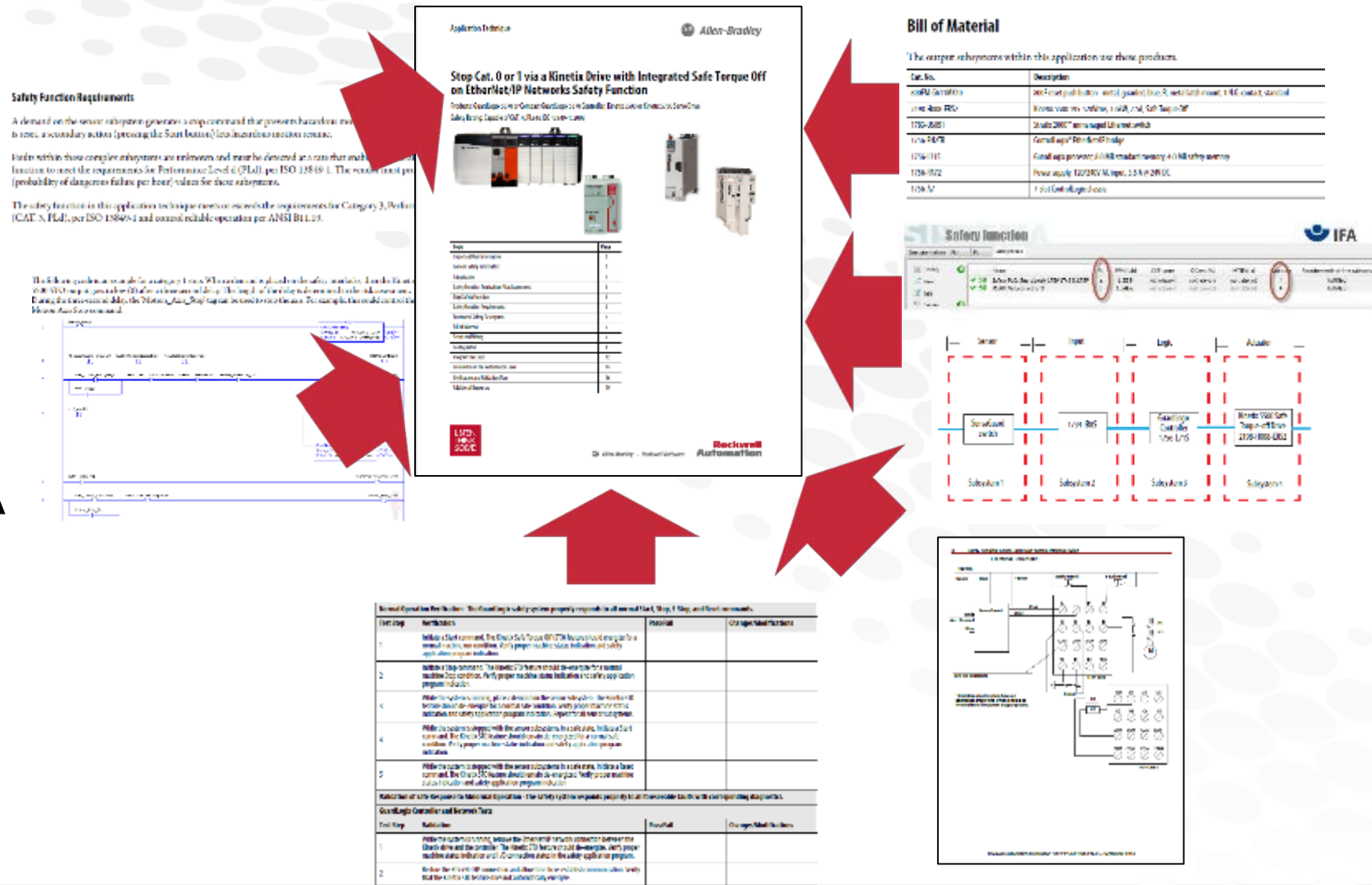
Postup konfigurace a programování

- Logické schéma bude vypadat zhruba takto:



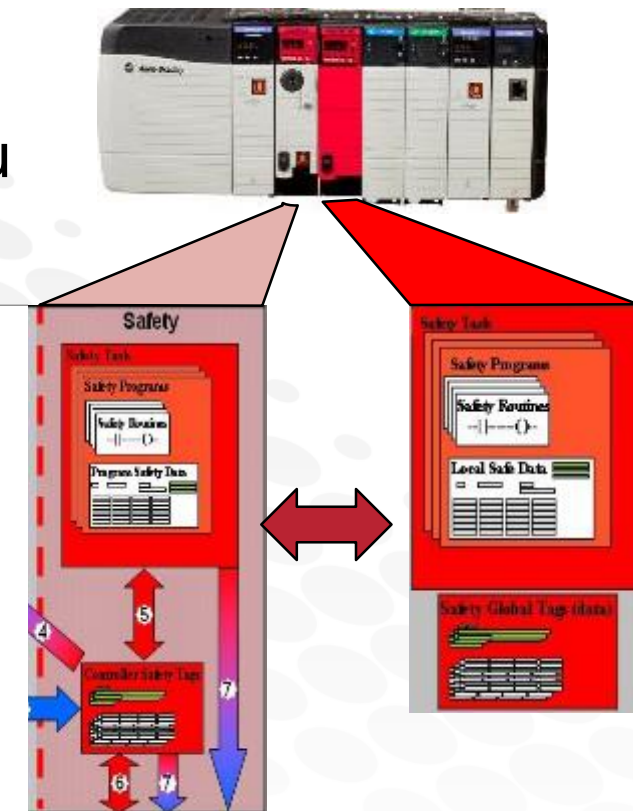
Předpřipravené bezpečnostní funkce

- Funkční popis (pro případé použití v SRD)
- Kusovník
- Zapojovací schéma
- Program/Konfigurace
- Kalkulace v SISTEMA
- Připravená Verifikace a & Validace



Jak pracuje CPU s integrovanou bezpečností

- Safety Task je PERIODICKÝ – nikdy jiný i v budoucnu
- Periodicky, primární CPU “iniciuje” sekundární CPU
- Vstupní obraz je ‘zmrazen’; nemění se během běhu programu
- Primární CPU posílá vstupní data sekundárnímu CPU
- Obě CPU provedou uživatelský kód ze „zmrazených“ dat
- Výsledky obou běhů jsou porovnány mezi sebou (primární $\leftrightarrow$ sekundární – s inverzním zpracováním)
- Pokud je výsledek správný, primární i sekundární CPU vystaví polovinu obrazu výstupních dat, z těch je sestavena zpráva pro výstupní body



Bezpečnostní „Tag“ a standardní „tag“

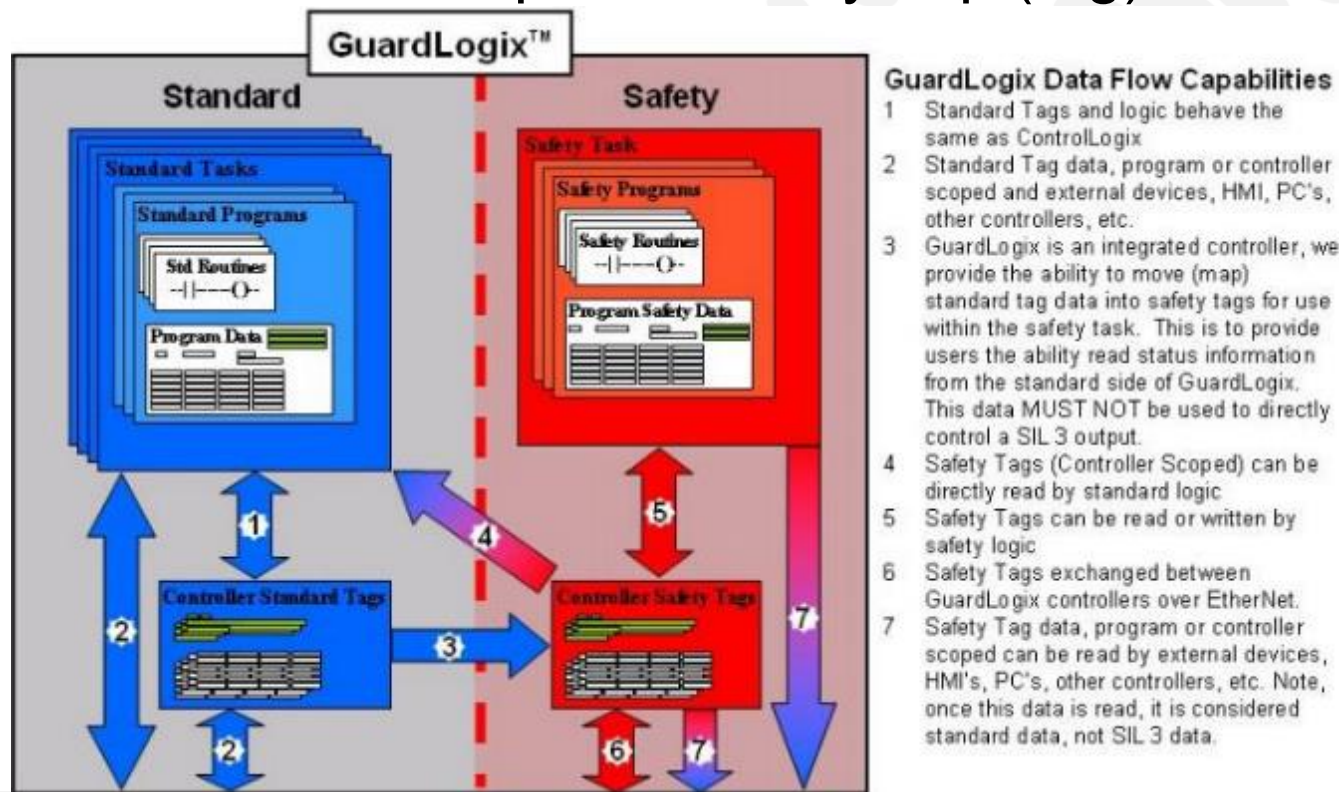
Jaký je základní rozdíl mezi bezpečnostními a standardními tagy?

- Bezpečnostní tagy jsou všechny generovány jako 1002
 - Na základě bezpečnostních I/O a Safety tasku.
 - Spravované VŽDY Safety taskem
- Standardní tagy jsou VŠECHNY generovány jako 1001
 - Na základě standardních I/O a Standardního tasku
 - Spravované většinou standardním taskem

Základní pravidla

Každé CPU má třídu „Class“ „standard“, bezpečnostní má i „safety“

- ~~Pravidlo #1 Nemohu používat standardní tagy v bezpečnostním tasku~~
- Pravidlo #2 Nemohu ovládat bezpečnostní výstup (tag) ze standardního tasku

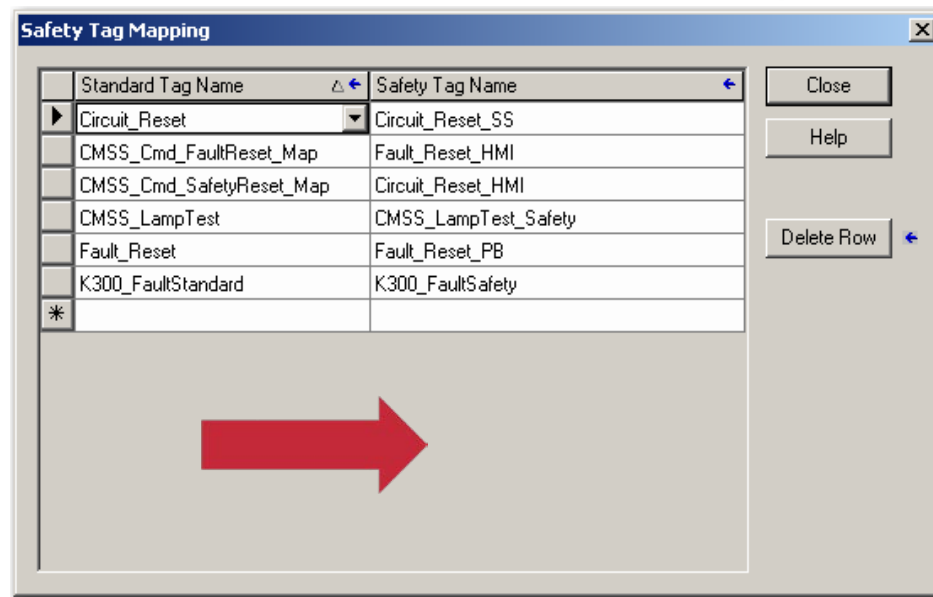


GuardLogix Data Flow Capabilities

- 1 Standard Tags and logic behave the same as ControlLogix
- 2 Standard Tag data, program or controller scoped and external devices, HMI, PC's, other controllers, etc.
- 3 GuardLogix is an integrated controller, we provide the ability to move (map) standard tag data into safety tags for use within the safety task. This is to provide users the ability read status information from the standard side of GuardLogix. This data MUST NOT be used to directly control a SIL 3 output.
- 4 Safety Tags (Controller Scoped) can be directly read by standard logic
- 5 Safety Tags can be read or written by safety logic
- 6 Safety Tags exchanged between GuardLogix controllers over EtherNet.
- 7 Safety Tag data, program or controller scoped can be read by external devices, HMI's, PC's, other controllers, etc. Note, once this data is read, it is considered standard data, not SIL 3 data.

Mapping Tool

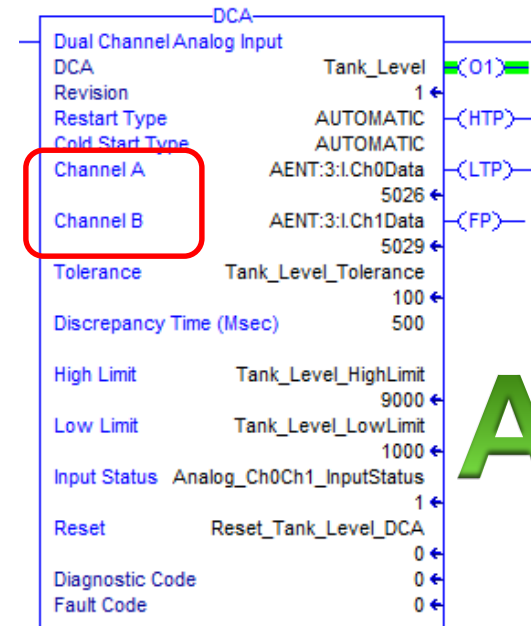
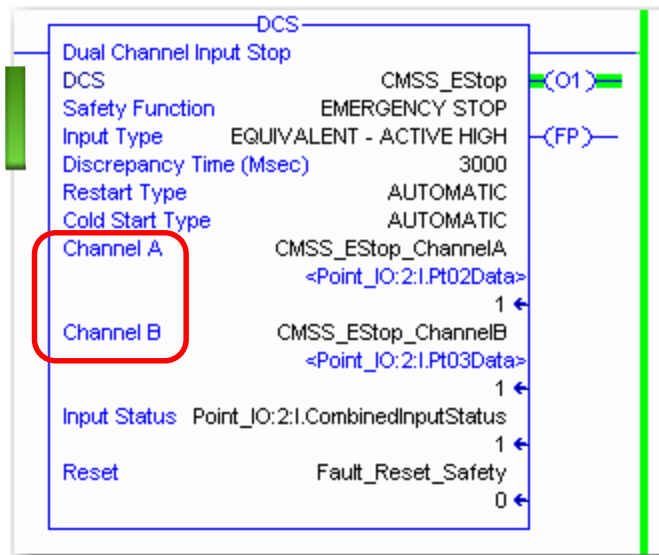
- ~~Staré pravidlo #1 Nemohu používat standardní tagy v bezpečnostním tasku~~
- Nové pravidlo #1: MOHU používat standardní tagy v bezpečnostním tasku, za použití „Mapping tool“
- Pravidlo #2 Nemohu ovládat bezpečnostní výstup (tag) ze standardního tasku



VŠECHNY certifikované bezpečnostní instrukce jsou dvojkanálové

- Dvojkanálové instrukce pomáhají diagnostice a potvrzení, že jsou kanály v rámci tolerance
- Pokud zůstanou mimo tolerance déle, než je nastaven tzv. „discrepancy time“, je deklarována chyba vstupů

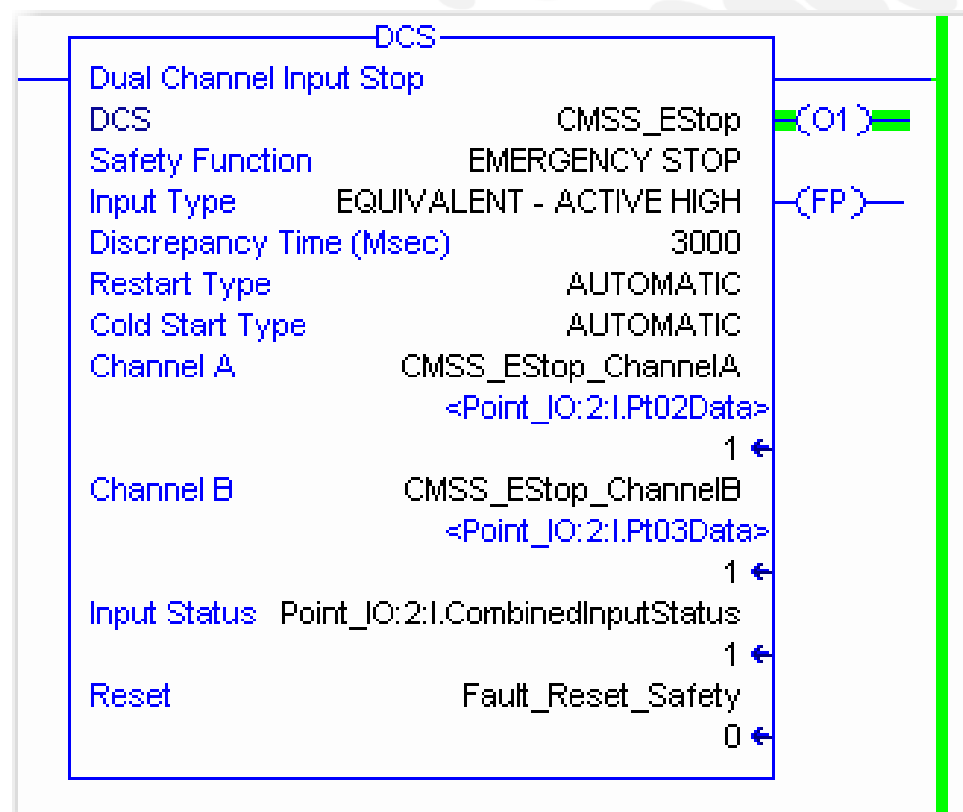
Digital



Analog

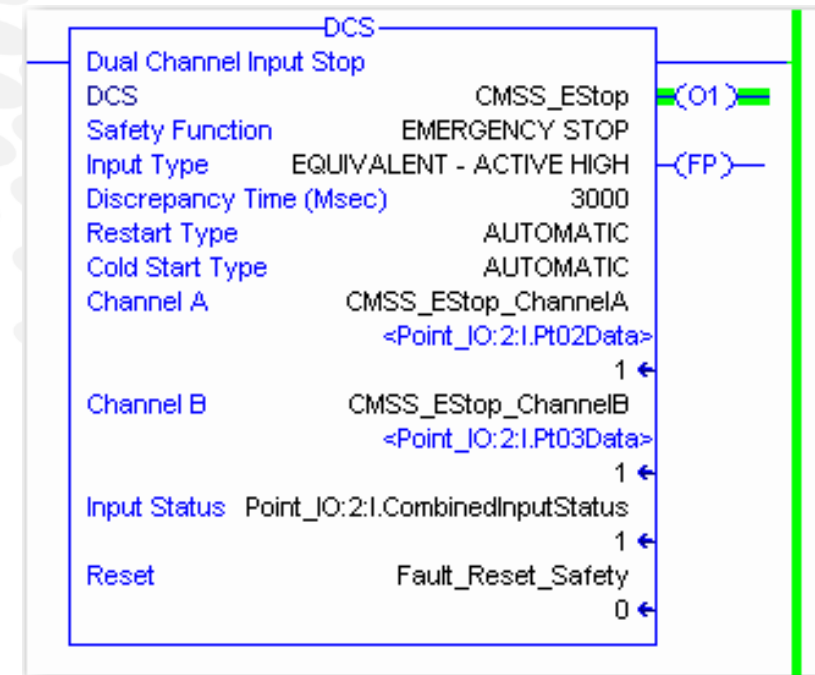
Instrukce DCS

DCS je základní vstupní instrukcí



Instrukce DCS

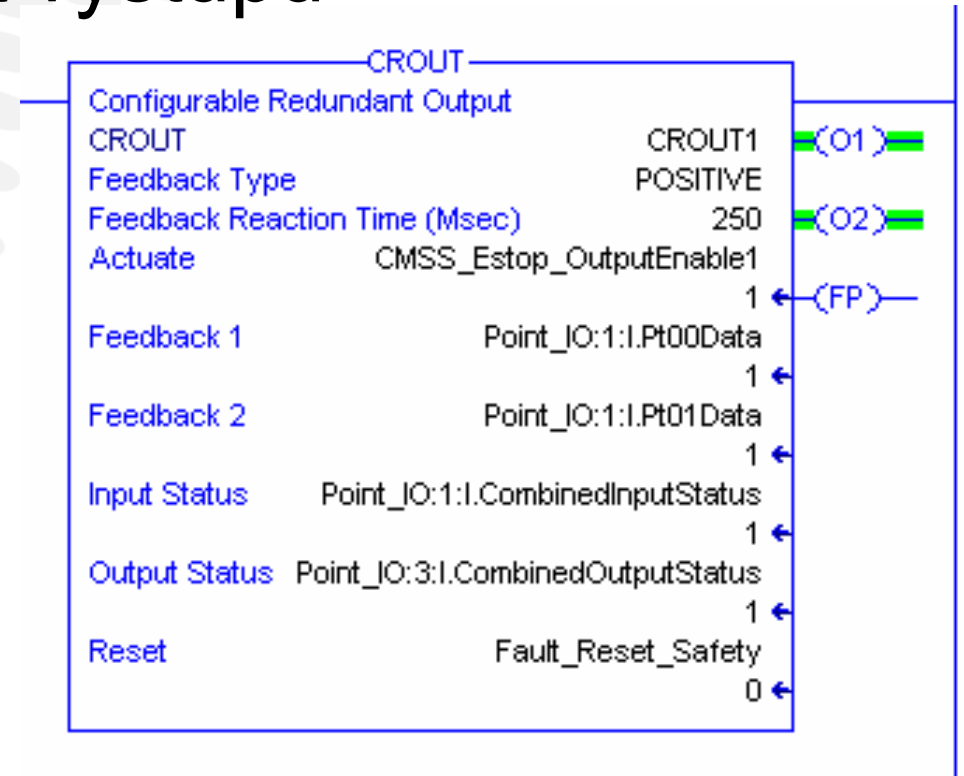
- Input Type
 - Equivalent nebo Complementary
- Discrepancy Time
 - Jak dlouho mohou být vstupy rozdílné od očekávaného stavu, než je deklarována chyba
- Restart Type
 - Je vyžadován 'Reset' pro aktivování výstupu funkce?
 - AUTOMATIC – NE
 - MANUAL - ANO
- Cold Start Type
 - Je vyžadován test bezpečnostní funkce po spuštění stroje?
 - AUTOMATIC – NE
 - MANUAL - ANO
- Input Status
 - Jsou validní data na vstupu funkce?
 - Pokud je status LO, výstup (O1) je vypnut i když jsou vstupy ChA a ChB v pořádku
- Reset
 - Reset poruch (FP)
 - Restartuje výstup (O1) pokud je Restart Type konfigurován jako „MANUAL“



Dual Channel Input Stop

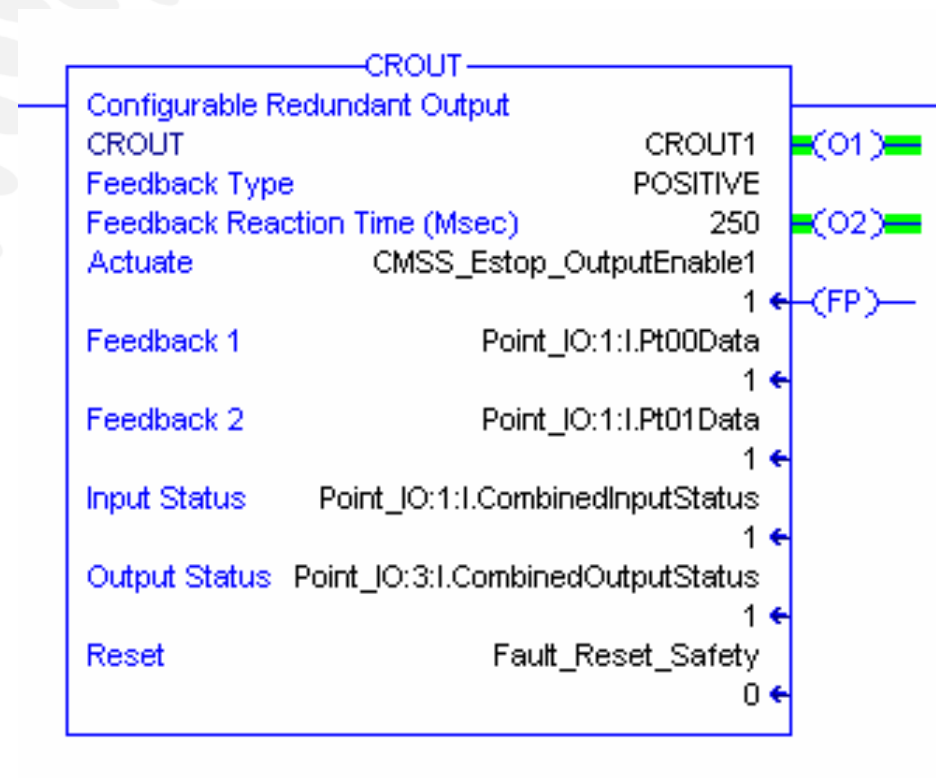
Instrukce CROUT

- Základní instrukce pro bezpečnost výstupů se zpětnou vazbou



Instrukce CROUT

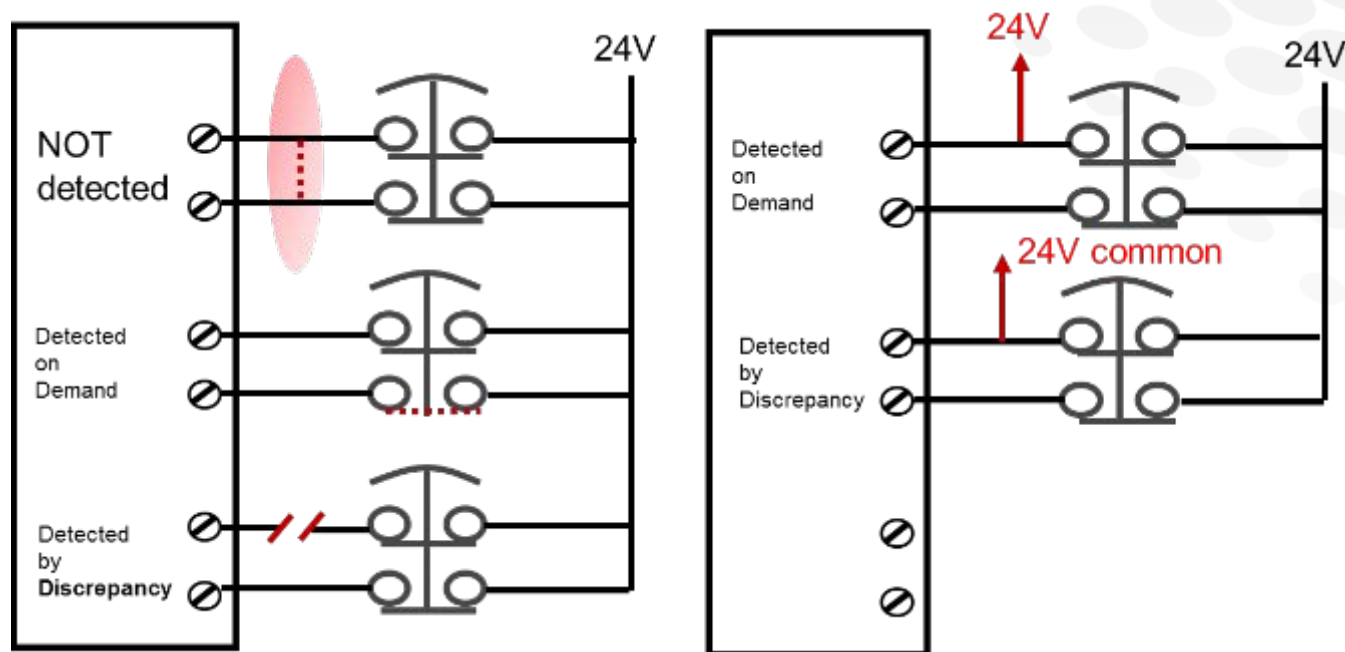
- Feedback Type
 - Positive nebo Negative
- Reaction Time
 - Jak dlouho čekat na zpětnou vazbu, před tím, než funkce deklaruje poruchu
- Actuate
 - Bez funkce restartu
 - Výstupy O1 a O2 jednoduše následují bit, pokud nejsou v bloku žádné chyby
- Input and Output Status
 - Jsou vstupní data v pořádku?
 - Jsou výstupní kanály ovládány tímto blokem a bez chyb?
- Reset
 - Resetuje chyby zpětné vazby (FP)



Configurable Redundant Output

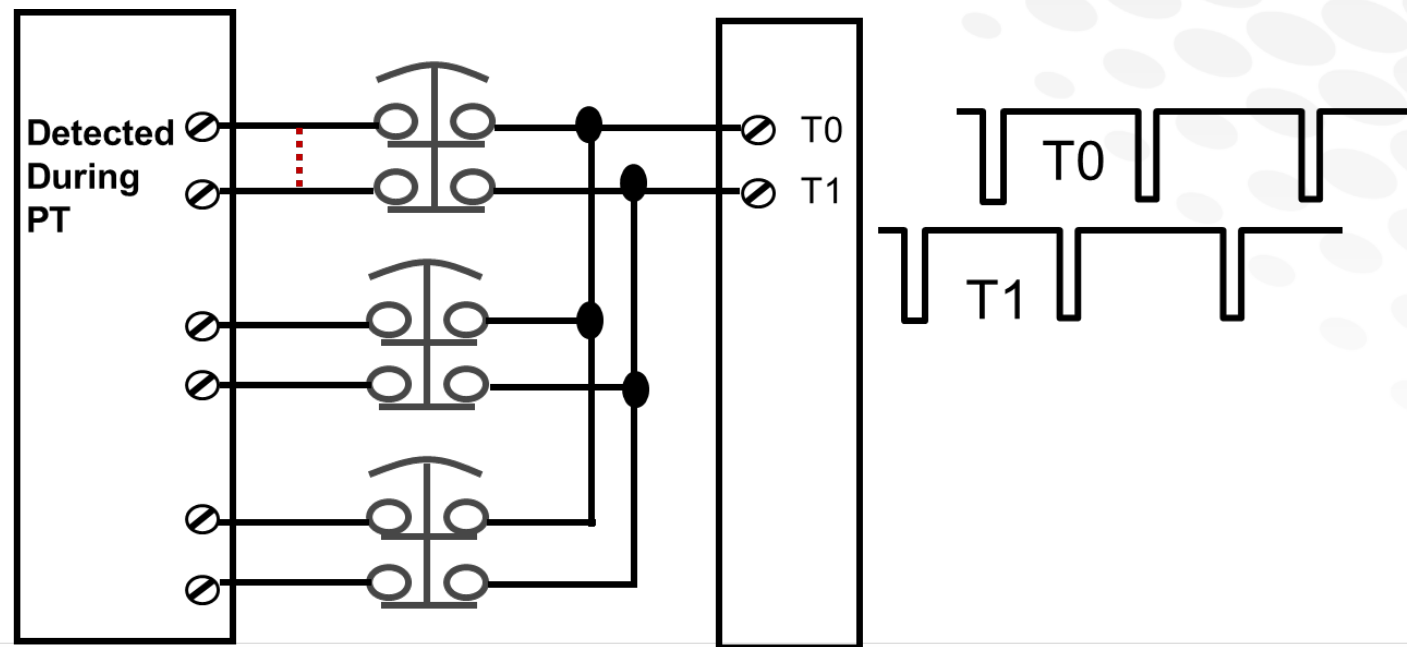
Dangerous Undetected (DU) Fault

- The highlighted fault is undetectable with this wiring; sourced from power rail
- The **channel-to-channel short is not detected**, and thus a second fault could lead to a loss of the safety function.



Pulse Testing

- The channel-channel short can be detected using a pulse test.
- Safety Controllers and Safety I/O have configurable pulse test capability.
- Test Outputs are used to source the 24V for the channel, and are intermittently pulse tested to detect shorts to 24V.



How to Configure Safety Input Channels

Channel Configuration / Single or Equivalent?

Channel	Channel Operation			
	Type	Discrepancy Time (ms)	Deadband	Channel Offset
0	Single	0	1	0
1				
2	Equivalent	1000	100	2000
3				

Point	Point Operation		Point Mode	Test Source	Input Delay Time (ms)	
	Type	Discrepancy Time (ms)			Off->On	On->Off
0	Single	0	Safety	None	0	0
1			Safety	None	0	0
2	Single	0	Safety Pulse Test	0	0	0
3			Safety Pulse Test	1	0	0
4	Equivalent	100	Safety	None	0	0
5			Safety	None	0	0
6	Single	0	Safety	None	0	0
7			Safety	None	0	0

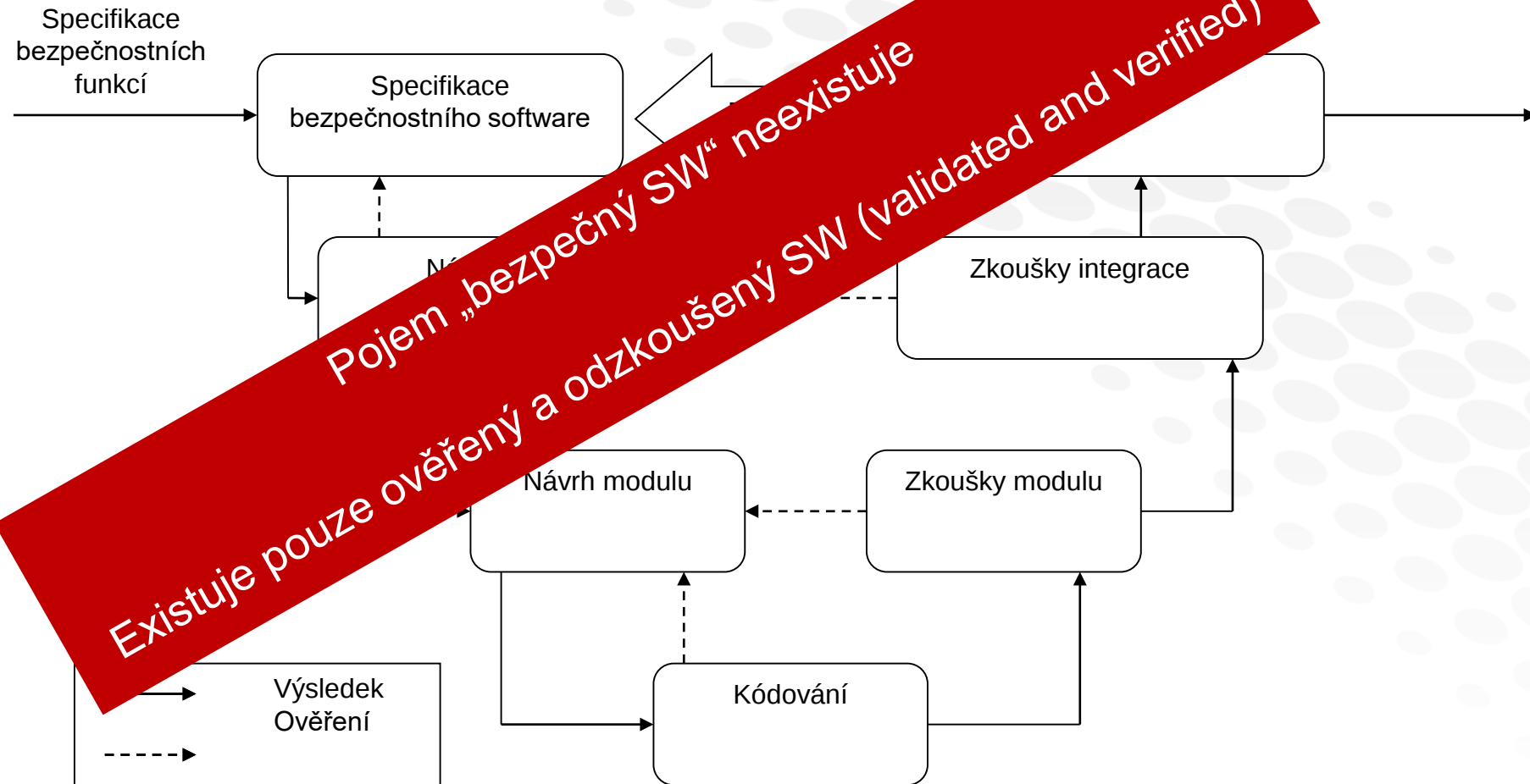
Single
Equivalent
Complementary

Input Error Latch Time: 1000 ms

Bezpečnostní SW

Požadavky na SW nalezneme v EN ISO 13849-1, kapitole 4.6, nebo v EN 61508-3

Postup u V-modelu bezpečnostního SW během životního cyklu

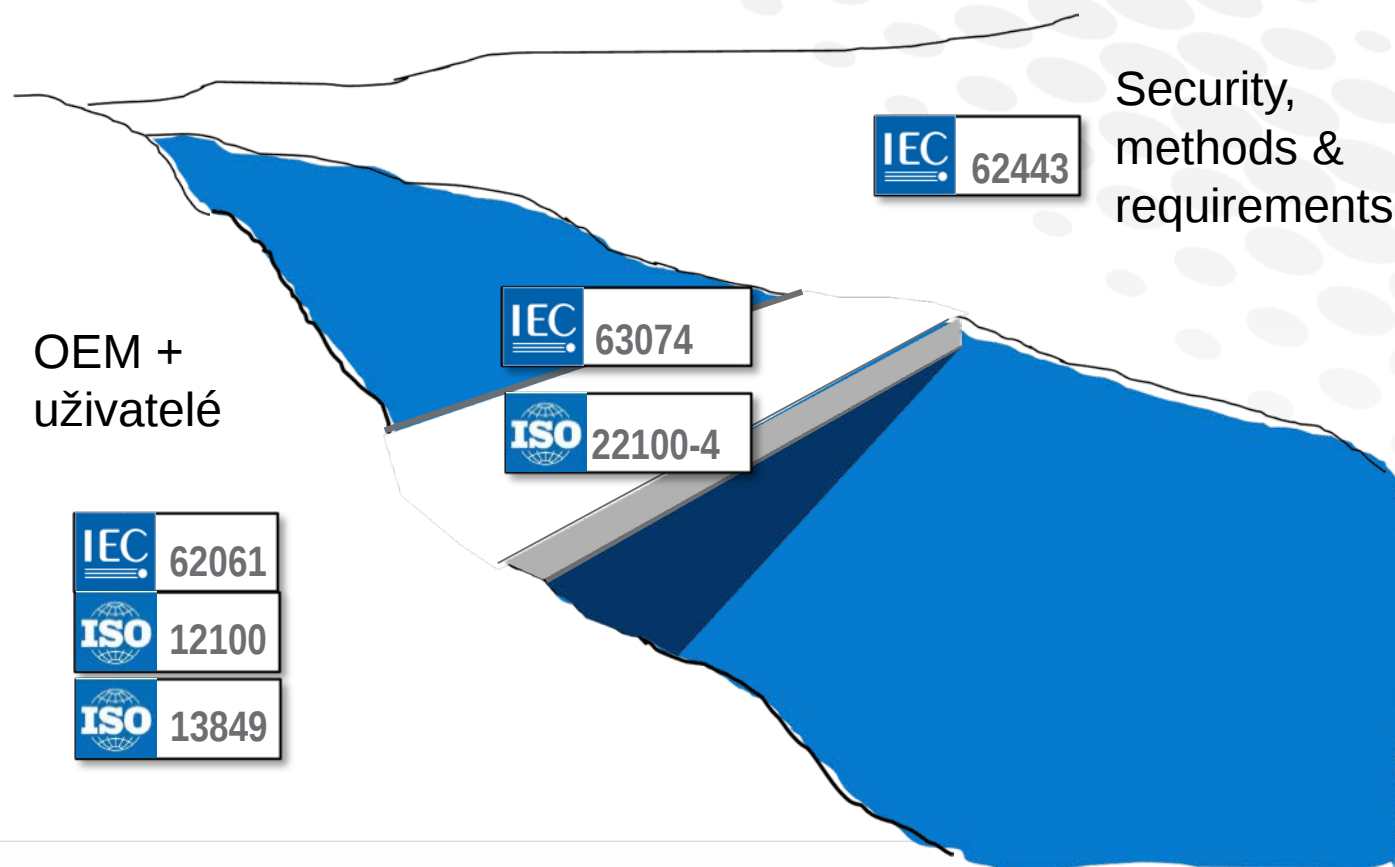


Je možná certifikace 3. stranou

- Pokud si přejete (nebo váš odběratel) mít aplikační kód validovaný třetí stranou, buďte PŘIPRAVENI na to, že DALEKO více času stráví validátor nad vaším procesem než nad samotným SW... Je třeba:
 - Řádně (až téměř dokonale) zdokumentovat životní cyklus
 - Například: máte správně vypracovanou SRS i pro software?
 - Programovat modulárně a strukturovaně
 - Program musí být „čitelný“, pochopitelný a musí jej být možné testovat

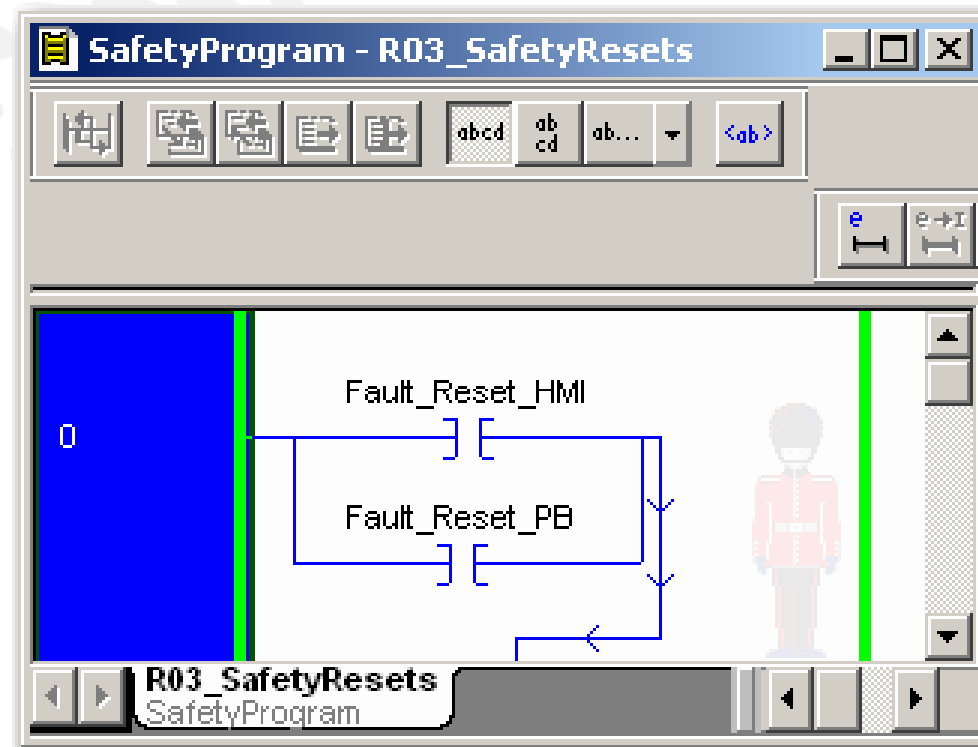
Security (zabezpečení) je součástí safety (bezpečnosti)

IEC TR 63074 – Security - Functional safety of control systems



Ochrana proti změnám

- Bezpečnostní systémy potřebují ochranu proti
 - Offline změnám bezpečnostního programu
 - Online změnám bezpečnostního programu
 - Změnám parametrům z HMI
 - Přehrání programu a přepsání bezpečnosti
 - etc...
- Zákeřné, záměrné, nedovolené?
- Neúmyslné, zapomenuté?



Agenda

1

PŘEHLED HW
SYSTÉMY S INTEGROVANOU BEZPEČNOSTÍ

2

RYCHLÉ PŘEDSTAVENÍ STUDIO 5000

3

NEJČASTĚJŠÍ SW BLOKY

4

JAK VÁM MŮŽEME POMOCI

Jak vám můžeme pomoci dosáhnout BEZPEČNÉ aplikace

- **OBSÁHLOST PORTFOLIA PRODUKTŮ**

Rockwell Automation je světová jednička ve vývoji, výrobě a prodeji produktů pro funkční bezpečnost



- **KOMPETENCE OSOB**

Každý technik Rockwell Automation má alespoň základní znalosti o funkční bezpečnosti, v každé zemi je specialista. Rockwell dlouhodobě udržuje a prohlubuje znalosti osob, které se starají o zákazníky v oblasti bezpečnostní techniky



- **SPOLUPRÁCE S TÜV RHEINLAND**

Rockwell spolupracuje nejen na certifikaci produktů, ale i v oblasti komplexního neustálého vzdělávání v oblasti funkční bezpečnosti nejen strojů, ale i procesů a zabezpečení.



Jak vám můžeme pomoci dosáhnout BEZPEČNÉ aplikace

- SOFTWARE

Rockwell má k dispozici volně šiřitelný software (SAB), který může spolupracovat se SW Sistema a podporuje zákazníky, kteří se snaží své projekty zvládnout sami. Rovněž má k dispozici SW nástroj RASWin.



- SLUŽBY

Rockwell nabízí služby na klíč malého i velkého rozsahu od analýzy a posouzení rizik po dodávku kompletního projektu s podklady pro vydání ES prohlášení o shodě





**Rockwell
Automation**

Innovation & Technology Forum

Děkuji



Kontaktujte mě přes LinkedIn! – **Karel Stibor**