

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

# Bezpečnost v moderním průmyslu

Mgr. Karel Stibor

Tato prezentace je spolufinancována Evropským sociálním fondem a státním rozpočtem České republiky.



Mgr. Karel Stibor

# ÚVOD

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# O autorovi

Mgr. Karel Stibor

- 2002 až 2007 Systemotronic, s.r.o., distributor produktů firmy PILZ, GmbH. v ČR a SR
- 2007 dodnes Rockwell Automation, s.r.o., mimo dalšího sortimentu největší světový výrobce bezpečnostní techniky
- 2004 dodnes člen TKEZPS jako subkomise TC44

Dotazy mohou zaznít kdykoliv během semináře, nebo později telefonicky: 602 671 178, či e-mailu [kstibor@ra.rockwell.com](mailto:kstibor@ra.rockwell.com)



# Obsah semináře - dopoledne

- > přehled legislativy potřebné pro úspěšné zhotovení projektu
- > Specifika legislativy pro nové stroje a zařízení
- > Specifika legislativy pro používané stroje
- > Normy spojené s bezpečnostní technikou

EN ISO 13849-1 „Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Všeobecné zásady pro konstrukci“ a 13849-2 „Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 2: Ověřování.“

EN 61508 „Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností“

EN 62061 „Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností.“

EN 14121 „Bezpečnost strojních zařízení - Posouzení rizika - Část 1: Zásady.“

EN 12100-1 „Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci - Část 1: Základní terminologie, metodologie.“ a 12100-2 „Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci - Část 2: Technické zásady.“

EN 60204-1 „Bezpečnost strojních zařízení - Elektrická zařízení strojů - Část 1: Všeobecné požadavky“

- > Bezpečnostní funkce a způsoby omezování rizika
- > SW nástroj Sistema

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Obsah semináře - odpoledne

Praktickou částí je myšleno typické řešení obvodů, jejich schématické nákresy a upozornění na chyby, které v praxi běžně vznikají.

- > Snímání přítomnosti osob
- > Bezpečnostní kryty
- > Logické prvky
- > LOTO systémy – bezpečné vypnutí strojů a technologických linek a jejich částí
- > Hlavní vypínače
- > Nouzové zastavení
- > Bezpečnostní stykače a relé, princip nuceného vedení
- > Klidový stav hřídelí
- > Dvouruční ovládání
- > Hlídaní izolačního stavu (elektrická bezpečnost ve vztahu ke strojní bezpečnosti)
- > Bezpečnost aplikací v prostorech s nebezpečím výbuchu



Mgr. Karel Stibor

# PŘEHLED LEGISLATIVY

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Bezpečnost v moderním průmyslu

## Přehled legislativy

- Splnění legislativy

- Legalizace provozovaných strojů a zařízení
- Zvýšení bezpečnosti uživatelů strojů
- Vyloučení pokutování či stíhání institucí

**Důvod 1**  
 „**lidský přístup**“  
 Představme si sebe jako obsluhu

**Důvod 2**  
 „**ekonomický**“  
 Pokuty, produktivita...

- Omezení pracovních úrazů

- Snížení nákladů na obsluhu
- Vyloučení hrozby platby odškodného poškozeným
- Zajištění potřebné výroby stroje
- Vyšší pracovní morálka
- Vyloučení možnosti stíhání kvůli hodnotě úrazovosti

**Důvod 3**  
 „**legislativní**“  
 Bezproblémový prodej/provoz

...bych měl přemýšlet o bezpečnosti?





# Bezpečnost v moderním průmyslu

## Přehled legislativy

Základem je mít stroj ve shodě s evropskými normami, je ve svém důsledku jedno, zda je stroj nový, nebo používaný

### Nový stroj

NV 176/2008Sb. upřesňuje, co je strojní zařízení – jedná se o soubor prvků, který je poháněn (mimo lidskou či zvířecí sílu) sestavený z navzájem spojených více částí, kdy alespoň jedna je pohyblivá.  
Detailní přehled výjimek nalezneme v §1

Dále je důležitá příloha 7, kde nalezneme informaci o nutné dokumentaci dodávané se zařízením (vč. jazykových mutací).

zákonu 97Sb. Jsou  
ena nařízení  
(hlavní pro  
jsou 17/2003,  
616/2006 a  
176/2008Sb.

Tyto nařízení se odvolávají na normy jako EN 60204, EN ISO 13849-1 ap.

Normy jsou nezávazné, ale jejich nesplnění může vést ve svém důsledku k porušení zákona...

### Používaný stroj

Základním dokumentem definujeme NV 378/2001Sb

Mimo požadovat mít každý

### ZAMĚSTNATEL

kteří právní zodpovědnost nemůže delegovat žádným způsobem na další pracovníky (pouze „starost o technické prostředky“)

Tento postup, včetně značky CE musí být uplatněn vždy, pokud provádím více než OPRAVU (rekonstrukci, renovaci, modernizaci atd.). OPRAVA je výměna nefunkčních prvků za shodné, nebo za ty se stejnou funkcí !!! Toto je oficiální vyjádření ČOI (Česká obchodní inspekce).

náradí.

(management, jednatel ap.)



mista a jejich ošetření v souladu s bezpečnostními normami

Pokud nebudou normy splněny, není možné označení stroje značkou CE





# Nařízení vlády a Evropská legislativa

		Obsah
NV. 176/2008 Sb.	2006/42/ES	NV 176/2008Sb. upřesňuje, co je strojní zařízení – jedná se o soubor prvků, který je poháněn (mimo lidskou či zvířecí sílu) sestavený z navzájem spojených více částí, kdy alespoň jedna je pohyblivá. Detailní přehled vyjímek nalezneme v §1 Dále je důležitá příloha 7, kde nalezneme informaci o nutné dokumentaci dodávané se zařízením (vč. jazykových mutací).
NV. 17/2003 Sb.	93/68/EHS	Dokument upravuje technické požadavky na zařízení nízkého napětí. Na základě tohoto dokumentu se aplikuje norma EN 60204-1
NV. 616/2006 Sb.	2004/108/ES	Dokument upravuje technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility.
Z. 22/1997 Sb.	x	Zákon o nových výrobcích
NV. 378/2001 Sb.	89/655/EHS	Bezpečný provoz, používání minimální požadavky na bezpečnost strojů, přístrojů a náradí
NV. 262/2006 Sb.	x	Zákonník práce

Ke stažení v CZ na [www.mvcr.cz](http://www.mvcr.cz), dokumenty Evropské Unie na <http://eur-lex.europa.eu>

15.10.2010



# Kde hrozí RIZIKA?



## Porozumění potenciálním rizikům ovlivňuje celkový vzhled a funkčnost stroje

Nezapomeňte, že rizika nezpůsobuje pouze pohyb,  
ale např. horké povrchy, nebezpečí pádu a další,  
se kterými si poradíte pouze vy sami...



15.10.2010



# 6 kroků pro dosažení bezpečného stroje

- 0) Obhídka stroje, diskuze nad konstruovaným strojem
- 1) Analýza rizikovosti (výsledkem jsou nebezpečná místa a PLr/SIL)
- 2) Projekt řešící analýzu rizikovosti (u nových strojů součástí dokumentace)
- 3) Aplikace projektu
- 4) Validace (přezkoušení funkčnosti, měření doběhových časů apod.)
- 5) Doplnění dokumentace o položky řešící bezpečnost
- 6) Vydání prohlášení o shodě/doplnění o bezpečnostní normy.

Pokud jste projektant, máte ze zákona povinnost **upozornit na nedostatky** (nejen v oblasti bezpečnosti) nadřízené, objednatele apod. Pro váš klid v duši doporučuji upozornit vždy **písemně**.



# První krok při zvyšování bezpečnosti

- Prvním krokem pro zvýšení bezpečnosti vašich aplikací je

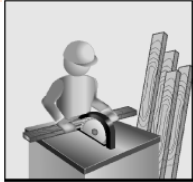
## **ANALÝZA RIZIKOVOSTI**

(též analýza rizik)

- Provádí se dle norem EN ISO 14121-1 a EN ISO 12100-1 a -2
- Výsledkem této analýzy je **návrh opatření snižujících riziko** a to v tomto pořadí:
  - Snížení rizik opatřeními zabudovanými v konstrukci stroje (např. oplocení, volba materiálu stroje, konstrukce...)
  - Snížení rizik bezpečnostní ochranou
  - Snížení rizik informacemi pro používání strojního zařízení (obsluha, seřizování a servis, montáž a demontáž)

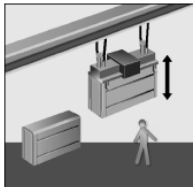


# Rizika dle EN 14121



## Řezné části

- pořezání
- oddělení



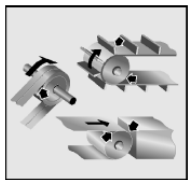
## Padající předměty

- stlačení
- naražení



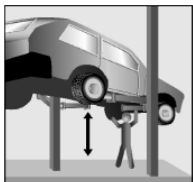
## Pohybující se prvky

- stlačení
- naražení
- stříh



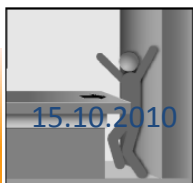
## Pohybující se prvky

- vtažení
- tření, odření
- naražení



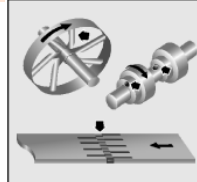
## Tíže, stabilita

- stlačení
- zachycení



## Přiblížení pohybujícího se prvku k pevné části

- stlačení
- naražení



## Rotující nebo pohybující se prvky

- oddělení
- navinutí



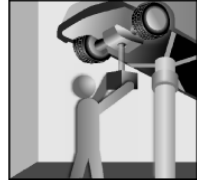
## Pohybující se prvky

- stlačení
- tření, odření
- naražení
- oddělení



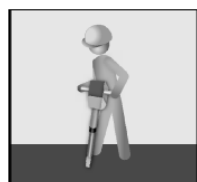
## Živé elektrické části

- zasažení proudem
- popálení
- propíchnutí
- opaření



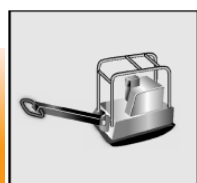
## Předměty nebo materiály s vysokou nebo nízkou teplotou

- popálení



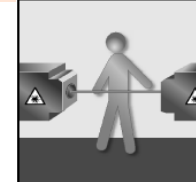
## Vibrační zařízení

- poškození kloubů
- cévní poškození



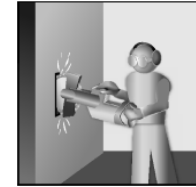
## Hluk výrobního procesu

- únava
- zhoršení sluchu
- ztráta vědomí
- stres



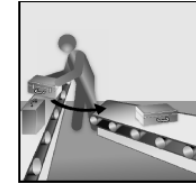
## Laserový paprsek

- popálení
- poškození zraku a kůže



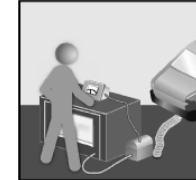
## Prach

- obtížné dýchání
- výbuch
- ztráta zraku



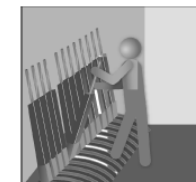
## Poloha těla

- nepohodlí
- námaha
- svalově kosterní poškození



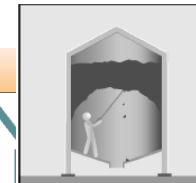
## Kouře

- obtížné dýchání
- dráždění
- otrava



## Umístění ovládacích zařízení

- vždy jako následek lidské chyby
- stres



## Tíže (ztuhnutí sypkého materiálu)

- zřícení, pád, stlačení, udušení
- propadnutí, sesedání
- zaklínění, zacpání

15.10.2010



# Snížení rizik opatřeními zabudovanými v konstrukci stroje

- Vychází z konstrukce stroje, vždy je na projekčním týmu, aby určil rizika a navrhl jejich minimalizaci. Jako tým doporučujeme zapojit maximální možné množství osob, nejméně pak:
  - Projektant elektro
  - Projektant mechanických konstrukcí
  - TechnologKdy minimálně jeden člen má zkušenosti s bezpečnostní technikou (nejen BOZP)



# Snížení rizik bezpečnostní ochranou

- Rizika se omezují vhodnými opatřeními a certifikovaným řešením:
  - Nouzové zastavení (na každé stroji a z...
  - Dvouruční ovládání
  - Snímání přítomnosti (tepelné optoelektronické prvky atd.)
  - ...
  - Pohyb (s vysokou závorou)
  - Hlídaní k (W)
  - ... nezaměňovat s

**Jednotlivé prvky musí splňovat požadavky bezpečnostních norem.**

**Stejně tak je důležité jejich správné zapojení!**



# Snížení rizik informacemi pro používání strojního zařízení

- Do této kategorie patří:
  - Piktogramy a bezpečnostní sdělení umístěné na stroji
  - Upozornění a postupy z návodu k použití (vč. seřizování, údržby apod.), zejména z povinné kapitoly s názvem „seznam zbytkových rizik“
  - Seznam zbytkových rizik
- Nezapomeňte prosím že každý provozovatel je povinnen vypracovat „místní provozně bezpečnostní předpis“ a seznámit s ním zaměstnance, kteří s ním přijdou do kontaktu !





# Legislativní požadavky na bezpečnost strojů

- Architektura bezpečnostních obvodů musí odpovídat normám:

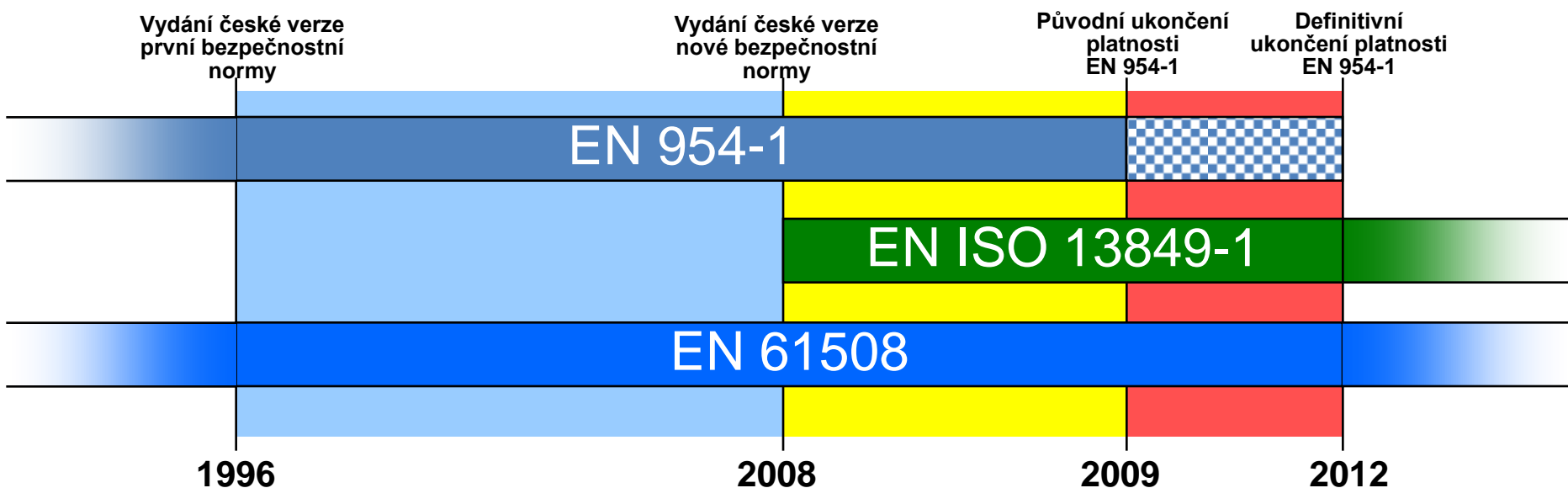
EN 954-1: - bezpečnostní kategorie - odpovídající zapojení		EN ISO 13849-1 - Úroveň PL - Kategorie zapojení		EN 61508 - úroveň SIL - odpovídající zapojení
B	POZOR, mezi sloupečky není shoda !!	a	POZOR, mezi sloupečky není shoda !!	Žádný zvláštní požadavek
1		b		
2		c		1
3		d		2
4		e		3

- Každý stroj musí být adekvátně zhodnocen minimálně dle jedné z uvedených norem;

15.10.2010



# Platnost naorem z oblasti bezpečnosti



15.10.2010



Mgr. Karel Stibor

# SPECIFIKA LEGISLATIVY PRO NOVÉ STROJE

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





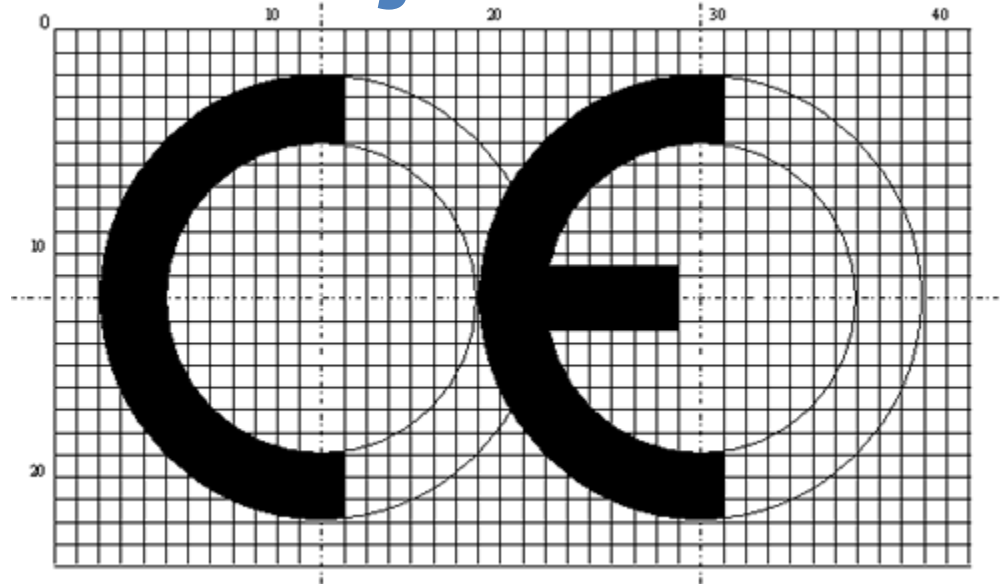
# Kdy použít který přístup?

Rozhodování jaký legislativní přístup  
použít je jednoduchý.  
Účinnost kupní smlouvy mezi  
výrobce a uživatelem...

Nezapomeňte prosím, že legislativa na stroj po  
generální opravě, modernizaci, rekonstrukci atd.  
pohlíží jako na stroj NOVÝ!



## Legální značka „ES Prohlášení o shodě“ na stroji či zařízení





# ES prohlášení o shodě

- **ES Prohlášení o shodě**
- řeší nařízení vlády č.176/2008 Sb., v §8
- **ES prohlášení o shodě je postup, při němž výrobce nebo jeho zplnomocněný zástupce prohlašuje, že strojní zařízení, které bude uvedeno na trh, splňuje všechny základní požadavky na ochranu zdraví a bezpečnost, které se na ně vztahují.**
- **Podpis na ES prohlášení o shodě opravňuje výrobce nebo jeho zplnomocněného zástupce, aby opatřil strojní zařízení označením CE.**
- **Před vydáním ES prohlášení o shodě musí výrobce nebo jeho zplnomocněný zástupce zajistit a být schopen zaručit, že požadovaná technická dokumentace je a zůstane u něho dostupná pro případné kontrolní účely. Dokumentace musí být u výrobce uložena nejméně 10 let od výroby posledního typového kusu!**



# Postup

Abych mohl na stroj umístit značku CE a vydat ES prohlášení o shodě, musí výrobek splňovat ZÁKLADNÍ požadavky dané normami.

Mohu zvolit samozřejmě vlastní cestu, ale potom musím dokázat že moje opatření je minimálně stejně dobré, spolehlivé atd. jako normativní požadavky.

Splnění bezpečnostních požadavků nových výrobků vychází tedy již ze zákona zákon č.22/1997Sb., o technických požadavcích na výrobky. Zákon sám o sobě nepokrývá bezpečnost, tu nalezneme v příslušných nařízeních vlády, a to:

NV č.17/2003 Sb „ technické požadavky na elektrická zařízení nn“

NV č. 616/2004 Sb. „elektromagnetická kompatibilita výrobků“

NV č. 176/2008 Sb. „technické požadavky na strojní zařízení“

Garantem dodržování této legislativy je MPO – ÚNMZ - ČOI)



# Nařízení vlády č.17/2003 Sb.

## Nařízení vlády č.17/2003 Sb.,

kterým se stanoví  
technické požadavky na elektrická zařízení nízkého  
napětí.

## Směrnice Evropského parlamentu a Rady 2006/95/ES,

ze dne 12. prosince 2006  
o harmonizaci právních předpisů členských států týkajících  
se  
elektrických zařízení používaných v určitých mezích napětí  
s platností 20. dnem po vyhlášení  
v Úředním věstníku Evropské unie (ÚVEU).





# Nařízení vlády č.616/2006 Sb.

## Nařízení vlády č. 616/2006 Sb.,

o technických požadavcích na výrobky  
z hlediska jejich elektromagnetické kompatibility  
( použití od 20.7.2007)

## Směrnice Evropského parlamentu a Rady 2004/108/ES

ze dne 15. prosince 2004

o sblížení právních předpisů členských států **týkajících**  
**se elektromagnetické kompatibility**

a o zrušení směrnice 89/336/EHS

(legislativa do 20.ledna 2007, použití od 20.7.2007)



# Nařízení vlády č.176/2008 Sb.

- Nařízení vlády 176/2008 Sb.,  
kterým se stanoví  
technické požadavky na strojní zařízení.

## Směrnice Evropského parlamentu a Rady 2006/42/ES

ze dne 17.května 2006  
o strojních zařízeních  
a o změně směrnice 95/16/ES



# Bezpečnost a dokumentace stroje - povinná pro výrobce i provozovatele

**Dokumentace, která musí být předána při prodeji a která musí být k dispozici po celou dobu provozu stroje či zařízení**

- **Průvodní dokumentace** (dle normy EN 12100-2, čl. 6.5 musí dodat výrobce, obsahuje např. návod k použití, zapojovací schémata, analýzu rizikovosti, prohlášení o shodě a podobně)
- **Provozní dokumentace** (vypracovává provozovatel – obsahuje např. revize u tlakových nádob, dokumentaci k seřizování, zprávu o výchozí revizi, provozní deník a podobně)
- **Místní provozně-bezpečnostní předpis** (vypracovává provozovatel na základě provozní dokumentace a informací z návodu k použití- zejména v ohledu na zbytkové riziko, na které výrobce upozornil.

Vysvětlení vychází z Evropské směrnice č.95/16/ES



- **Návod pro obsluhu (elektrické zařízení)**
  - Technická dokumentace musí zahrnovat návod pro obsluhu popisující podrobně správné postupy pro seřizování a používání elektrických zařízení. Zvláštní pozornost je třeba věnovat použitým bezpečnostním opatřením.
  - Pokud může být provoz zařízení programován, musí být uvedeny podrobné informace o metodách programování, požadovaném zařízení, ověřování programu a přídatných bezpečnostních postupech (kde jsou požadovány).
- **Návod pro údržbu (elektrické zařízení)**
  - Technická dokumentace musí zahrnovat návod pro údržbu popisující podrobně správné postupy pro nastavování, obsluhu a preventivní prohlídku, a opravy. Součástí této příručky mají být doporučení pro intervaly a záznamy o údržbě/servisu. Pokud jsou použity metody pro ověřování správného provozu (např. programy pro testování programového vybavení), musí být používání těchto metod podrobně popsáno.



Mgr. Karel Stibor

# SPECIFIKA LEGISLATIVY PRO POUŽÍVANÉ STROJE

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Kdy použít který přístup?

Rozhodování jaký legislativní přístup  
použít je jednoduchý.  
Účinnost kupní smlouvy mezi  
výrobce a uživatelem...

Nezapomeňte prosím, že legislativa na stroj po  
generální opravě, modernizaci, rekonstrukci atd.  
pohlíží jako na stroj NOVÝ!



# CÍL aplikace bezpečnosti

Splnit podmínku nařízení vlády  
378/2001 Sb. „kterým se stanoví bližší požadavky na bezpečný provoz  
a používání strojů, technických zařízení,  
přístrojů a nářadí“  
o maximální době mezi kontrolou bezpečnosti stroje...

**12 měsíců !!!**

Pozor, zde se lišíme od zbytku EU. V rámci EU má provozovatel povinnost revidovat bezpečnost při výjimečných událostech (změna okolí stroje, stěhování atd.), u nás jsou předpisy přísnější. Zahraniční „kolegové“ proto často nechápou že je třeba dělat pravidelné revize...



# Posuzování bezpečnosti provozovaných strojů

## Provozované výrobky - Bezpečnost strojů, technických zařízení, přístrojů a nářadí

V roce 2001 bylo vydáno nařízení vlády (NV) čís. 378/2001 Sb., s účinností od **1.ledna 2003**, kterým se stanoví bližší požadavky na bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí, s uvedením **minimálních požadavků na bezpečný provoz a používání** zařízení v závislosti na příslušné riziko vytvářené daným zařízením.

Toto nařízení se vztahuje, v souladu s právem Evropských společenství (Směrnice Rady 89/655/EHS), na bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí, pokud požadavky na bezpečnost provozu a používání zařízení nestanoví zvláštní právní předpis.





- **Kontrola bezpečnosti provozu zařízení  
před uvedením do provozu**

je prováděna podle průvodní dokumentace od výrobce.

Není-li výrobce znám nebo není-li průvodní dokumentace k dispozici, stanoví rozsah kontroly zařízení zaměstnavatel (uživatel) místním provozním bezpečnostním předpisem.



# Posuzování bezpečnosti provozovaných strojů

- Zařízení musí být vybaveno provozní dokumentací. Následná kontrola musí být prováděna

**nejméně jednou za 12 měsíců**

v rozsahu stanoveném místním provozním bezpečnostním předpisem nestanoví-li zvláštní právní předpis, popřípadě průvodní dokumentace nebo normové hodnoty rozsah a četnost kontrol jinak.

Provozní dokumentace musí být uchovávána po celou dobu provozu zařízení.



# Posuzování bezpečnosti provozovaných strojů

## Zákon 262/2006 Sb.,

ze dne 21.dubna 2006

zákoník práce

### Část pátá

### Hlava 1

## Bezpečnost a ochrana zdraví při práci



# Posuzování bezpečnosti provozovaných strojů

## Předcházení ohrožení života a zdraví při práci

§101

Zaměstnavatel je **povinen** zajistit bezpečnost a ochranu zdraví zaměstnanců při práci s ohledem **na rizika** možného ohrožení jejich života a zdraví, která se týkají výkonu práce (dále jen „rizika“).

Péče o bezpečnost a ochranu zdraví při práci, která zůstává uložena zaměstnavateli podle odstavce 1 nebo zvláštním právním předpisem,

je nedílnou a rovnocennou součástí

**pracovních povinností vedoucích** zaměstnanců na všech stupních řízení v rozsahu pracovních míst, která zastávají.



# Posuzování bezpečnosti provozovaných strojů

## Zákon 309/2006 Sb.

ze dne 23.května 2006,

kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci).

### • §4

#### • **Požadavky na výrobní a pracovní prostředky a zařízení**

- Zaměstnavatel je povinen zajistit, aby stroje, technická zařízení, dopravní prostředky, a nářadí byly z hlediska bezpečnosti a ochrany zdraví při práci vhodné pro práci, při které budou používány. Stroje, technická zařízení, dopravní prostředky a nářadí musí být
  - Vybaveny ochrannými zařízeními, která chrání život a zdraví zaměstnanců,
  - Vybaveny nebo upraveny tak, aby odpovídaly ergonomickým požadavkům a aby zaměstnanci nebyli vystaveni nepříznivým faktorům pracovních podmínek
  - Pravidelně řádně udržovány, kontrolovány, a revidovány.
- Bližší požadavky na bezpečný provoz a používání strojů, technických zařízení, dopravních prostředků a nářadí stanoví prováděcí právní předpis.



Mgr. Karel Stibor

# NORMY SPOJENÉ S BEZPEČNOSTNÍ TECHNIKOU

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Přehled

**EN ISO 13849-1** „Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Všeobecné zásady pro konstrukci“

**EN ISO 13849-2** „Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 2: Ověřování.“

**EN 61508** „Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností“

**EN 62061** „Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností.“

**EN 14121** „Bezpečnost strojních zařízení - Posouzení rizika - Část 1: Zásady.“

**EN 12100-1** „Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci - Část 1: Základní terminologie, metodologie.“ a **12100-2** „Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci - Část 2: Technické zásady.“

**EN 60204-1** „Bezpečnost strojních zařízení - Elektrická zařízení strojů - Část 1: Všeobecné požadavky“



# POZOR

Nechci se v žádném případě stavět do pozice „vykladače norem“. I když jsem stál u překladu některých z nich, právo na tuto činnost mají pouze soudy a soudní znalci !

Informace v této části berte prosím jako doporučení vzniklá v dlouhodobé praxi. Pro komplexní informaci prostudujte celou příslušnou normu.

Nechtějte po nikom kopie norem.  
Jejich kopírováním porušujete zákon!





# Struktura norem

**V úvodu je nutné upozornit, že každá norma je z hlediska uváděných požadavků, zařazena pod určitý typ:**

**Norma typu A** – základní bezpečnostní norma, uvádějící základní pojmy, zásady pro konstrukci a všeobecná hlediska, která mohou být aplikována na všechna strojní zařízení.

**Norma typu B** – skupinová bezpečnostní norma, zabývající se jedním bezpečnostním hlediskem nebo jedním typem bezpečnostního zařízení, které může být použito pro větší počet strojních zařízení.

**norma typu B1-** se týká jednotlivých bezpečnostních hledisek (např. bezpečných vzdáleností, teploty povrchu, hluku) atd.

**norma typu B2-** se týká příslušných bezpečnostních zařízení (např. dvouručních ovládacích zařízení, blokovacích zařízení, zařízení citlivých na tlak, ochranných krytů),



# Struktura norem

**Norma typu C** – bezpečnostní normy pro stroje, určující detailní bezpečnostní požadavky pro jednotlivý stroj nebo skupinu strojů.

Pokud se norma typu C odchyluje od jednoho nebo více opatření, kterými se zabývá část této normy, má přednost dodržení normy typu C.

(Norma typu C je norma výrobová)

Závaznost jednotlivých norem je dána jejich vyhlášením ve Věstníku jako norem harmonizovaných (popřípadě norem určených) i když splnění základních požadavků stanovených evropskými směrnicemi nebo nařízením vlády, je možné prokázat i jiným způsobem než těmito normami. Tato možnost však nebývá výrobcům vzhledem ke složitosti legislativního řešení využívána.

**Harmonizovaná norma** – je norma, která je v souladu s uvedeným dokumentem.



# EN ISO 13849-1

Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů –

Část 1: Všeobecné zásady pro konstrukci

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Základní norma bezpečnostní techniky

## EN ISO 13849-1

- **Předmět normy EN ISO 13849-1**

Tato část ISO 13849 uvádí 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, které zahrnují úroveň vlastností požadovanou k vykonávání bezpečnostních funkcí. Norma platí pro bezpečnostní části ovládacích systémů (SRP/CS) bez ohledu na druh používané technologie a energie (elektrické, hydraulické, pneumatické, mechanické, atd.) pro všechny druhy strojních zařízení.

Norma nspecifikuje bezpečnostní funkce nebo úrovně vlastností, které mají být použity v jednotlivém případě.

- **SRP/CS - bezpečnostní část ovládacího systému**

*(safety-related part of a control system)*

**část ovládacího systému, která reaguje na bezpečnostní vstupní signály a vytváří bezpečnostní výstupní signály**



# Základní norma bezpečnostní techniky

## EN ISO 13849-1

- **analýza rizika** (*risk analysis*)  
kombinace specifikace mezních hodnot stroje, identifikace nebezpečí a odhadu rizika
- **úroveň vlastností; PL** (*performance level (PL)*)  
diskrétní úroveň používaná k určení schopností bezpečnostních částí ovládacích systémů k vykonávání bezpečnostní funkce při předvídatelných podmínkách
- **požadovaná úroveň vlastností; PLr** (*required performance level (PLr)*)  
úroveň vlastností (PL) používaná k tomu, aby bylo dosaženo pro každou bezpečnostní funkci požadovaného snížení rizika
- **střední doba do nebezpečné poruchy; MTTFd** (*mean time to dangerous failure (MTTFd)*)  
očekávaná střední doba do nebezpečné poruchy



# Základní norma bezpečnostní techniky

## EN ISO 13849-1

- **Bezpečnostní část ovládacího systému *SRP/CS***  
***(safety-related part of a control systém)***
- část ovládacího systému, která reaguje na bezpečnostní vstupní signály a vytváří bezpečnostní výstupní signály  
Kombinované bezpečnostní části ovládacího systému začínají v bodu, ve kterém jsou bezpečnostní vstupní signály iniciovány (zahrnující například ovládací vačku nebo kladičku spínače polohy) a končí na výstupu prvků silového ovládání (zahrnující například hlavní kontakty stykače).  
Jsou-li pro diagnostiku použity monitorovací systémy, jsou tyto systémy považovány za bezpečnostní části ovládacího systému (SRP/CS).



# Základní norma bezpečnostní techniky

## EN ISO 13849-1

- **Diagnostické pokrytí; DC**

*(diagnostic coverage (DC))*

- míra účinnosti diagnostiky, která může být určena jako podíl intenzity poruch detekovaných nebezpečných poruch a intenzity poruch všech nebezpečných poruch
- Diagnostické pokrytí může existovat pro celý bezpečnostní systém nebo pro části bezpečnostního systému.
  - Například diagnostické pokrytí může existovat pro senzory a/nebo logický systém a/nebo koncové prvky.
  - **Definice je převzata z IEC 61508-4:1998, 3.8.6.**



# Základní norma bezpečnostní techniky

## EN ISO 13849-1

- **Ochranné opatření** (*protective measure*)  
opatření určené k dosažení snížení rizika
- **Realizované konstruktérem:** opatření zabudovaná v konstrukci, bezpečnostní ochrana a doplňková ochranná opatření, informace pro používání.
- **Realizované uživatelem:** organizace (bezpečné pracovní postupy, kontrola, dovolené pracovní systémy), zajištění a používání dalších bezpečnostních zařízení; používání osobních ochranných prostředků, zaškolení.
- Definice je převzata z ISO 12100-1:2003, 3.12.





# Základní norma bezpečnostní techniky

## EN ISO 13849-1

- **Doba používání; TM** (*mission time (TM)*)  
doba předpokládaného používání bezpečnostních částí ovládacího systému (SRP/CS)
  
- **Ovládací systém stroje** (*machine control system*)  
systém, který reaguje na vstupní signály od částí prvků stroje, obsluhy, vnějšího ovládacího zařízení nebo od jakýchkoliv jejich kombinací a který vytváří výstupní signály tak, že se stroj chová předpokládaným způsobem  
**Ovládací systém stroje** může použít jakoukoliv technologii nebo jakoukoliv kombinaci různých technologií (např. elektrickou/elektronickou, hydraulickou, pneumatickou, mechanickou).



# EN ISO 13849-1

## EN 62061

- Úroveň integrity bezpečnosti; SIL  
*(safety integrity level (SIL))*

diskrétní úroveň (jedna ze čtyř možných) pro stanovení požadavků integrity bezpečnosti bezpečnostních funkcí, přiřazených k E/E/PE bezpečnostním systémům, kde úroveň integrity bezpečnosti 4 má nejvyšší úroveň integrity bezpečnosti a úroveň 1 má nejnižší úroveň integrity bezpečnosti

[IEC 61508-4:1998, 3.5.6]



# EN ISO 13849-1

## EN 62061

- **Informace o doporučeném používání**

### **EN 62061 a této části EN ISO 13849**

EN 62061 a tato část EN ISO 13849 specifikují požadavky pro konstrukci a realizaci bezpečnostních částí ovládacích systémů strojních zařízení.

Používání těchto mezinárodních norem, podle jejich předmětu, může být předpokladem pro splnění relevantních základních bezpečnostních požadavků.

Následující tabulka sumarizuje **předměty normy** EN 62061 a této části EN ISO 13849.



# EN ISO 13849-1

## EN 62061

	Technologie realizující bezpečnostní ovládací funkci	ISO 13849-1	IEC 62061
A	Neelektrická, např. hydraulika	X	Nezahrnuje
B	Elektromechanická, např. relé a/nebo neúplná elektronika	Omezená na stanovenou architekturu a) a až do PL = e	Všechny architektury a až do SIL 3
C	Úplná elektronika, např. programovatelná	Omezená na stanovenou architekturu a) a až do PL = d	Všechny architektury a až do SIL 3
D	A kombinovaná s B	Omezená na stanovenou architekturu a) a až do PL = e	X <sup>c)</sup>
E	C kombinovaná s B	Omezená na stanovenou architekturu (viz poznámku 1) a až do PL = d	Všechny architektury a až do SIL 3
F	C kombinovaná s A, nebo C kombinovaná s A a B	X <sup>b)</sup>	X <sup>c)</sup>

X udává, že tímto předmětem se zabývá mezinárodní norma, která je uvedena v záhlaví sloupce.

a) Stanovené architektury jsou definovány v 6.2, aby byl zjednodušen způsob pro kvantifikaci úrovně vlastností.

b) Pro úplnou elektroniku: používání stanovených architektur podle této části ISO 13849 až do PL = d nebo jakékoliv architektury podle IEC 62061.

c) Pro neelektrické technologie, používání částí podle této části ISO 13849 jako subsystémů.

15.10.2010



# Základní norma bezpečnostní techniky

## EN ISO 13849-1

Aby pomohl konstruktérovi a usnadnil posouzení dosažené **úrovně vlastností bezpečnostní funkce (PL)**, používá tento dokument metodologii, která je založena na kategorizaci struktur podle specifických konstrukčních kritérií a specifikovaného chování v podmínkách závady. Těmto kategoriím je přidělena jedna z pěti úrovní, označených jako **kategorie B, 1, 2, 3 a 4**.

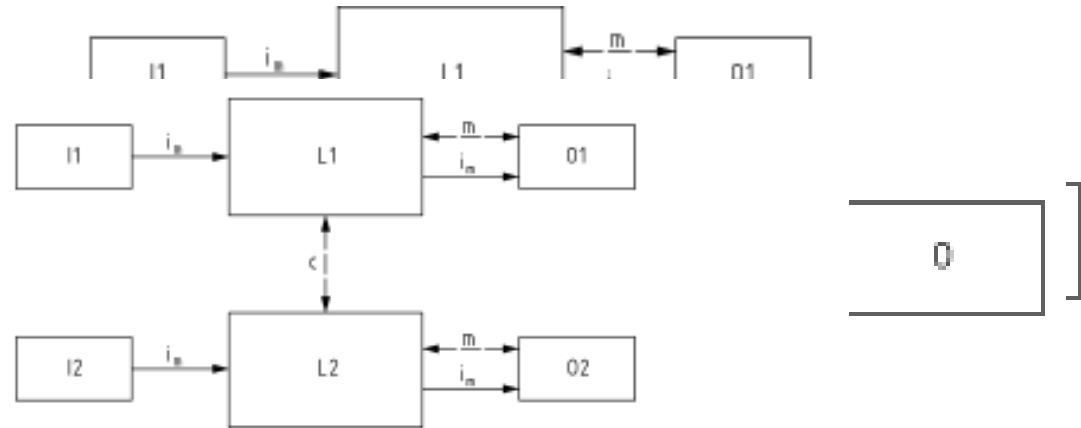
**Úrovně vlastností a kategorie** se mohou vztahovat na bezpečnostní části ovládacích systémů, jako jsou:

- ochranná zařízení (např. dvouruční ovládání, blokovací zařízení), elektrická snímací ochranná zařízení (např. fotoelektrické clony), zařízení citlivá na tlak;
  - ovládací jednotky (např. logická jednotka pro ovládací funkce, zpracování dat, monitorování, atd.) a
  - prvky silového ovládání (např. relé, ventily, atd.),
- a stejně tak na ovládací systémy, které vykonávají bezpečnostní funkce u všech druhů strojních zařízení – od jednoduchých zařízení (např. malých kuchyňských strojů nebo automatických dveří a vrat) až po výrobní zařízení (např. balicí stroje, tiskové stroje, lisy).



# Základní norma bezpečnostní techniky EN ISO 13849-1

ČSN EN ISO 13849-1



## Legenda

$i_m$  prostředky (Plné čáry pro monitorování znázorňují diagnostické pokrytí, které je vyšší než ve stanovené architektuře pro kategorii 3.)

I	vstupní zařízení	$i_m$	prostředky vzájemného propojení
L	logika	c	křížové monitorování
O	výstupní zařízení	I1, I2	vstupní zařízení, např. senzor
		L1, L2	logika
		m	monitorování
		O1, O2	výstupní zařízení, např. hlavní stykač

Obrázek 12 – Stanovená architektura pro kategorii 4

kategorii 1

Obrázky z EN ISO 13849-1



# Základní norma bezpečnostní techniky

## EN ISO 13849-1

**Vlastnosti každé bezpečnostní funkce a požadovaná úroveň vlastností** musí být stanoveny a dokumentovány ve specifikaci bezpečnostních požadavků.

V této části **EN ISO 13849** jsou **úrovně vlastností** bezpečnostní funkce definovány ve formě **pravděpodobnosti nebezpečné poruchy za hodinu**. Je stanoveno pět úrovní vlastností (a až e) s definovanými rozsahy pravděpodobnosti nebezpečné poruchy za hodinu.

- **Úrovně vlastností – PL (bezpečnostní funkce)**

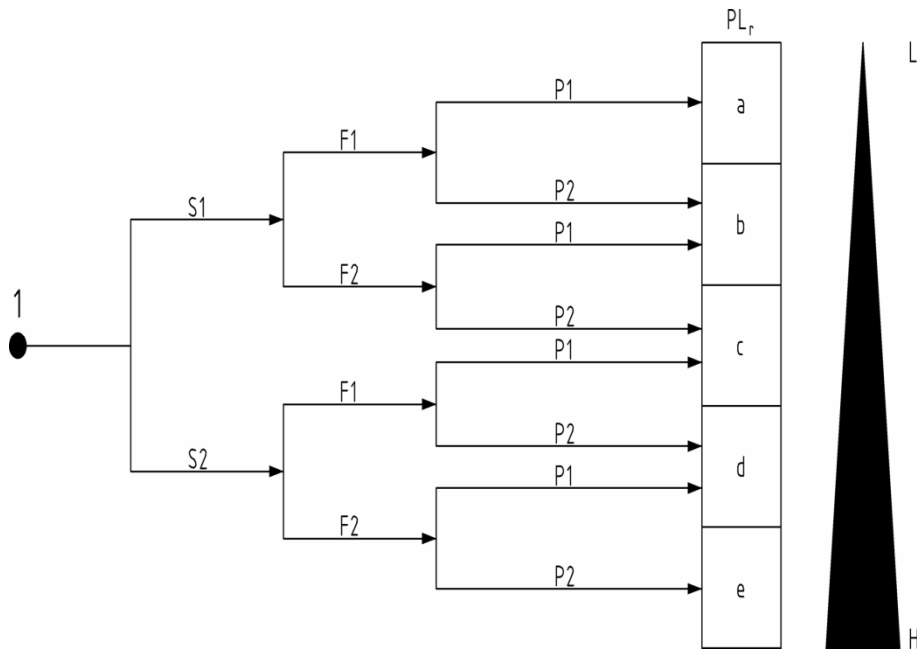
**Průměrná pravděpodobnost nebezpečné poruchy za hodinu (1/h)**

<b>a</b>	$\geq 10^{-5}$ až $< 10^{-4}$	(odpovídá době do cca 2let)
<b>b</b>	$\geq 3 \times 10^{-6}$ až $< 10^{-5}$	(odpovídá době od cca 2 do 30let)
<b>c</b>	$\geq 10^{-6}$ až $< 3 \times 10^{-6}$	(odpovídá době od cca 30 do 100let)
<b>d</b>	$\geq 10^{-7}$ až $< 10^{-6}$	(odpovídá době od cca 100 do 1000let)
<b>e</b>	$\geq 10^{-8}$ až $< 10^{-7}$	(odpovídá době cca nad 1000let)



# Základní norma bezpečnostní techniky

## EN ISO 13849-1



### • Určení požadované úrovně vlastností (PLr)

Posouzení rizika předpokládá situaci před opatřením předpokládané bezpečnostní funkce. Snížení rizika jinými technickými opatřeními, nezávislémi na ovládacím systému (např. mechanické ochranné kryty) nebo dalšími bezpečnostními funkcemi, může být při určení požadované úrovně vlastností (PLr) předpokládané bezpečnostní funkce také bráno v úvahu; těchto opatření zvolen počáteční bod

### Závažnost zranění (označené S) –

relativně snadno odhadnutelná (např. tržná rána, amputace, smrtelná nehoda).

**Četnost výskytu (označené F) –** pro zlepšení odhadu jsou používány pomocné parametry:

- četnost a doba vystavení nebezpečí (F)
- možnost vyloučení nebezpečí nebo omezení škody (P).

Zkušenosti ukazují, že parametry mohou být kombinovány, aby bylo docíleno odstupňování rizika od nízkého k vysokému.

**Je významné, že jde o kvalitativní proces, který udává pouze odhad rizika.**





# Základní norma bezpečnostní techniky EN ISO 13849-1

- Návod pro volbu parametrů S, F a P pro odhad rizika

- Závažnost zranění S1 a S2

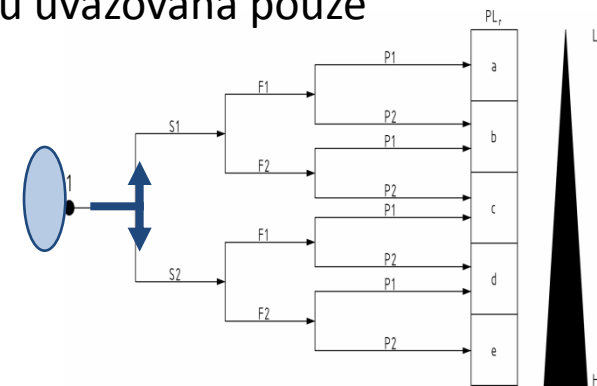
Při určení závažnosti zranění S1 a S2 by měly být vzaty v úvahu obvyklé následky úrazů a běžné léčebné postupy. Například pohmoždění a/nebo tržné rány bez komplikací mají být klasifikovány jako **S1**,

zatímco amputace nebo smrt by měly být klasifikovány jako **S2**.

V odhadu rizika, při vzniklé poruše bezpečnostní funkce, jsou uvažována pouze

**lehká zranění** (obvykle s přechodnými následky),

**závažná zranění** (obvykle s trvalými následky) a smrt.





# Základní norma bezpečnostní techniky

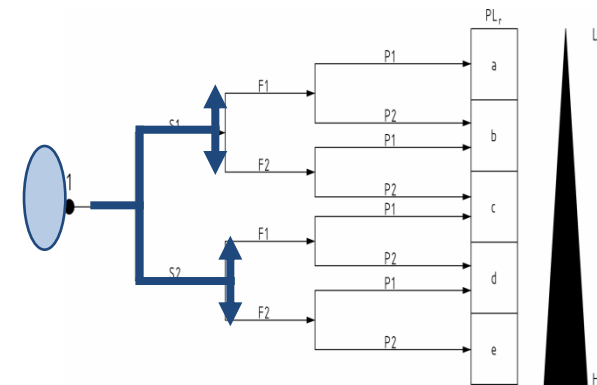
## EN ISO 13849-1

### • Četnost a/nebo doba vystavení nebezpečí F1 a F2

• Obecně platná perioda času, která má být zvolena pro parametr F1 nebo F2 nemůže být specifikována. Nicméně následující výklad může usnadnit, v případě pochybností, správné rozhodnutí.

Parametr F2 má být zvolen tehdy, je-li osoba vystavena nebezpečí často nebo nepřetržitě. Je nepodstatné, zda je vystavena nebezpečí táž osoba nebo postupně různé osoby, např. při používání výtahů. Parametr četnosti má být zvolen podle četnosti a doby trvání přístupu k nebezpečí.

Je-li četnost vystavení vyšší než jednou za hodinu, má být v tomto případě, bez jakéhokoliv zdůvodnění, zvolen parametr F2.





# Základní norma bezpečnostní techniky

## EN ISO 13849-1

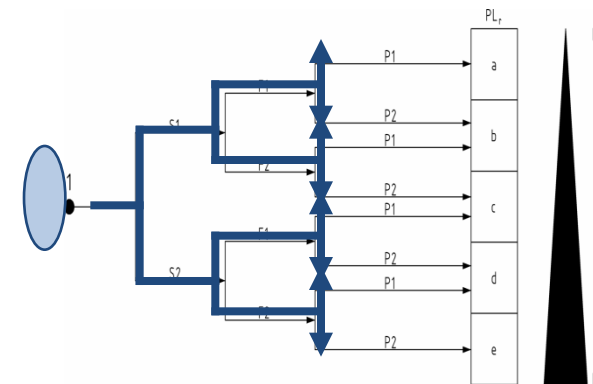
### Možnost vyloučení nebezpečí P1 a P2

Je důležité vědět, zda může být poznána nebezpečná situace a zda může být vyloučena dříve, než může dojít k úrazu. Například důležitá je úvaha, zda může být nebezpečí přímo identifikováno jeho fyzikálními vlastnostmi nebo zda může být poznáno pouze technickými prostředky, např. sdělovači.

Jiná důležitá hlediska, která ovlivňují volbu parametru P zahrnují, například:

- provoz s dozorem nebo bez dozoru;
- provoz s odborníky nebo laiky;
- rychlost s jakou vzniká nebezpečí (např. rychle nebo pomalu);
- možnosti vyvarování se nebezpečí (např. uniknutím);
- praktické bezpečnostní zkušenosti vztahující se k procesu.

Vyskytne-li se nebezpečná situace a je-li reálná možnost vyloučení úrazu nebo významného snížení jeho účinků, má být zvolen pouze parametr P1; parametr P2 má být zvolen tehdy, není-li téměř žádná možnost vyloučení nebezpečí.





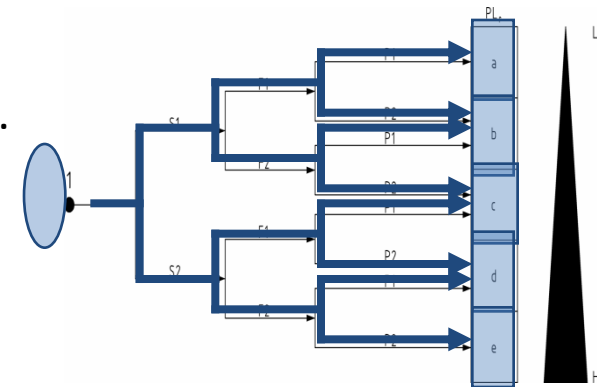
# Základní norma bezpečnostní techniky EN ISO 13849-1

- K dosažení **úrovně vlastností (PL)** jsou, vedle **průměrné pravděpodobnosti nebezpečné poruchy za hodinu**, nezbytná také jiná opatření.

Podle posouzení rizika (viz ISO 14121) stroje, musí konstruktér rozhodnout o příspěvku ke **snížení rizika**, který je nutno vykonávat každou relevantní bezpečnostní funkcí, která je uskutečňována **bezpečnostními částmi ovládacího systému (SRP/CS)**.

Tento příspěvek však nepokrývá celkové riziko ovládaného strojního zařízení, např. není zahrnuto celkové riziko mechanického lisu nebo pracího stroje, ale část rizika sníženého aplikací určitých bezpečnostních funkcí.

Příklady těchto funkcí jsou funkce zastavení, která je iniciována pomocí elektrického snímacího ochranného zařízení u lisu nebo funkce dveří s blokováním pracího stroje.





# Základní norma bezpečnostní techniky

## EN ISO 13849-1

- Po určení PLr následuje výpočet PL pro všechny SRP/CS (všechny bezpečnostní funkce stroje se všemi prvky).
- Po výpočtu se porovná PL s PLr, pokud se hodnoty alespoň rovnají, následuje validace dle EN ISO 13849-2
- Pozor, málokdo si uvědomuje, že pro výpočty je nutné mít:
  - kompletní schéma elektroinstalace (alespoň bezpečnostních obvodů)
  - analýzu rizikovosti
  - logické schéma bezpečnostní logiky
  - pokud se jedná o programovatelnou logiku, tak výpis bezpečnostního ovládacího programu.

Po výpočtu nelze NIC v řetězci měnit (pouze údržba „kus za kus“ a to od jednoho výrobce s jedněmi parametry!



# EN ISO 13849-2

Bezpečnost strojních zařízení - Bezpečnostní části ovladacích systémů –

Část 2: Ověřování.

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# EN ISO 13849-2

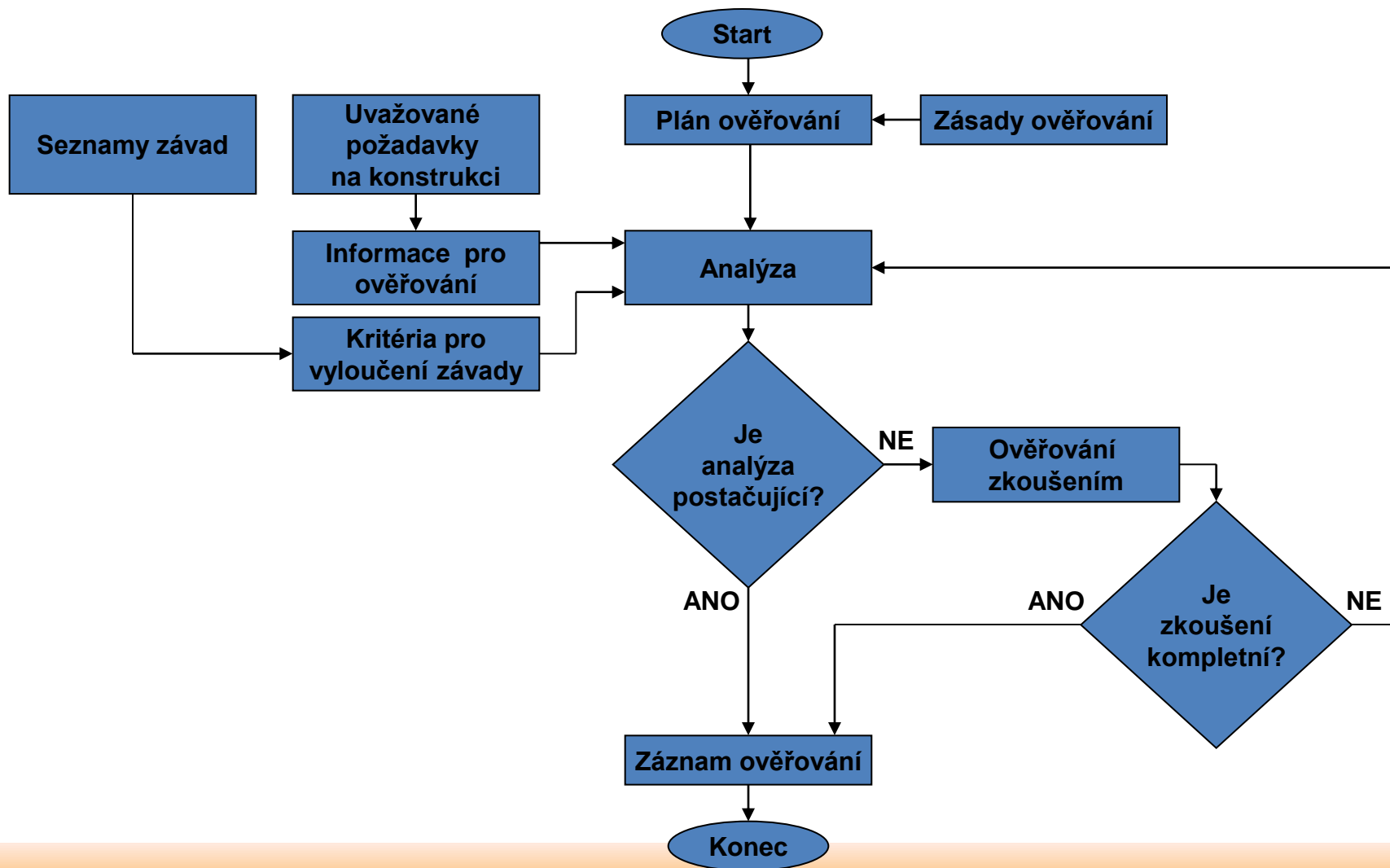
## Zásady ověřování

- Účelem ověřování je potvrdit specifikaci a shodu konstrukce bezpečnostních částí ovládacího systému v rámci celkové specifikace bezpečnostních požadavků. strojního zařízení.
- Ověřování musí prokázat, že každá bezpečnostní část splňuje požadavky EN ISO 13849-1, zvláště:
  - specifikované bezpečnostní vlastnosti bezpečnostních funkcí poskytovaných touto částí, jak bylo stanoveno racionální konstrukcí
  - požadavky specifikované kategorie
- Ověřování má být provedeno osobami nezúčastněných na konstrukci bezpečnostní části.
- Stupeň nezávislosti má odrážet bezpečnostní vlastnosti bezpečnostní části.
- Ověřování se skládá z používání analýzy a je-li to nezbytné, z provedení zkoušek podle plánu ověřování. Vyváženost mezi analýzou a/nebo zkoušením závisí na technologii.
- Analýza má být zahájena co možná nejdříve a to současně s procesem konstrukce tak, aby problémy mohly být včas korigovány a to ve stádiu, kdy je náprava relativně snadná. Pro některé části může být nezbytné oddálení analýzy, dokud není konstrukce správně vyvinuta.



# EN ISO 13849-2

## Proces ověřování



15.10.2010





# EN ISO 13849-2

## Požadavky pro kategorie

Požadavek podkladu	Kategorie pro kterou je podklad požadován				
	B	1	2	3	4
Základní bezpečnostní zásady	X	X	X	X	X
Očekávané provozní namáhání	X	X	X	X	X
Vlivy zpracovávaného materiálu	X	X	X	X	X
Vlastnosti během jiných relevantních vnějších vlivů	X	X	X	X	X
Osvědčené součásti	-	X	-	-	-
Osvědčené bezpečnostní zásady	-	X	X	X	X
Postup kontroly bezpečnostní funkce (funkcí)	-	-	X	-	-
Intervaly kontroly, pokud jsou stanoveny	-	-	X	-	-
Předvídatelné uvažované jednotlivé závady v konstrukci a používaná metoda detekce	-	-	X	X	X
Identifikované poruchy se společným režimem a jak jim zamezit	-	-	-	X	X
Předvídatelné vyloučené jednotlivé závady	-	-	-	X	X
Závady, které mají být detekovány	-	-	X	X	X
Různá nahromadění závad uvažovaných v konstrukci	-	-	-	-	X
Jak je zachována bezpečnostní funkce v případě každé ze závad	-	-	-	X	X
Jak je zachována bezpečnostní funkce při každé kombinaci (kombinacích) závad	-	-	-	-	X



# EN ISO 13849-2

## Přílohy

- A Nástroje ověřování pro mechanické systémy
- B Nástroje ověřování pro pneumatické systémy
- C Nástroje ověřování pro hydraulické systémy
- D Nástroje ověřování pro elektrické systémy



# EN 61508

Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností

15.10.2010

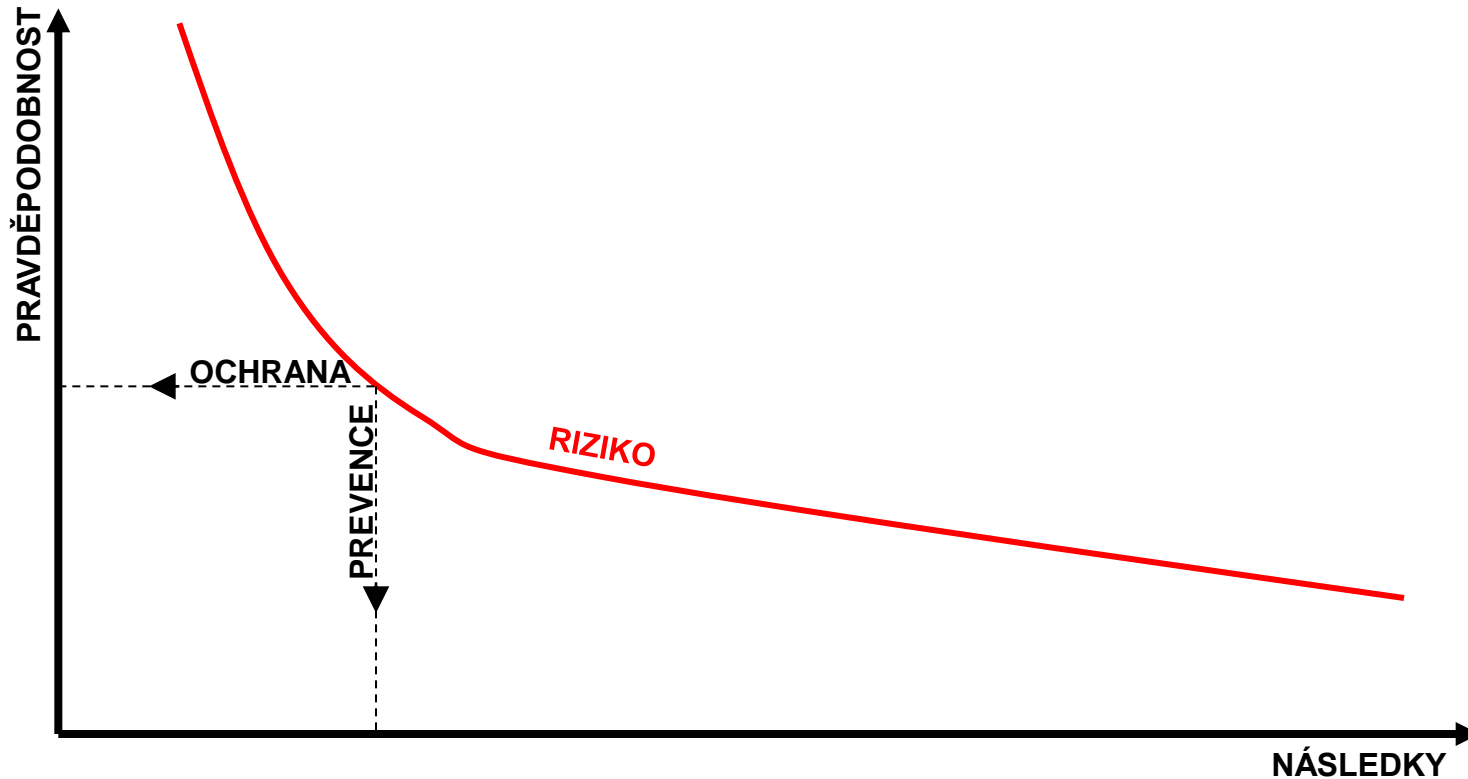
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# EN 61508

Norma EN 61508 pohlíží na omezování rizika pouze z pohledu statistiky.



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





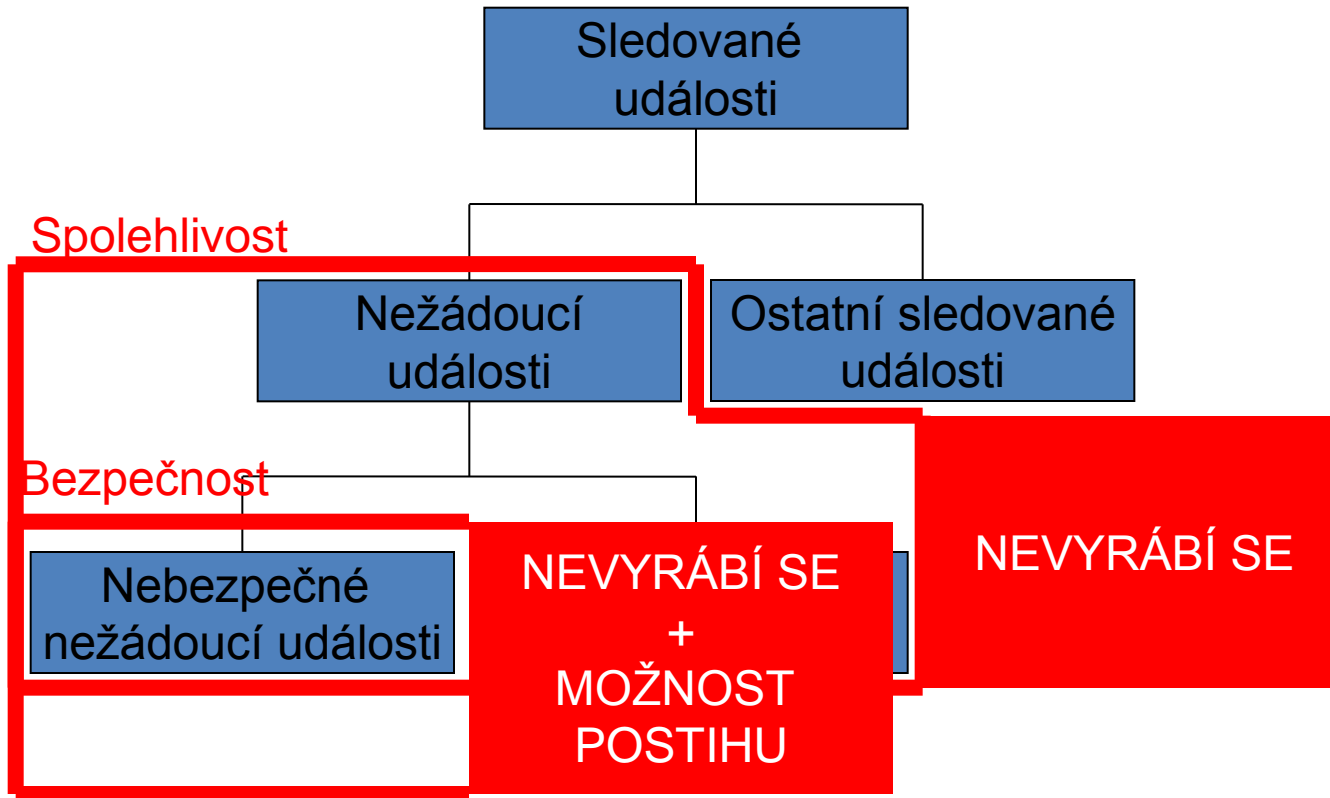
# EN 61508

## Události

Dělení událostí uvažuje o

Spolehlivosti jako o obecném riziku (poruchy, výpadky napájení apod.)

Bezpečnosti jako o riziku vzhledem k zdraví a životu





# EN 61508

## Co řeší norma?

- Funkční bezpečnost během celého cyklu
- Předepisuje spolehlivost jako integritu bezpečnosti a kvalifikuje ji konkrétními ukazateli
- Předepisuje postupy:
  - Analýzu nebezpečí a rizika
  - Specifikaci bezpečnostních funkcí
  - Přiřazení integrity bezpečnosti bezpečnostním funkcím
  - Výběr vhodných prostředků k realizaci bezpečnostních funkcí
  - Verifikované a validované způsoby návrhu, výroby, instalace, provozu a údržby HW i SW složek částí řídicích obvodů se vztahem k bezpečnosti



# EN 61508

## Co řeší norma?

- Návrh řídicího systému musí počítat i s lidskými schopnostmi a omezeními, včetně předpokládání chybného použití
- Návrh systémů včetně diagnostiky a funkcí reagujících na poruchy musí být dokumentován!
- Část dokumentační a realizační nelze aplikovat samostatně.
- Řešení musí vždy odpovídat dokumentaci a požadavkům na realizaci.
- Vždy je třeba vycházet z rizikové analýzy.
- Problematika musí být vždy týmovou prací.



# EN 61508

## SIL

**režim s nízkým (malým) vyžádáním:** kde četnost vyžadání provozu systému souvisejícího s bezpečností není větší než jednou ročně a není větší než dvojnásobek četnosti kontrolních (periodických) zkoušek

**režim s vysokým (velkým) nebo trvalým vyžádáním:** kde četnost vyžadání provozu systému souvisejícího s bezpečností je větší než jednou ročně nebo je větší než dvojnásobek četnosti kontrolních (periodických) zkoušek

SIL	Režim s nízkým vyžádáním [hod <sup>-1</sup> ]	Režim s vysokým vyžádáním [hod <sup>-1</sup> ]
4	$\geq 10^{-5}$ až $< 10^{-4}$	$\geq 10^{-9}$ až $< 10^{-8}$ (pravd. neb. poruchy 1x za 10 let)
3	$\geq 10^{-4}$ až $< 10^{-3}$	$\geq 10^{-8}$ až $< 10^{-7}$ (pravd. neb. poruchy 1x za 100 let)
2	$\geq 10^{-3}$ až $< 10^{-2}$	$\geq 10^{-7}$ až $< 10^{-6}$ (pravd. neb. poruchy 1x za 1000 let)
1	$\geq 10^{-2}$ až $< 10^{-1}$	$\geq 10^{-6}$ až $< 10^{-5}$ (pravd. neb. poruchy 1x za 10.000 let)

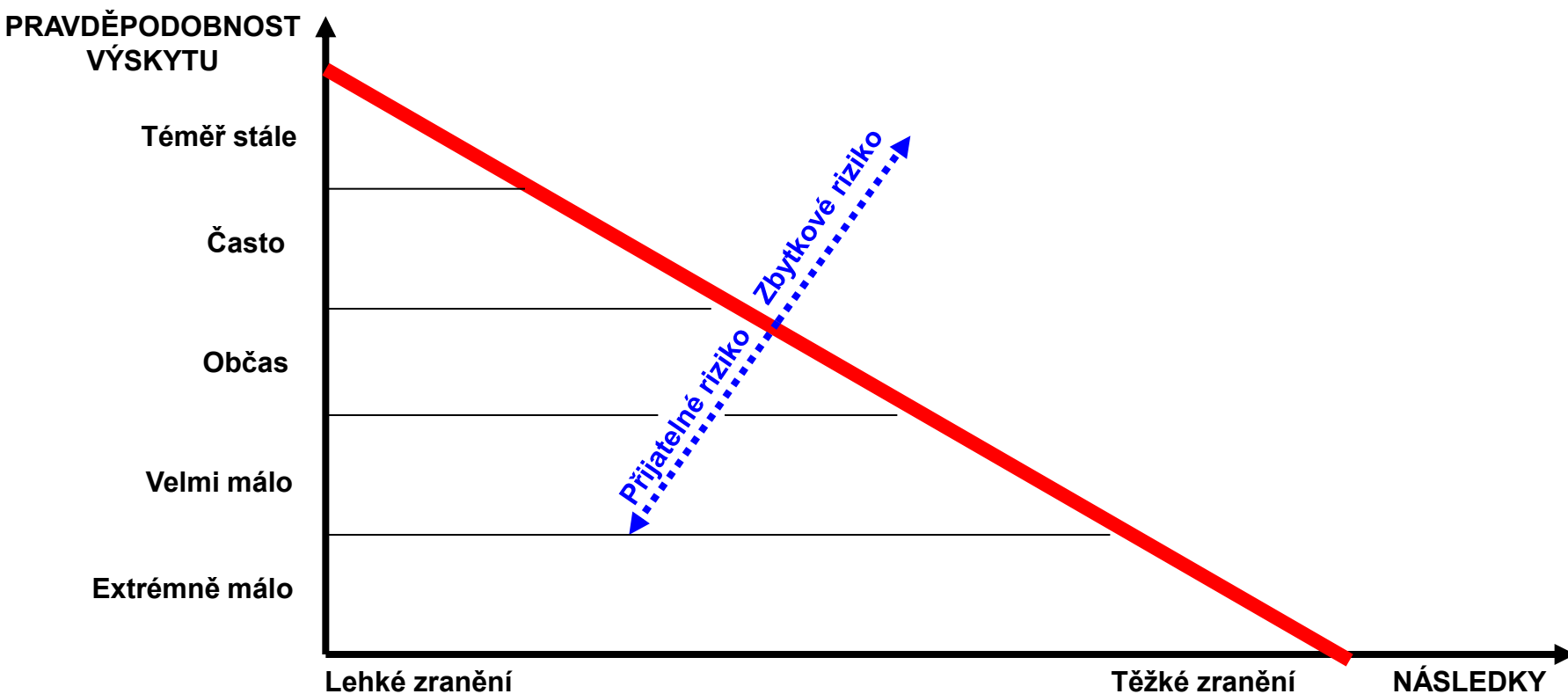




# EN 61508

## SIL

Zbytkové riziko = závažnost zranění \* pravděpodobnost výskytu



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# EN 61508

## SIL

$W_1$ - velmi malá pravděpodobnost nežádoucích výskytů  
 $W_2$ - malá pravděpodobnost nežádoucích výskytů  
 $W_3$ - vysoká pravděpodobnost nežádoucích výskytů

osob s trvalými následky nebo

$C_D$ - smrt veškerého počtu osob

$P_A$ - možné vyhnout se nebezpečí za určitých podmínek  
 $P_B$ - téměř nemožné vyhnout se nebezpečí (veliká rychlost výskytu apod.)

$F_A$ - vzácnější až častější vystavení nebezpečí  
 $F_B$ - častější až trvalé vystavení nebezpečí

**C** = Následek rizikového parametru  
**F** = Četnost a doba působení rizikového parametru  
**P** = Možnost se nebezpečnému rizikového parametru vyhnout  
**W** = Pravděpodobnost nežádoucího výskytu

--- = Žádné bezpečnostní požadavky  
**a** = Žádné speciální bezpeč. požadavky  
**b** = Jediný E/E/PES není dostatečný  
**1, 2, 3, 4** = Úroveň integrity bezpečnosti

Diagram rizika z EN 61508-5, obrázek D1



# EN 61508

## SIL

Odolnost proti vadám N znamená, že N+1 vad by mohlo vyvolat ztrátu bezpečnostní funkce

Podíl bezpečných poruch	Typ architektury	Odolnost proti vadám		
		N=0	N=1	N=2
<60%	Typ A	SIL 1	SIL 2	SIL 3
	Typ B	Nedovolena	SIL 1	SIL 2
60%...<90%	Typ A	SIL 2	SIL 3	SIL 4
	Typ B	SIL 1	SIL 2	SIL 3
90%...<99%	Typ A	SIL 3	SIL 4	SIL 4
	Typ B	SIL 2	SIL 3	
>99%	Typ A	SIL 3	SIL 4	SIL 4
	Typ B	SIL 3		

Typ A – jsou dobře definovány poruchové stavy v všech jednotlivých prvků, lze plně určit chování prvků v případě poruchy, jsou spolehlivé údaje o poruchách z provozu

Typ B – není definován poruchový stav alespoň jednoho prvku, nelze plně určit chování prvku v případě poruchy, nejsou k dispozici spolehlivé údaje o poruchách z provozu



# EN ISO 14121

Bezpečnost strojních zařízení - Posouzení rizika

15.10.2010

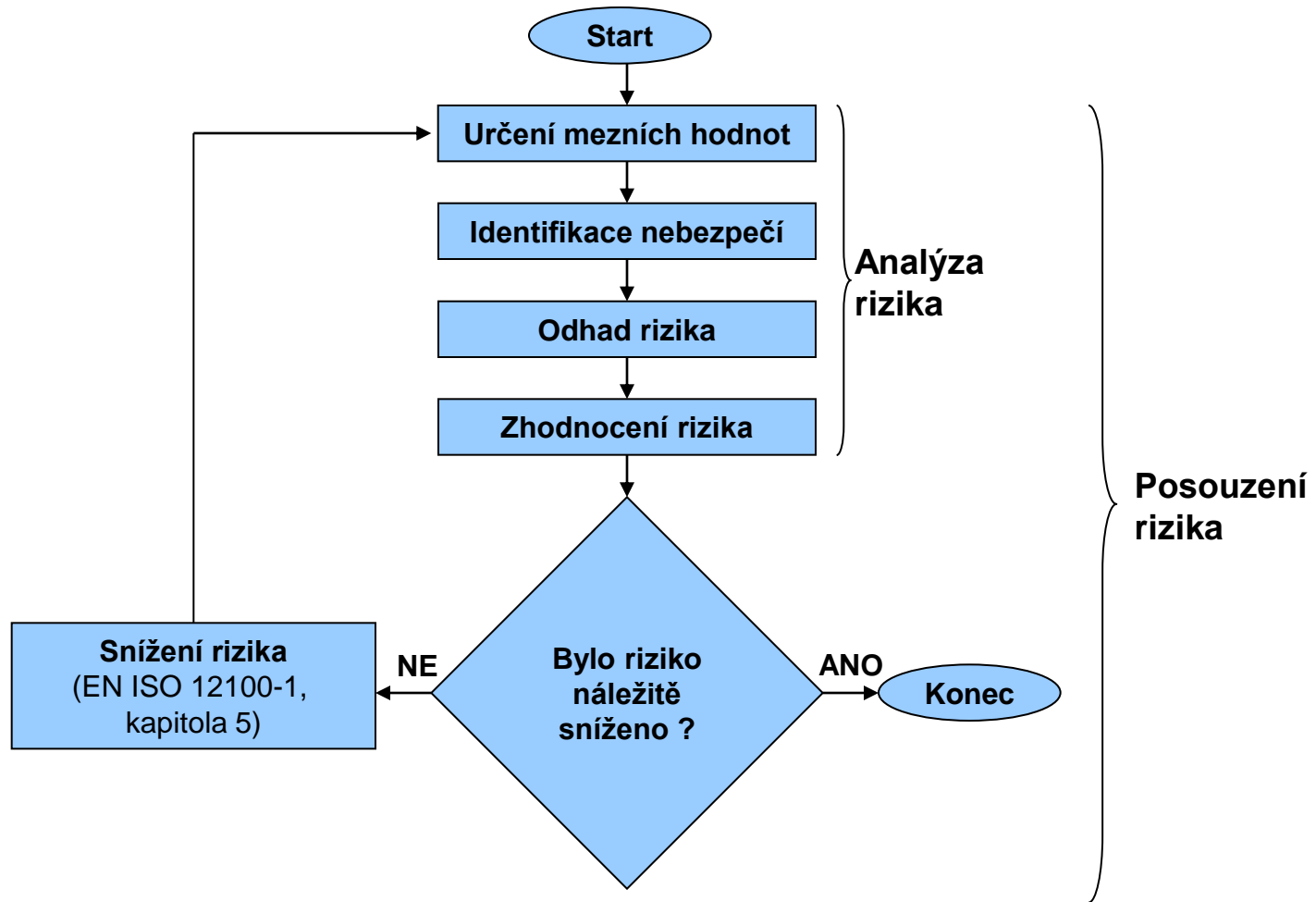
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# EN ISO 14121

## Proces snižení rizika





# EN ISO 14121

## Určení mezních hodnot

Vymezení používání (režimy, určení stroje, zkušenost uživatelů, ostatní osoby)

- Vymezení prostoru

- Rozsah pohybu

- Požadavky na prostor vzájemného působení člověk-stroj

- Rozhraní stroj-dodávka energie

- Vymezení doby

- vymezení životnosti strojního zařízení s přihlédnutím předpokládanému

  - použití a předvídanému nesprávnému použití

- doporučené intervaly údržby

- Ostatní vymezení

- prostředí (teploty, vlhkost, Eex, prašnost atd.)

- udržitelnost + úroveň požadované čistoty

- vlastnosti zpracovávaného materiálu



# EN ISO 14121

## Identifikace nebezpečí

Je třeba rozdělit nebezpečí do všech fází životního cyklu stroje: doprava, montáž a instalace, uvedení do provozu, používání, údržba, servis a seřizování, vyřazení z provozu, demontáž a likvidace

Identifikace úkolů:

seřizování, zkoušení, učení/programování, změna procesu/nástroje  
spuštění, všechny režimy provozu, přívod do stroje, odstraňování výrobku od stroje, zastavování stroje  
nouzové zastavení stroje  
opětné obnovení provozu po zablokování, vyhledávání závad/odstraňování poruch (zásah obsluhy), čištění a udržitelnost, preventivní údržba, údržba za účelem opravy



# EN ISO 14121

## Odhad rizika

Prvky rizika:

všeobecně: závažnost škod, pravděpodobnost výskytu, možnost vyvarovat se nebezpečí

Hlediska, která mají být uvažována při odhadu rizika:

vystavené osoby

druh, četnost a doba trvání vystavení

vztah mezi vystavením a účinky

lidské faktory

vhodnost ochranných opatření

možnost vyřazení nebo obejití ochranných opatření

možnost udržení ochranných opatření

informace pro používání





# EN ISO 14121

## Zhodnocení rizika

### Dosažení odpovídajícího snížení rizika:

Metoda tří kroků:

- Nebezpečí bylo vyloučeno nebo riziko bylo sníženo konstrukcí
- Riziko bylo sníženo použitím bezpečnostní ochrany
- Riziko bylo označeno v návodu k použití jako zbytkové riziko

### Porovnání rizik:

- podobné strojní zařízení je v souladu s relevantními normami;
- předpokládané používání, rozumně předvídatelné nesprávné použití, konstrukce a výroba obou strojů jsou srovnatelné;
- nebezpečí a prvky rizika jsou srovnatelné;
- technické parametry jsou srovnatelné;
- podmínky pro používání jsou srovnatelné.



# EN ISO 14121

## Dokumentace

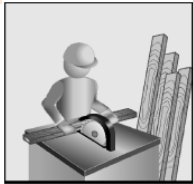
Dokumentace posouzení rizika musí prokázat postup, který byl použit a výsledky, kterých bylo dosaženo. Tato dokumentace obsahuje, pokud je to použitelné, následující:

- a) popis strojního zařízení pro které bylo posouzení rizika provedeno (např. specifikace, stanovení mezních hodnot, předpokládané používání);
- b) všechny relevantní předpoklady, které byly použity (např. zatížení, pevnost, bezpečnostní součinitele);
- c) identifikovaná nebezpečí, nebezpečné situace a nebezpečné události uvažované při posouzení rizika
- d) informace, na kterých bylo založeno posouzení rizika:
  - 1) použité údaje a zdroje (např. historie úrazovosti, zkušenosti získané ze snížení rizika u podobných strojních zařízení);
  - 2) nejistota spojená s použitými údaji a její dopad na posouzení rizika;
- e) cíle snížení rizika, které mají být ochrannými opatřeními dosaženy, pro jejichž volbu mají být uvedeny odkazy na normy nebo jiné použité specifikace;
- f) ochranná opatření realizovaná k vyloučení identifikovaných nebezpečí nebo snížení rizika;
- g) zbytková rizika, která jsou spojena se strojním zařízením;
- h) výsledek posouzení rizika (viz obrázek 1);
- i) všechny formuláře vyplněné při posouzení rizika.



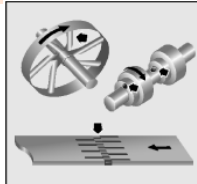
# EN 14121

## Kategorizace rizik (příloha A)



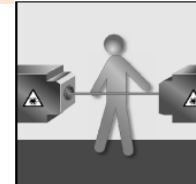
### Řezné části

- pořezání
- oddělení



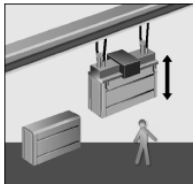
### Rotující nebo pohybující se prvky

- oddělení
- navinutí



### Laserový paprsek

- popálení
- poškození zraku a kůže



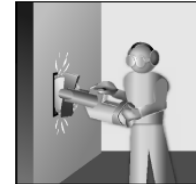
### Padající předměty

- stlačení
- naražení



### Pohybující se prvky

- stlačení
- tření, odření
- naražení
- oddělení



### Prach

- obtížné dýchání
- výbuch
- ztráta zraku



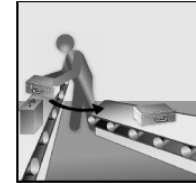
### Pohybující se prvky

- stlačení
- naražení
- stříh



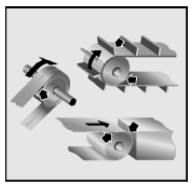
### Živé elektrické části

- zasažení proudem
- popálení
- propíchnutí
- opaření



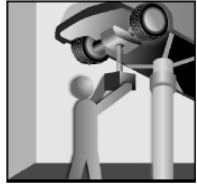
### Poloha těla

- nepohodlí
- námaha
- svalově kosterní poškození



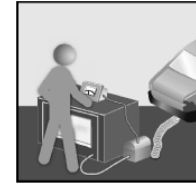
### Pohybující se prvky

- vtažení
- tření, odření
- naražení



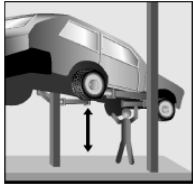
### Předměty nebo materiály s vysokou nebo nízkou teplotou

- popálení



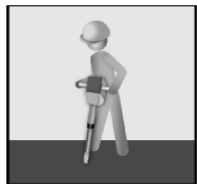
### Kouře

- obtížné dýchání
- dráždění
- otrava



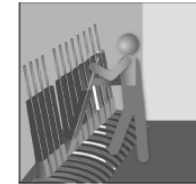
### Tíže, stabilita

- stlačení
- zachycení



### Vibrační zařízení

- poškození kloubů
- cévní poškození



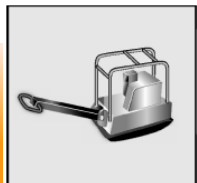
### Umístění ovládacích zařízení

- vždy jako následek lidské chyby
- stres



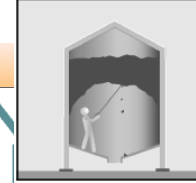
### Přiblížení pohybujícího se prvku k pevné části

- stlačení
- naražení



### Hluk výrobního procesu

- únava
- zhoršení sluchu
- ztráta vědomí
- stres



### Tíže (ztuhnutí sypkého materiálu)

- zřícení, pád, stlačení, udušení
- propadnutí, sesedání
- zaklínění, zacpání

15.10.2010



# EN ISO 12100-1

Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci –

Část 1: Základní terminologie, metodologie

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# EN ISO 12100-1

## Nebezpečí, která je nutno vzít v úvahu při konstruování strojního zařízení

Mechanické nebezpečí

Elektrické nebezpečí

Tepelné nebezpečí

Nebezpečí vytvářená hlukem

Nebezpečí vytvářená vibracemi

Nebezpečí vytvářená zářením

Nebezpečí vytvářená látkami a materiály

Nebezpečí zanedbáním ergonomických zásad při konstrukci stroje

Nebezpečí uklouznutí a pádu

Kombinace nebezpečí

Nebezpečí spojená s prostředím, ve kterém je stroj používán



# EN ISO 12100-1

## Strategie snižování rizika

### Všeobecné opatření

Konstruktér musí vzít v úvahu zkušenosti uživatelů

Ke splnění cíle snížení rizika je třeba brát v úvahu celý životní cyklus se všemi předpokládanými použitími, postupy je často třeba vícenásobně opakovat.

Ochranná opatření nesmí bránit používání stroje

Pokud existují normalizované metody, mají být v konstrukci použity

### Stanovení mezních hodnot stroje

mezní hodnoty používání (ve všech režimech)

mezní hodnoty prostoru

mezní hodnoty času

### Identifikace nebezpečí

vzájemné působení člověka a stroje během celého životního cyklu a všech fázích provozu stroje

možné stavy stroje

nepředpokládané chování obsluhy, nebo předvídatelné selhání stroje

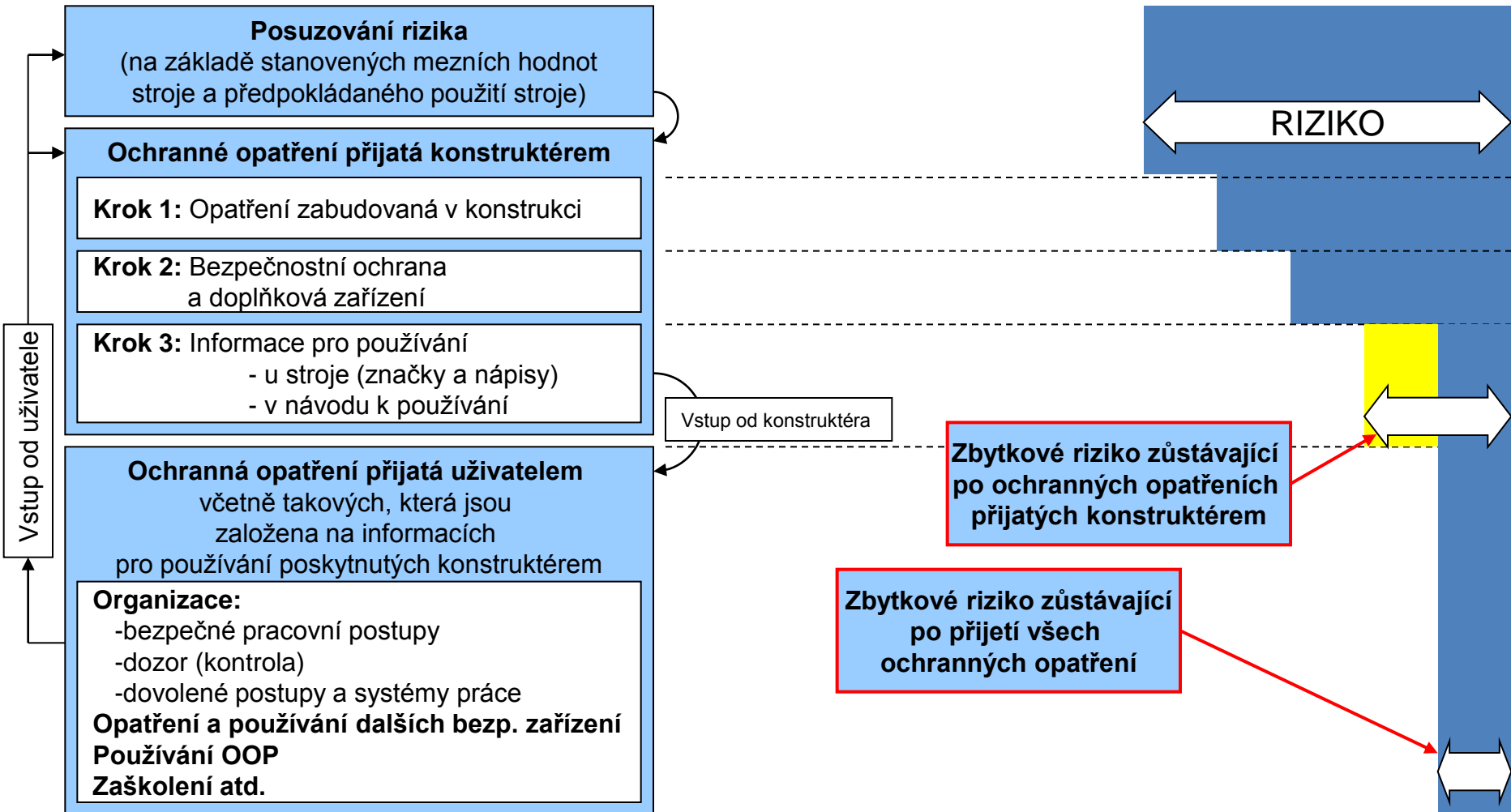
### Vyloučení nebezpečí nebo snížení rizika ochrannými opatřeními

### Dosažení cílů snížení rizika



# EN ISO 12100-1

## Proces snižování rizika z pohledu





# EN ISO 12100-2

Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci –

Část 2: Technické zásady

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ







# EN ISO 12100-2

## Opatření zabudovaná v konstrukci stroje

Všeobecné požadavky

Uvažování geometrických faktorů a fyzikálních hledisek

Uvažování všeobecných technických znalostí pro konstrukci stroje

Volba vhodné technologie

Používání principu pozitivního (nuceného) mechanického působení součásti na jinou součást

Opatření pro stabilitu

Nebezpečí vytvářená zářením

Dodržování ergonomických zásad

Zamezení elektrickému nebezpečí

Zamezení nebezpečím od pneumatického a hydraulického zařízení

Používání opatření zabudovaných v konstrukci pro řídicí systémy

Minimalizace pravděpodobnosti poruchy bezpečnostních funkcí

Omezení ohrožení nebezpečími pomocí spolehlivosti zařízení

Omezení ohrožení nebezpečími pomocí mechanizace a automatizace vkládání  
(podávání)/vykládání (vyjímání)

Omezení ohrožení nebezpečími umístěním seřizovacích a údržbových míst vně nebezpečných  
prostorů



# EN ISO 12100-2

## Bezpečnostní ochrana a doplňková opatření

Všeobecné požadavky

Volba a praktické používání ochranných krytů a ochranných zařízení

Požadavky na konstrukci ochranných krytů a ochranných zařízení

Bezpečnostní ochrana ke snížení emisí

Doplňková ochranná opatření



# EN ISO 12100-2

## Informace pro používání

Všeobecné požadavky

Umístění a charakter informací pro používání

Signály a výstražná zařízení

Značení, značky (piktogramy), psané výstrahy

Průvodní dokumentace (zvláště návod k používání)



# EN ISO 60204-1 ed. 2

Bezpečnost strojních zařízení – Elektrická zařízení strojů –  
Část 1: Všeobecné požadavky

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





## Poskytované informace

- Informace dodávané s elektrickým zařízením musí zahrnovat:
  - **Hlavní dokument** (seznam částí nebo seznam dokumentů);
  - **Doplňující dokumenty** zahrnující:
    - jasný, úplný popis zařízení, instalace a montáže, a připojení k elektrickému napájení (elektrickým napájením);
    - požadavky na elektrické (elektrická) napájení;
    - informace o pracovním prostředí (např. osvětlení, vibrace, hladiny hluku, znečišťující látky v ovzduší), kde to přichází v úvahu;
    - přehledové (blokové) schéma (přehledová (bloková) schémata), kde to přichází v úvahu;
    - obvodové schéma (obvodová schémata);



# EN 60204-1 ed.2

## Informace (kde to přichází v úvahu) o:

- programování, pokud je nutné pro používání zařízení;
- sledu činnosti (činností);
- četnosti prohlídek; četnosti a metodě funkčních zkoušek;
- návodu pro seřizování, údržbu a opravy, zejména ochranných zařízení a obvodů;
- seznamu doporučených náhradních dílů; a
- seznamu dodávaných nástrojů.
- popis (včetně propojovacích schémat) **bezpečnostních ochran, blokovacích funkcí a blokování ochranných krytů proti nebezpečím, zejména u strojů, které pracují koordinovaným způsobem;**
- popis bezpečnostních opatření a prostředků poskytovaných, kde je to nutné pro **dočasné vyřazení bezpečnostních ochran z činnosti (např. pro seřizování nebo údržbu);**
- pokyny pro postupy zajišťování stroje pro bezpečnou údržbu (viz také 17.8);
- informace o manipulaci, dopravě a skladování;
- informace týkající se zatěžovacích proudů, špičkových rozběhových proudů a dovolených poklesů napětí, kde to přichází v úvahu;
- **informace o zbytkovém riziku v důsledku přijatých ochranných opatření, údaj, zda je požadováno jakékoliv konkrétní školení a specifikace veškerých nutných zařízení pro ochranu osob.**



## EN 60204-1 ed.2: 2006

### Bezpečnost strojní zařízení

### Elektrická zařízení strojů - Část 1:Všeobecné požadavky

Tato část EN (IEC) 60204 platí pro používání elektrických, elektronických a programovatelných elektronických zařízení a systémů u strojů, které nejsou během činnosti přenosné rukou, včetně skupiny strojů, které pracují společně koordinovaným způsobem.

Tato část EN (IEC) 60204 je aplikační norma a není určena k tomu, aby **omezovala** nebo brzdila technický pokrok.

**V této části EN (IEC) 60204 termín *elektrický*** zahrnuje elektrické, elektronické a programovatelné elektronické předměty.



## Hlavní vypínač

**musí být použit: pro každý zdroj napájení stroje (strojů);**

Napájení může být připojeno přímo ke stroji nebo přes napájecí systém.

Je-li to požadováno (např. pro práci na stroji, včetně elektrického zařízení), musí hlavní vypínač odpojit (izolovat) elektrické zařízení stroje od napájení.

V případě použití dvou nebo více hlavních vypínačů musí být použito také ochranné blokování pro jejich správnou funkci, aby se zabránilo nebezpečné situaci, včetně poškození stroje nebo rozpracovaného výrobku.

Pokud není stroj vybaven vidlicí pro připojení k napájení, doporučuje se, aby napájecí vodiče byly ukončeny na hlavním vypínači.





**Hlavním vypínačem** může být jeden ze stanovených typů v čl. 5.3.2

- a) až d) a musí splňovat všechny následující požadavky:  
musí bezpečně odpojit elektrické zařízení od napájení a mít  
jednu polohu VYPNUTO (odpojeno)  
a  
jednu polohu ZAPNUTO (připojeno)

s označením „O“ a „I“ ,

Kde **nejsou** vnější ovládací prostředky (prvky) určeny pro **nouzové operace (funkce)**, doporučuje se, aby byly v barvě ČERNÉ nebo ŠEDÉ a **musí být vybaven** prostředky (prvky) umožňujícími jeho zablokování v poloze VYPNUTO (odpojeno) (např. pomocí visacích zámků). Je-li vypínač takto zablokován, musí být zabráněno jak dálkovému, tak místnímu zapnutí;



## Napájení řídicích obvodů

Jsou-li řídicí obvody napájeny ze střídavého zdroje, musí být pro jejich napájení použity **transformátory pro napájení řídicích a ovládacích obvodů**.

Takové transformátory musí mít **oddělená vinutí**. Pokud je použito několik transformátorů, doporučuje se, aby vinutí těchto transformátorů byla zapojena tak, aby sekundární napětí byla ve fázi.

Tam, kde jsou stejnosměrné řídicí obvody odvozené ze střídavého napájení připojeny k ochrannému obvodu (viz 8.2.1), musí být napájeny z odděleného vinutí transformátoru střídavého řídicího obvodu nebo jiným transformátorem řídicího obvodu.

- **Transformátory podle IEC 61558-2-17 splňují tento požadavek.**
- Transformátory **nejsou** povinné pro stroje s jedním spouštěčem motoru a/nebo maximálně dvěma řídicími přístroji (např. blokovací zařízení, řídicí jednotka start/stop).



## Opatření pro omezení rizika v případě poruchy na minimum

Použití osvědčených technik a součástí obvodů

**Tato opatření zahrnují mimo jiné:**

- připojení řídicích obvodů k ochrannému obvodu pro funkční účely;
- zapojení řídicích přístrojů podle 9.4.3.1;
- zastavení odpojením od napětí (viz 9.2.2);
- přepínání všech vodičů řídicích obvodů k řízenému zařízení;
- spínací přístroje s nuceným vypínáním (viz IEC 60947-5-1);
- návrh obvodu zaměřený na omezení možnosti poruch způsobujících nežádoucí činnosti.



## Zemní spojení

- Zemní spojení u jakéhokoliv řídicího obvodu nesmí způsobit neúmyslné spuštění, potenciálně nebezpečné pohyby, nebo zabránit zastavení stroje.

Metody zajišťující splnění těchto požadavků jsou mimo jiné tyto:

- **Řídicí obvody napájené transformátory pro napájení řídicích a ovládacích obvodů:**

V případě uzemněného napájení řídicího obvodu je společný vodič připojen k ochrannému obvodu v místě napájení.



## • **Nouzové funkce (nouzové zastavení, nouzové vypnutí) - Všeobecně**

- Tato část IEC 60204 stanoví požadavky na funkce nouzového zastavení a nouzového vypnutí dle nouzových provozů uvedených v příloze E; obě tyto funkce jsou v této části IEC 60204 vyvolány jedním zákrokem člověka.
- Jakmile se ovládací prvek funkce nouzového zastavení (viz 10.7) nebo nouzového vypnutí (viz 10.8) přestane ovládat, musí být působení tohoto povelu **zachováno (aretace)**, dokud nedojde k resetování (výchozí stav). Toto resetování (výchozí stav) musí být možné pouze ručním působením na tom prvku, kde byl povel vyvolán. **Obnovení povelu nesmí znovu spustit strojní zařízení, ale pouze umožnit nové spuštění.**
- Nesmí být možné znovu spustit strojní zařízení, dokud nejsou znovu nastaveny všechny povely pro nouzové zastavení. Nesmí být možné připojit strojní zařízení znovu k elektrickému napájení, dokud nejsou znovu nastaveny do výchozí polohy všechny povely pro nouzové vypnutí.
- **POZNÁMKA** Nouzové zastavení a nouzové vypnutí jsou doplňující ochranná opatření, která nejsou primárními prostředky omezení rizika proti nebezpečím (např. zachycení, zapletení se, úraz elektrickým proudem nebo popálení) u stroje (viz ISO 12100 (všechny části)).



## Nouzové zastavení

Zásady pro navrhování zařízení nouzového zastavování, včetně funkčních hledisek, jsou uvedeny v **ISO 13850**.

Nouzové zastavení musí **fungovat buď jako zastavení kategorie 0 nebo jako zastavení kategorie 1**.

**Výběr kategorie nouzového zastavení závisí na výsledcích hodnocení rizika stroje.**

- **Kromě požadavků na zastavení, jsou na funkci nouzového zastavení kladeny následující požadavky:**

musí být nadřazena všem ostatním funkcím a činnostem ve všech režimech; napájení ovládacích částí stroje, které mohou způsobit **nebezpečný stav** (nebezpečné stavy), musí být buď okamžitě přerušeno (**zastavení kategorie 0**), nebo musí být řízeno tak, aby byl nebezpečný pohyb zastaven co nejrychleji (**zastavení kategorie 1**), aniž by vznikla jiná nebezpečí; reset (návrat do výchozího stavu), nesmí vyvolat opětné spuštění.



## Nouzové vypnutí

- Funkční hlediska nouzového vypnutí jsou uvedena v 536.4 IEC 60364-5-53.
- **Nouzové vypnutí má být zajištěno tam**, kde:  
ochrany před nebezpečným dotykem živých částí (např. s vodiči, přípojnicemi, soupravami sběracích kroužků s kartáči, řídicím zařízením v prostorech pro obsluhu elektrického zařízení) se dosahuje pouze umístěním mimo dosah nebo zábranami (viz 6.2.6); nebo  
existuje možnost jiných nebezpečí nebo poškození způsobených elektřinou.



Mgr. Karel Stibor

# BEZPEČNOSTNÍ FUNKCE A PROSTŘEDKY OMEZOVÁNÍ RIZIKA

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ







# Snížení rizik bezpečnostní ochranou

- **Rizika se omezují vhodnými opatřeními s certifikovaným řešením:**
  - Nouzové zastavení (na každém stroji a zařízení)
  - Dvouruční ovládání
  - Snímání přítomnosti/nepřítomnosti (nášlapné rohože, optoelektronické prvky atd.)
  - Omezení přístupu do nebezpečného prostoru
  - Pohyb bezpečnou rychlostí (v součinnosti např. se světelnou závorou)
  - Hlídkání koncových prvků (zpětné hlášení bezpečnostnímu HW)
  - Zamezení proti opětovnému zapnutí (tlačítko Reset – nezaměňovat s Restartem)



# Všeobecné požadavky a funkce

## EN 60204-1 ed.2 Bezpečnost strojních zařízení – Elektrická zařízení strojů Část 1: Všeobecné požadavky

EN ISO 13849-1

EN 60204-1 ed.2 čl. 9.2.5.4

### Nouzové funkce

nouzové zastavení  
(EN 13850),  
nouzové vypnutí  
(IEC 60364-5-53)





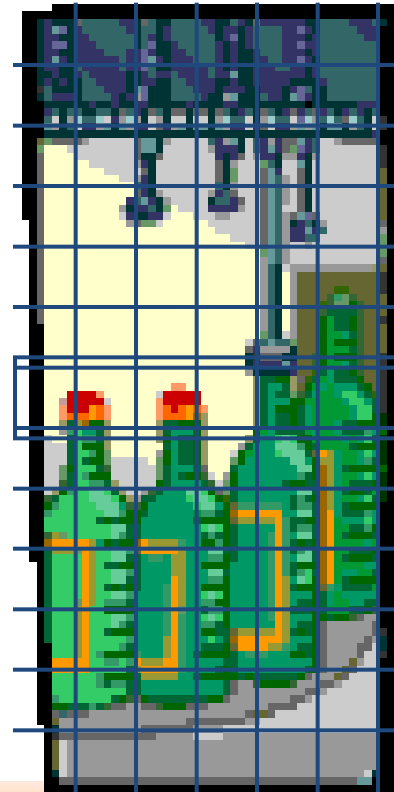
# Zajištění bezpečnostních krytů

Nejedná se CELKOVĚ o kryty, pouze hlídání (blokování) jejich zavření...

**EN 1088** - Bezpečnost strojních zařízení – Blokovací zařízení spojená s ochrannými kryty - Zásady pro konstrukci a volbu

**EN 60204-1 ed.2**

**EN ISO 13849-1**



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Elektrická snímací zařízení

**EN 1088** Bezpečnost strojních zařízení – Blokovací zařízení spojená s ochrannými kryty - Zásady pro konstrukci a volbu

**EN 61496-1** Bezpečnost strojních zařízení - Elektrická snímací ochranná zařízení - Část 1: Všeobecné požadavky a zkoušky

**EN 60204-1 ed.2,**

**CLC/TS 61496-2 ed.2**



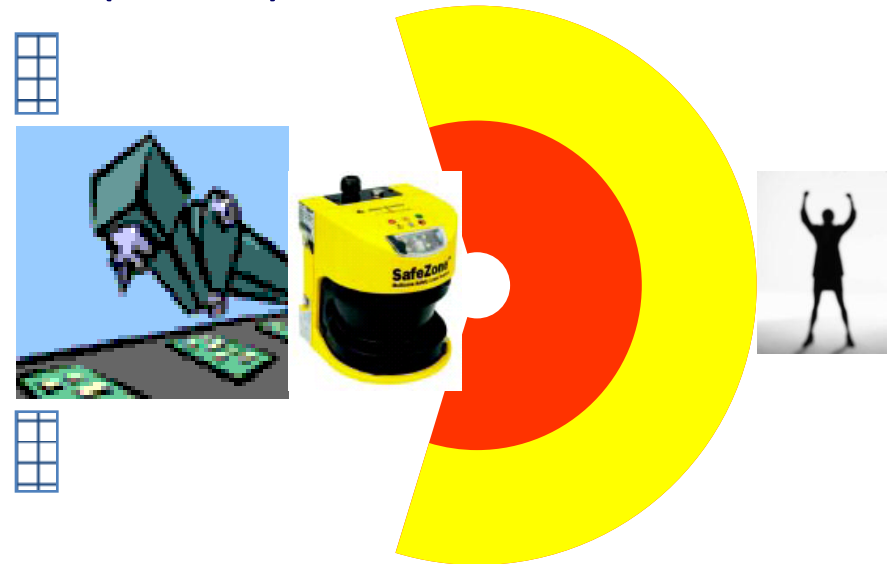


# Elektrická snímací zařízení

**EN 61496-1** Bezpečnost strojních zařízení - Elektrická snímací ochranná zařízení - Část 1: Všeobecné požadavky a zkoušky

**CLC/TS 61496-2 ed.2** Bezpečnost strojních zařízení - Elektrická snímací ochranná zařízení - Část 2: Zvláštní požadavky na aktivní optoelektronická ochranná zařízení (AOPD)

**CLC/TS 50418** Bezpečnost strojních zařízení – Elektrická snímací ochranná zařízení - Pasivní infračervená ochranná zařízení (PIPD) Světelné závory



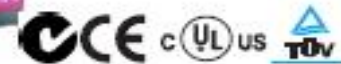


# Bezpečnostní části řídicích systémů

**EN ISO 13849-1** Bezpečnost strojních zařízení - Bezpečnostní části řídicích systémů - Část 1: Všeobecné zásady pro konstrukci

**EN ISO 13849-2** Bezpečnost strojních zařízení - Bezpečnostní části řídicích systémů - Část 2: Ověřování

**EN 60204-1, ed.2 čl.9 – Řídicí obvody a řídicí funkce**





Mgr. Karel Stibor

# NÁSTROJ SISTEMA

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Představení nástroje Sistema

**SISTEMA** je softwarový nástroj pro implementaci EN ISO 13849-1 (Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů)

- EN ISO 13849-1 nahrazuje starou EN 954-1.
- **SISTEMA** je preferovaný nástroj mnoha výrobců doporučovaný i TÜV, v budoucnu plně podporovaný ČOI a UNMZ
- Nástroj je bezplatný
- Je vyvinuta IFA (Institut Für Arbeitsschutz) v Německu (dřívější BGIA) jako nestrannou certifikační autoritou

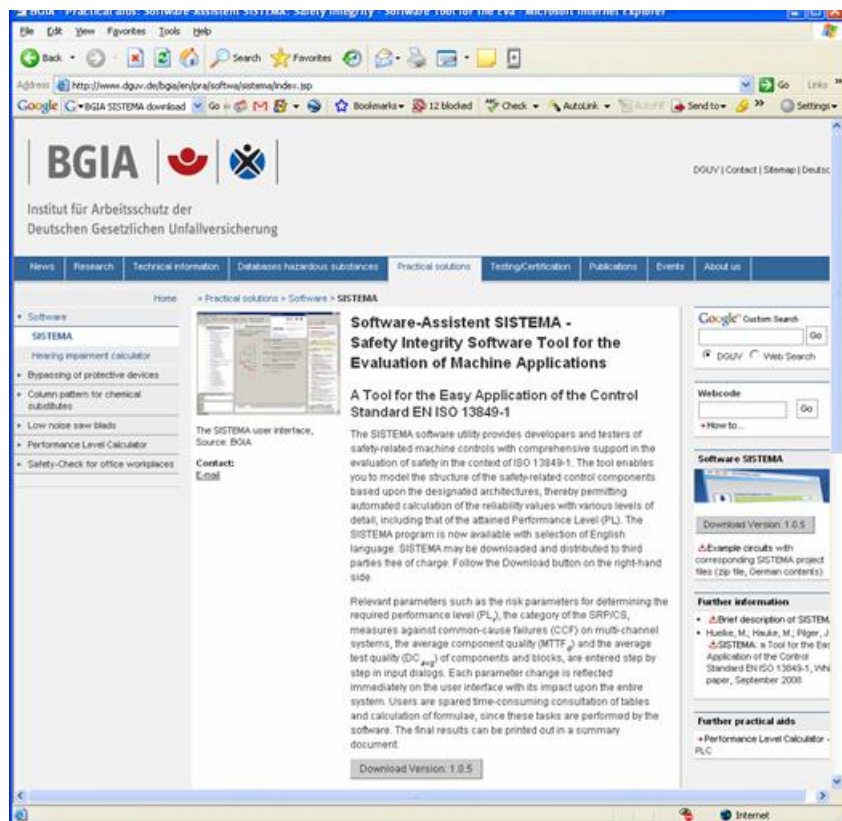




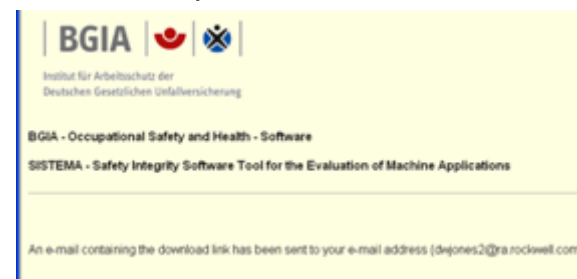
# Odkud získat?

## Jak získat SISTEMU (dostupná prozatím v Němčině a Angličtině)

1 Navštivte <http://www.dguv.de/bgia/en/prg/softwa/sistema/index.jsp>



2 Klikněte na **Download** – Dostanete e-mail s odkazem pro nahrání



3 Přihlašte se, nahrajte si program a následujte instrukce pro instalaci



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



113



**SISTEMA** vyžaduje vstupní údaje funkčních dat.

Data mohou být zadávána manuálně, nebo automaticky nahráním dat z knihoven výrobců.

Balluff, BBH Products, Bernecker & Rainer Industrie-Elektronik, Bihl Wiedemann, Bosch Rexroth, Eaton Electrical Sector EMEA, Moeller, EUCHNER, Fiessler Elektronik, Gunnebo Troax, JOKAB SAFETY, Lenze Automation, Leuze electronic, Pepperl Fuchs, Pilz, Pizzato Elettrica, REER, Riese electronic, Rockwell Automation, Schmersal, Schneider Electric Automation, SEW EURODRIVE, SICK, Wenglor sensoric, Wieland Electric



# Po instalaci

Nyní by jste měli být schopni spustit program SISTEMA

Klikněte na logo SISTEMA v panelu rychlého spuštění



*Pokud jste si nainstalovali SISTEMU v Anglické mutaci, toto je výchozí obrazovka po spuštění:*





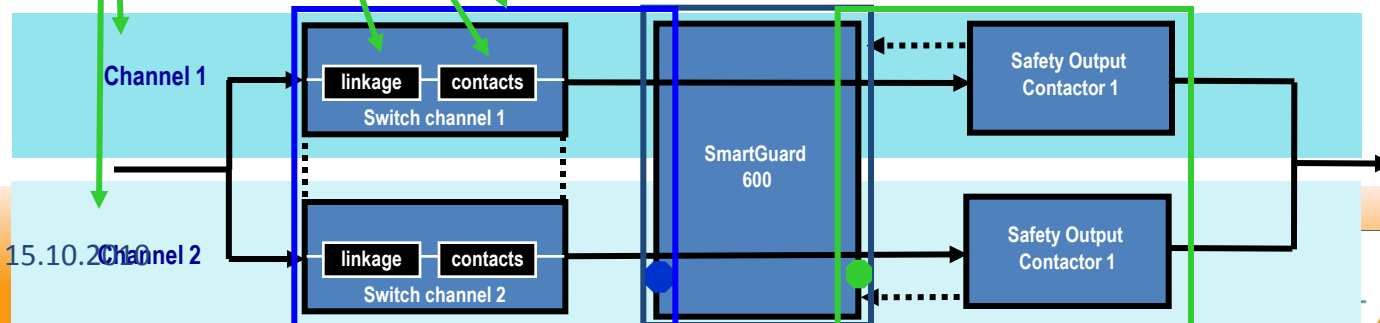
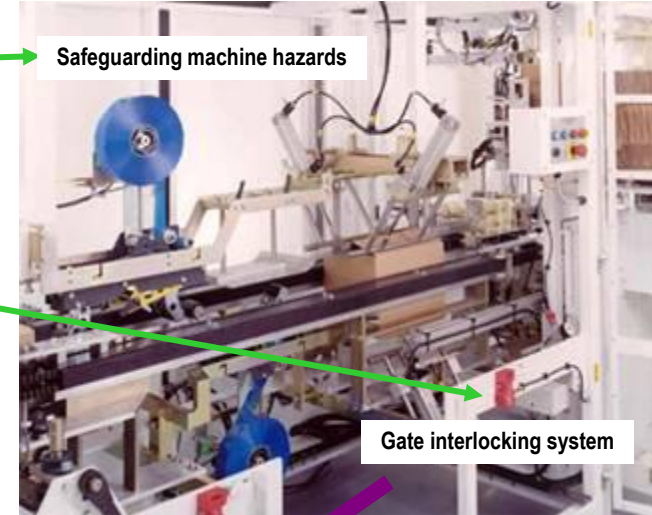
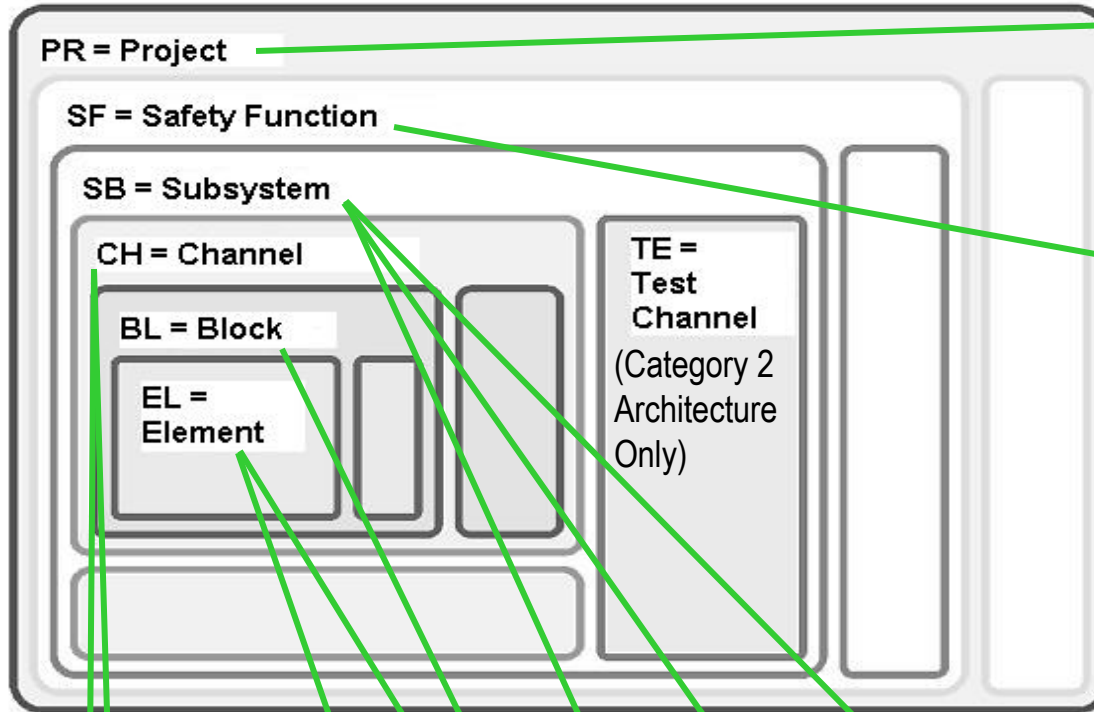
# Terminologie

- SISTEMA má 7 základních elementů ze kterých se skládá každý projekt
  - **Project** (obecně odkazuje na stroj nebo nebezpečný bod, na jehož analýzu je použita SISTEMA)
  - **Safety Function** (jakákoliv funkce stroje v analýze, jehož porucha může vést k přímému zvýšení rizika)
  - **Subsystem** (část řídicího systému, která zpracovává a generuje bezpečnostní signály; více subsystémů může být spojeno do série k implementaci bezpečnostní funkce)
  - **Channel** (oblast, jejíž jedinnou oblastí je strukturovat řídicí systém; subsystém může mít jeden nebo dva kanály v závislosti na kategoriích)
  - **Test channel** (má funkci opakovaného testování a zjišťování jeho správného provedení. Testovací kanály jsou součástí subsystému).
  - **Block** (Představuje funkční blok v jehož kontextu je logický blok schématu. Dělí kanál do logických funkčních jednotek, jako např. senzory, logika a stykače)
  - **Element** (nejnižší hierarchická úroveň základních prvků. Element může být elektronický, elektromechanický, hydraulický, mechanický nebo pneumatický)



# Terminologie

- Vztah mezi 7mi elementy

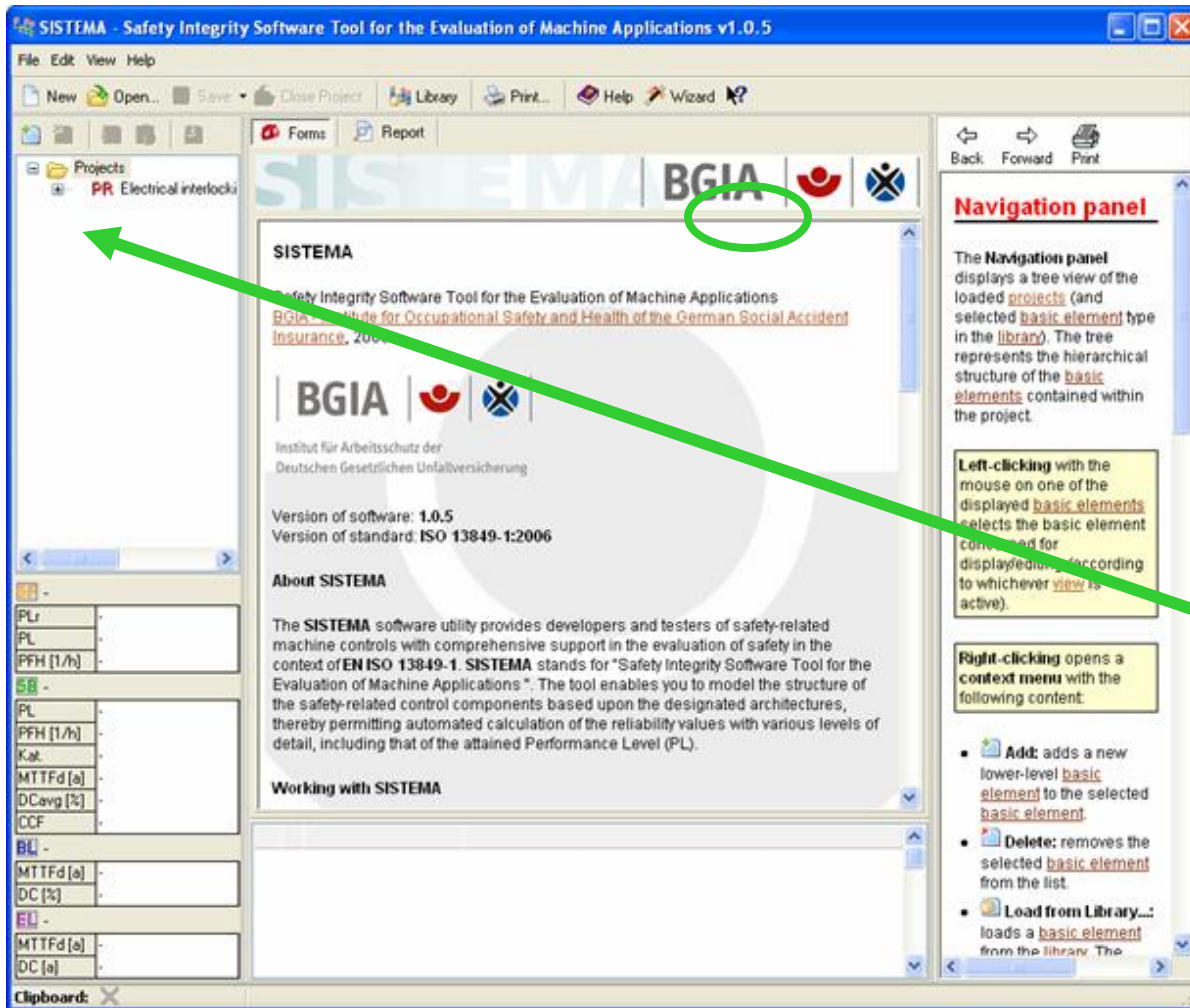


15.10.2010





# Seznámení s programem



Při prvním spuštění si pořádně prohlédněte program. Nemějte obavy pokud budete u první práce sklíčení, vše se časem vyjasní.

**Dva tipy:**

**1** Začněte se dívat sem. Jsou zde zobrazovány základní popisy funkčnosti a struktura SISTEMY

**2** Potom klikněte na toto menu k otevření struktury příkladu projektu obsaženého v každé instalaci. Jedná se o nekonvenční příklad, nicméně demonstruje přizpůsobitelnost SISTEMY

At this stage do not save changes

15.10.2010



# Kde co najdeme v hlavním okně programu

**Stromová  
struktura  
elementů  
projektu**

The screenshot shows the SIMEMA software interface. The main window is titled 'Block' and contains a form for editing a block's documentation. The block name is 'Interlock Switch: Trojan 5'. The documentation field contains a catalog number and a URL. The left sidebar shows a tree view of the project structure, with a red box highlighting the 'SB Input device: Trojan 5' and its sub-elements. The right sidebar contains a 'Navigation panel' with a tree view and a list of actions like 'Add', 'Delete', 'Load from Library...', 'Copy to Library...', 'Cut', 'Copy', 'Paste', and 'Move One Place Up'. A red box highlights the 'Add' action. The bottom of the interface shows a table of parameters for the selected block, including 'MTTFd', 'DC', and 'CCF'.

**Shrnutí  
dat**

**Pracovní  
prostor**

**Informace o  
stavu**

**Okno  
pomoci**



## KROK 1

### Knihovna prvků SISTEMA

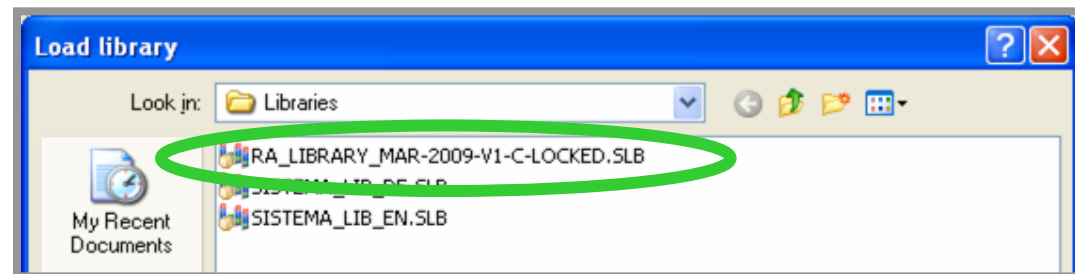
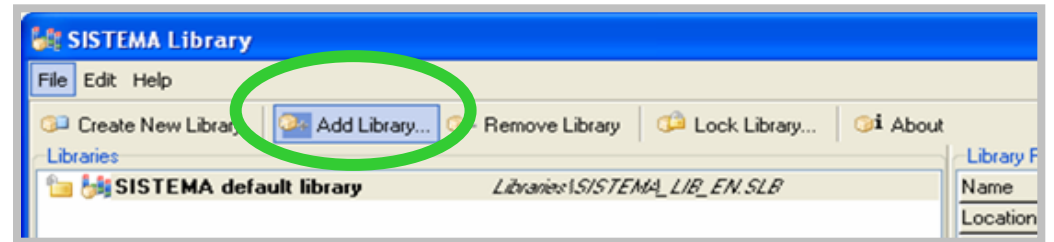
- Nyní se ujistěte, že SISTEMA běží.
- Nahrajte si některou z knihoven produktů. Příklad dále je vytvořes s knihovnou Rockwell Automation Safety
- Naučíte se, jak nahrát data a procházení knihovny produktů (Rockwell Automation)
- Používání knihoven značně zvyšuje efektivitu a rychlost práce se SW SISTEMA
- SISTEMA nenahrává knihovny automaticky, je třeba je udržovat aktuální manuálně





# Přidání knihovny

1. Spustíte SISTEMU
2. Klikněte na “Library”
3. Klikněte na “Add Library”
4. Klikněte na “RA\_ Library”



Nyní jste nahráli knihovnu prvků Rockwell Automation

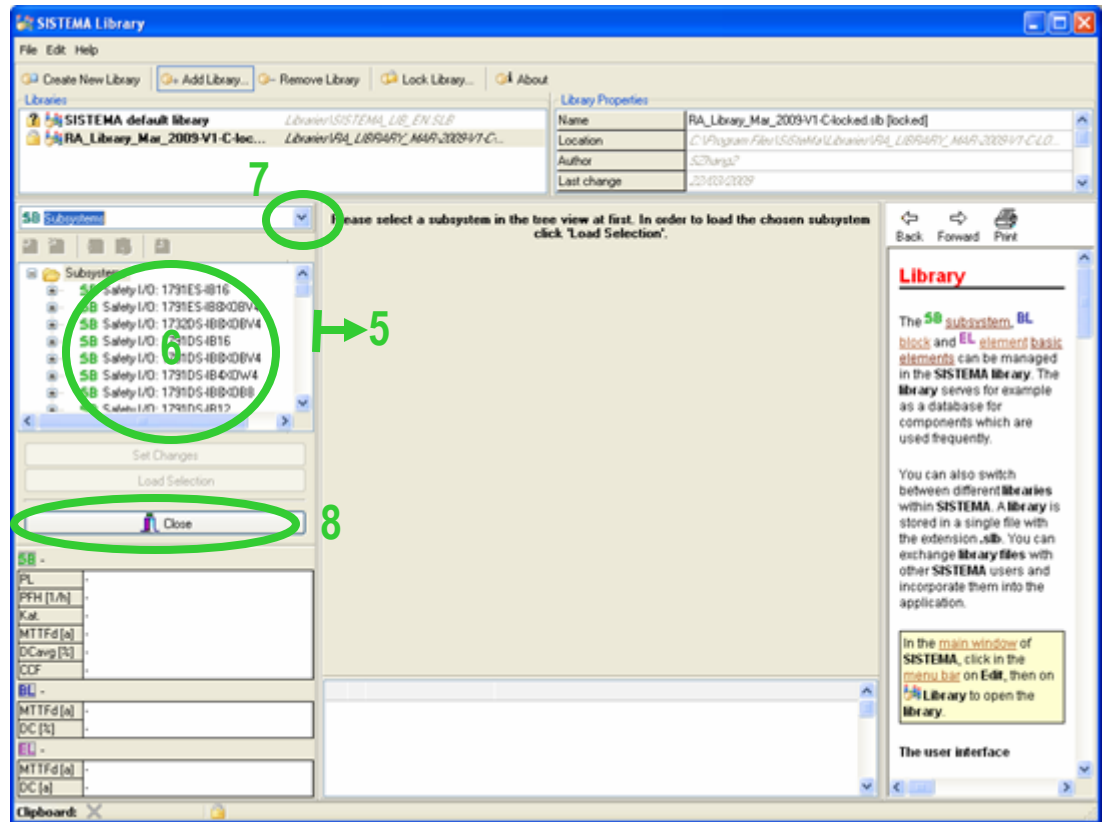


# Okno knihovny prvků

5. Zkuste přetáhnout hranice tak jak potřebujete
6. Prohlédněte si "Subsystémy"
7. Klikněte na „combo-box“ a prohlédněte si bloky a elementy

Uvědomte si, že sada samo-monitorovacích prvků jsou subsystémy

Jednodušší zařízení jsou vedeny jako bloky nebo elementy i přesto, že v jednonálovém zapojení může být blok subsystémem (stykač).





# Přehled obrazovky prvků

Sekce knihoven



Vlastnosti knihovny

Prvky knihovny



Zobrazení vlastností vybraného prvku

Pro zobrazení vlastností prvku na něj klikněte. Zobrazí se detaily.

8. Zavřete okno knihovny pro návrat do hlavního okna



8

Tímto krokem končí prohlídka programu



## KROK 2

### Vytváření projektu

- **Opět se ujistěte, že program běží**
- **Pro úspěšné dokončení tohoto kroku doporučujeme splnit krok 1**
- **Naučíte se, jak použít SISTEMU pro srovnání požadované PLr a dosažené PL typické bezpečnostní funkce.**
- **Pro práci je používána knihovna produktů firmy Rockwell Automation**



# SISTEMA

## KROK 2 Vytváření typického projektu

### Terminologie a použití

Zkratky a vysvětlení typů dat potřebných jako vstup do SW Sistema.  
Pro celé znění použijte EN ISO 13849-1

PL – Úroveň vlastností (Performance Level)

PFH or PFHd – Pravděpodobnost (nebezpečné) poruchy za hodinu

Category – Kategorie architektury dle EN ISO 13849-1

Mission Time – Doba pokrývající předpokládané použití SRP/CS

MTTFd – MTTFd v EN ISO 13849-1 je parametr komponentu a/nebo jednoho kanálu bez jakékoliv pozornosti kladené na ostatní faktory, jako diagnostika, zatímco PFHD je parametr subsystému který diagnostiku a architekturu systému zohledňuje

B10d – zadávaná na úrovni elementů – počet cyklů, dokud 10% komponentů nebude mít nebezpečnou poruchu

nop – počet operačních cyklů

T10d – Vychází z hodnoty B10d – střední doba, dokud 10% komponentů nebezpečně selže. Může být použit jak „Mission Time“ nebo interval mezi funkční zkouškou

DC – Diagnostické pokrytí

CCF – Porucha se společnou příčinou

FE - vyloučení poruchy

### Vstupy na úrovni subsystémů:

PL, PFH, Category, Mission Time (všechny jsou vyplněny automaticky, když je subsystém nahráván z knihovny)

nebo:

Category, MTTFd( každého kanálu), DCavg (průměrné diagnostické pokrytí), CCF(odolnost k poruchám se společnou příčinou), Mission Time. Fault Exclusion pokud jsou použitelné

### Vstupy na úrovni bloků:

MTTFd (nebo B10d zadávané na úrovni elementů), DC (diagnostické pokrytí), Mission Time, Fault Exclusion pokud jsou použitelné.

### Vstupy na úrovni elementů:

MTTFd, DC(diagnostické pokrytí), Mission Time, Fault Exclusion pokud jsou použitelné

nebo

B10d, nop (počet operačních cyklů)



# SISTEMA

## KROK 2 Vytváření typického projektu

Náš **PROJEKT** je zajištění pracovního prostoru tohoto stroje, který pojmenujeme „**XBD2**“



Musíme provést **analýzu úkonů** a **analýzu rizikovosti**  
To odhalí požadované **bezpečnostní funkce**



# SISTEMA

## KROK 2 Vytváření typického projektu

Jedna z potřebných bezpečnostních funkcí je sledování (popřípadě zamykání) bezpečnostního krytu. Funkci pojmenujeme „X guard door interlocking system“



Nyní začneme pracovat s programem SISTEMA

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

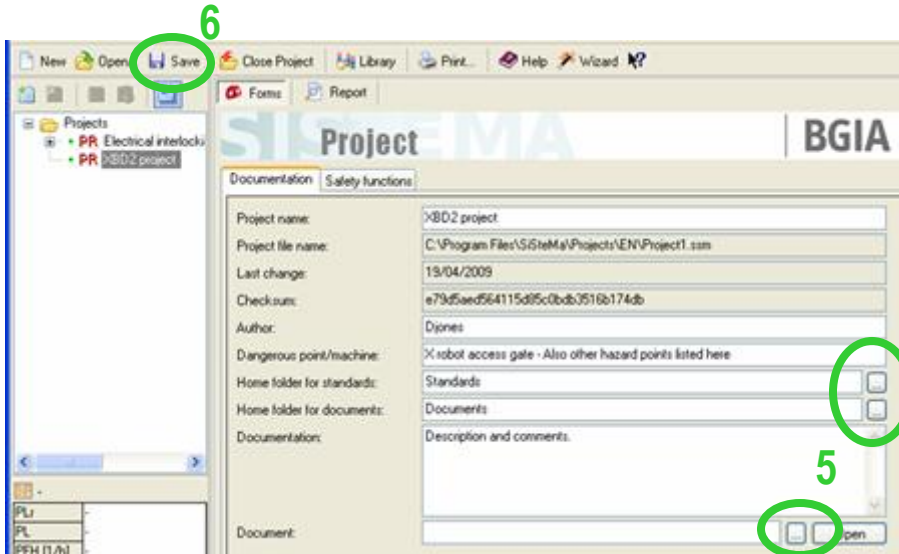
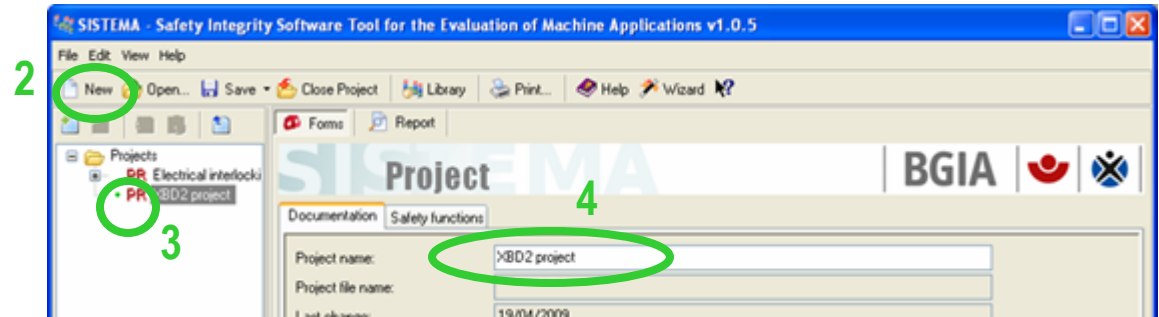




# SISTEMA

## KROK 2 Vytváření typického projektu

1. Spustíme SISTEMU
2. Klikneme na “New”
3. Nový projekt (PR) se objeví ve stromu projektu – klikněte na “PR” pro zobrazení stránky projektu
4. Zadejte jméno projektu (XBD2 project)
5. (Volitelné) Zadejte odkazy na výkresy a další dokumentaci přímo na vaše soubory. Použijte tlačítka „Procházet“.
6. Klikněte na “Save as” – název souboru – např. “XBD2 Project”



Nyní jste vytvořili **Project** – Příští krok jsou **Safety Function**



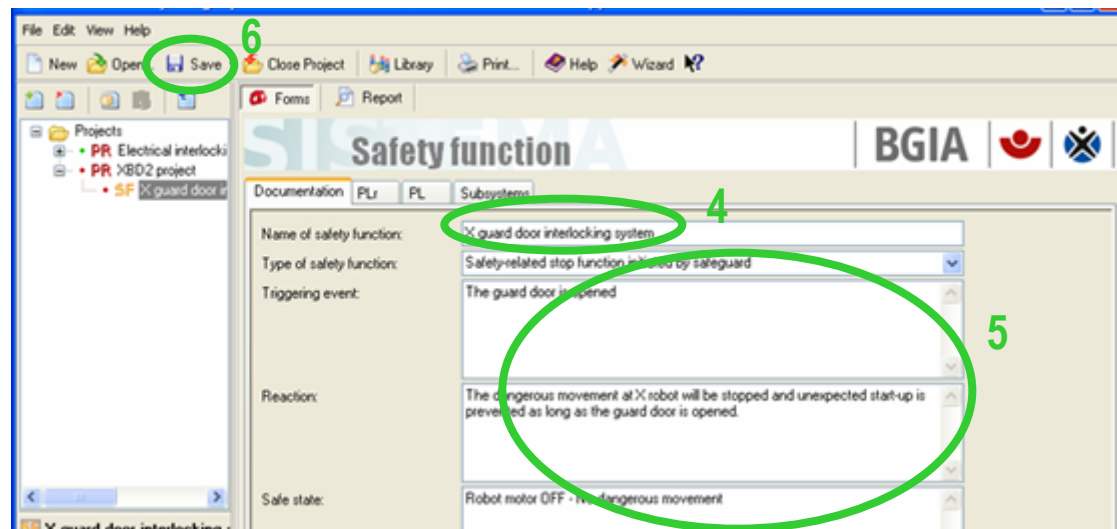
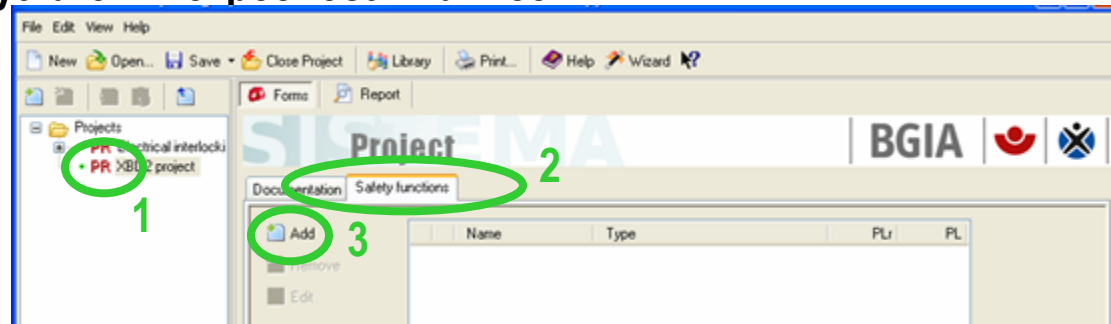


# SISTEMA

## KROK 2 Vytváření typického projektu

### Vytváření Bezpečnostní funkce

1. Klikněte na “PR XBD2 projekt” (pokud jste jinde) abyste zobrazili okno projektu
2. Klikněte na “Safety Functions”
3. Klikněte na “Add” pro přidání okna “Safety function”
4. Zadejte jméno bezpečnostní funkce (X guard door interlocking system)
5. Zadejte detaily a odkazy na jiné soubory, pokud je to třeba. Tyto budou přidány do reportu generovaného na konci procesu. Některé z polí musíte vyplnit pro úspěšné dokončení projektu.
6. Klikněte na “Save”



Nyní jste vytvořili bezpečnostní funkci. Dalším krokem je určit PLr



# SISTEMA

## KROK 2 Vytváření typického projektu

### Určení PLr

1. Klikněte na “PLr” pro zobrazení grafu rizik
2. Ujistěte se, že je vybrána položka “Determine PLr from Risk Graph”
3. Klikněte na “S, F and P” políčka dle potřeby. V tomto případě předpokládejme, že jsme položky vybrali správně pro náš případ
4. Všimněte si, že během procesu budou updatovány hodnoty v poli „Data Summary“
5. Pole zobrazování informací v této fázi nemusí zobrazovat relevantní informace. Pro tentokrát ji ignorujte
6. Klikněte na “Save”

The screenshot shows the SISTEMA software interface. The main window title is "SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications v1.0.5". The interface includes a menu bar (File, Edit, View, Help) and a toolbar with icons for New, Open, Save, Close Project, Library, Print, Help, and Wizard. The main workspace is titled "Safety function" and contains a risk graph with nodes S1, F1, P1, F2, P2, and a legend for Severity of injury (S), Frequency and/or exposure times to hazard (F), and Possibility of avoiding hazard or limiting harm (P). The "Data Summary" table is visible on the left, and a message box at the bottom indicates that no performance level could be computed.

Severity of injury (S)	Frequency and/or exposure times to hazard (F)	Possibility of avoiding hazard or limiting harm (P)
S1 Slight (normally reversible injury)	F1 Seldom to quite often and/or exposure time is short	P1 Possible under specific conditions
S2 Serious (normally irreversible injury or death)	F2 Frequent to continuous and/or exposure time is long	P2 Scarcely possible

Message box: X guard door interlocking No performance level could be computed as there can be no probability of failure estimated based on failure exclusions. Please check whether the required performance level d is permissible based on failure exclusions.

Nyní jsme určili PLr jako PLd – Dalším krokem je návrh systému pro dosažení PLd

15.10.2010



# SISTEMA

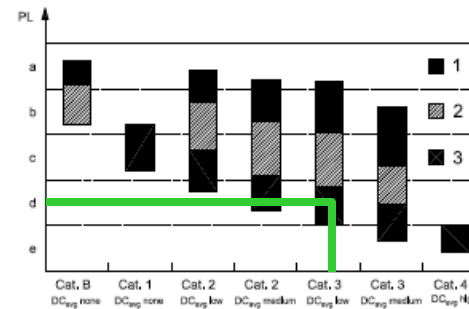
## KROK 2 Vytváření typického projektu

### Návrh systému

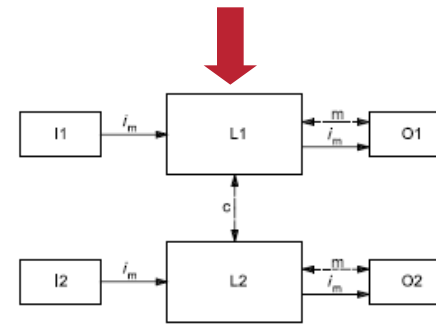
Použijeme obrázek 5 z EN ISO 13849

To achieve PLd we have decided on a Designated Architecture Category 3

- Bezpečnostní kryt bez zamykání monitoruje „X robot guard door“.
- Pozice bezpečnostního krytu je monitorována senzorem Trojan 440K-T který má 2 elektrické kanály
- Stav senzoru Trojan je monitorován bezpečnostním systémem SmartGuard 600
- Dva výstupní bezpečnostní stykače 100S jsou připojeny na výstupy bezpečnostního systému SmartGuard 600.
- Zapojovací schéma může být připojen jako odkaz v okně „Safety function“

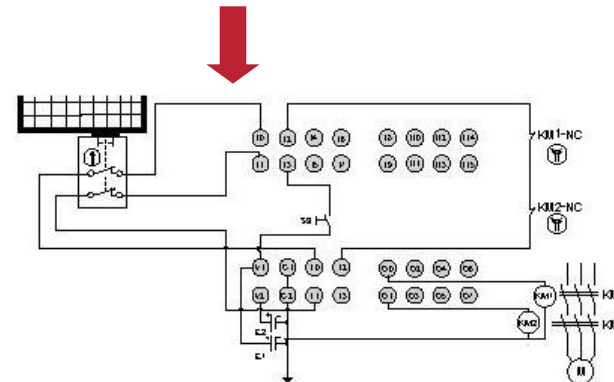


Vztah mezi kategorií, DC a MTTFd



$i_m$  interconnecting means  
 c cross monitoring  
 I1, I2 input device, e.g. sensor  
 L1, L2 logic  
 m monitoring  
 O1, O2 output device, e.g. main contactor

Navržená kategorie 3



Implementace systému

15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu

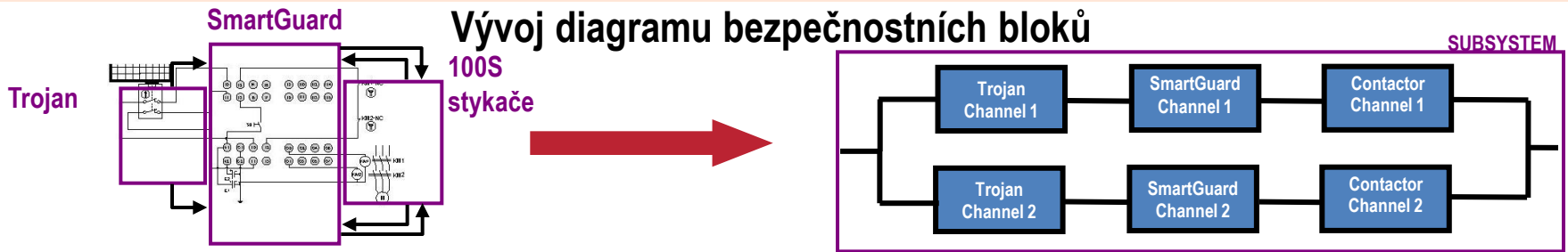


Diagram bezpečnostních funkcí

Musíme uspořádat tento systém do logických posloupností a převést ho na bezpečnostní funkce. **Uvědomte si prosím, že toto je pohled čistě logický a nemá nic společného s fyzickým zapojením komponent.**

Spínače Trojan a stykače je nutno zapojit ve 3. kategorii zapojením kombinací subkanálu pomocí individuálních bloků a přídavné diagnostiky, kterou zajišťuje SmartGuard.

Data pro SmartGuard jsou dostupná v knihovně subsystémů. To znamená, že to je samostatný subsystém, který má diagnostiku a kategorii 4. Protože má jinou kategorii, je umístěn v jiném subsystému.

Diagram může být rovněž uspořádán ve výhodnější konfiguraci, pokud zůstane zachována správná logická posloupnost. V této verzi jsou subsystémy kategorie 3 kombinovány. Data vstupů budou zjednodušeny.

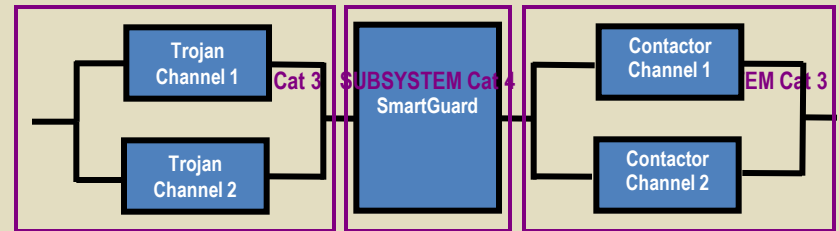


Diagram bezpečnostních funkcí – rozdílné kategorie

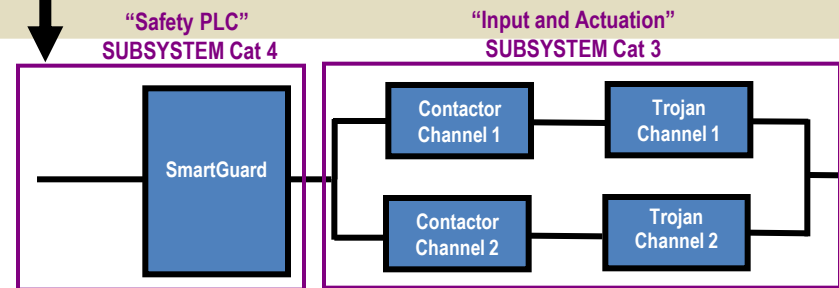


Diagram bezpečnostních funkcí – zjednodušený

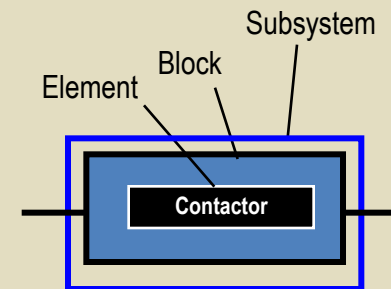
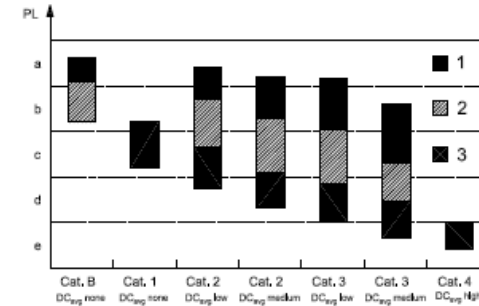


# SISTEMA

## KROK 2 Vytváření typického projektu

### Tipy

1. Obrázek 5 z EN ISO 13849-1 dává informaci, jaká kategorie systému je vyžadována. Rozhodnutí pro použití kategorie 3 je příklad rozhodnutí na základě obrázku č.5.
2. Je obvyklé, že data získaná pro "Block" jsou stejná jako pro "Element". Například pro stykač jsou dána data pro kompletní zařízení, ne pro jeho jednotlivé části. V tomto případě může být z knihovny nahrán jako blok nebo jako element. Abychom tuto skutečnost dokázali, nahrajeme Trojan jako "Element" a stykače jako "Blok"
3. Kdybychom konstruovali jednokanálový systém bez diagnostiky, potom by stykač mohl být přímo subsystémem.
4. Bloky s rozdílnými funkcemi ale stejnou kategorií mohou být kombinovány v jeden subsystém. Kde mají bloky jiné kategorie nebo struktury, musíme je umístit do oddělených subsystémů.





# SISTEMA

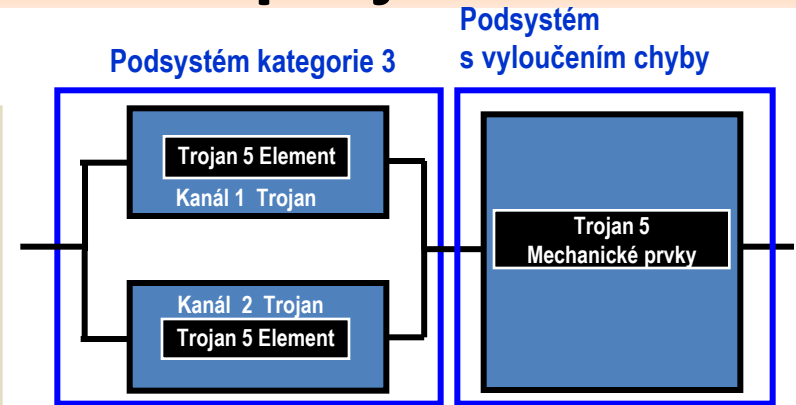
## KROK 2 Vytváření typického projektu

### Použití „Vyloučení chyby“ (FE)

Dokumentace pro Trojan vysvětluje jak se uplatňuje vyloučení chyby pro některé mechanické body, které mohou způsobit poruchu, jako akční prvek a vačka. Pro požadavky vyloučení chyby u PLd 5 lze považovat za mechanickou vazbu.

Poznámka: Pokud použití vyloučení chyby není akceptovatelné (např. pro PLe nebo jiné důvody) potom je nutné použít dvou separátních zařízení.

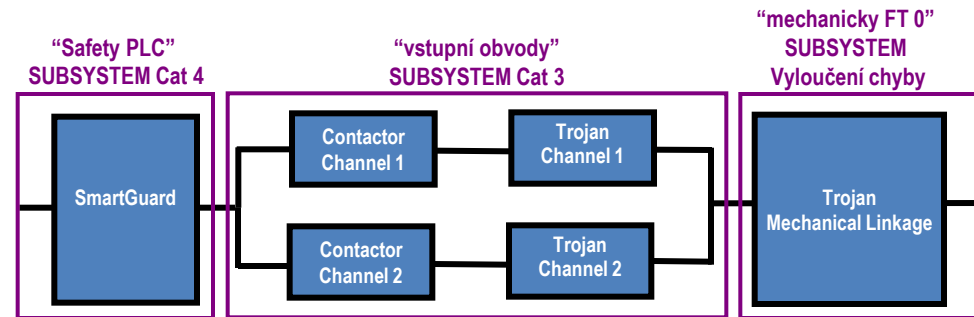
Alternativně může být použita použít technologii, která umožňuje použít prvky s jedním kritickým místem jako například některé typy bezkontaktních dveřních senzorů



Mechanickou vazbu můžeme ze struktury z částí s kategorií 3, pokud lze odůvodnit vyloučení chyby, přesunout do bodu s jedním kritickým místem, kvůli jednoduchosti zadávání dat. Bude rovněž přidán jako jiný subsystem, protože má jinou strukturu než ostatní subsystemy.

Z těchto důvodů výsledný diagram bezpečnostních funkcí bude vypadat takto:

Faktor vyloučení chyby nebude ovlivňovat kalkulaci, je však důležité aby byl zmíněn v závěrečném reportu, aby věrně reflektoval skutečný stav a mohly být přijaty případné opatření (častější kontrola funkčnosti apod.)





# SISTEMA

## KROK 2 Vytváření typického projektu

**PRO SROVNÁNÍ: Použití vyloučení chyby (FE - Fault Exclusion)**

Obecně – do **PLd**, - vyloučení chyby může být použito

Obecně - pro **PLe**, - vyloučení chyby by nemělo být použito

Níže pro podrobnější vysvětlení:

Vstupní spínací subsystém se skládá ze dvojice elektrických kanálů spínače Trojan. Pro potřeby vyloučení chyby u PLd může být toto použito pro mechanickou vazbu. Toto je příklad, který použijeme v našem příkladu subsystému. Potřebujeme se ujistit, že spínač nebude vystaven podmínkám používání (zásah, teplota, vibrace, atd.) které mohou způsobit poškození mechanické vazbě na elektrické obvody. Pro požadavky PLe je mnohem méně snadné ospravedlnit použití vyloučení chyby (viz EN ISO 13849-1 článek 7.3).

Jestli může být vyloučená chyby použito nebo ne, pak buď:

- Musí být použito dvojice fyzických spínačů, nebo
- Použijte dvojkánalový bezkontaktní spínač..Tyto nemají možnost jednotlivé chyby.

Je důležité, že tam, kde se vyloučení chyby používají, musí být řádně odůvodněny a platné pro předpokládané doby životnost subsystémů nebo systémů.

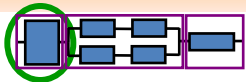
- Obecně, kde je vyžadována PLe pro bezpečnostní funkce implementované SRP/CS nebo SRECS není normální, abychom spoléhali na vyloučení chyby a dosáhli této PL.. Toto je závislé na technologii použité v konkrétních podmínkách. This is dependent upon the technology used and the intended operating environment. Proto je nezbytné, aby konstruktér věnoval další péči exponovaným částem, při požadavcích na užití vyloučení chyby.
- Obecně není vyloučení chyby použitelné pro mechanické aspekty elektromechanických polohových spínačů a manuálně ovládaných prvků (např. zařízení nouzového zastavení) v souladu s požadavky k dosažení PLe řídicího systému. Tyto vyloučení chyby mohou být aplikována jako specifické mechanické chybové podmínky (např. opotřebením, koroze, zlomení), které jsou popsány v tabulce A.4 EN ISO 13849-2.
- Například dveřní snímací systém, který musí dosáhnout PLe bude muset zahrnout odolnost minimálně proti jedné chybě (např. pomocí dvojice nezávislých mechanických spínačů) tak, aby bylo dosaženo požadované PL i přesto, že toto není obvyklé řešení pro vyloučení chyby jako zlomení aktuátoru spínače. Mělo by být však akceptováno pro vyloučení chyby, jako krátké spojení a podobně, pokud je zapojení provedeno dle požadavků potřebných norem.
- Další informace použití vyloučení chyby bude v přicházející revizi normy EN ISO 13849-2

15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu



1. Klikněte pravým tlačítkem na "SF"
2. Ze zobrazeného menu vyberte "Load from Library" pro zobrazení okna knihoven
3. Pokud máte více knihoven, vyberte RA Library
4. Vyberte "SB Subsystem" z Combo-boxu
5. Klikněte na "SmartGuard 600"
6. Klikněte na „Load selection“ – okno knihoven se samo zavře. SmartGuard se nyní objeví v hierarchickém stromě projektu
7. Klikněte na "Save"

The screenshot shows the SISTEMA software interface. The main window displays a project tree on the left with a context menu open over the 'SF' element. The menu option 'Load from Library...' is selected. A dialog box titled 'SISTEMA Library' is open, showing a list of libraries. The 'RA Library\_Mar\_2009-V1-C-loc' is selected. Below the library list, the 'SB Subsystems' dropdown is open, showing a list of subsystems. The 'SB Safety PLC: SmartGuard 600 DeviceNet' is selected. The 'Load Selection' button is highlighted. The background shows the 'Safety function' and 'Subsystem' windows.

15.10.2010





# SISTEMA

## KROK 2 Vytváření typického projektu

### Prohlédněte si data pro SmartGuard nahraná z knihovny

1. Klikněte na “SB” pro zobrazení odpovídající stránky s informacemi o SmartGuard. Povšimněte si, že se data zobrazují i v oblasti souhrnu dat.
2. Klikněte na “Category” pro zobrazení, že pro SmartGuard je uvedeno použití v kategorii 4
3. Klikněte na “PL”. Povšimněte si, že je zaškrtnuta volba “Enter PL/PFH directly”. Protože RA deklaruje tyto data, není nutné jít hlouběji.
4. Povšimněte si, že informační panel poskytuje dodatečné informace a podmínky použití.

**SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications v1.0.5**

File Edit View Help

New Open... Save Close Project Library Print... Help Wizard

Forms Report

Projects

- PR Electrical interlocking of a
- PR XBD2 project
- X guard door interlocking
- SB Safety PLC: SmartG**

1

3 Subsystem

2

Documentation: PL Category MTTFd DCavg CCF Blocks

Name of Subsystem: Safety PLC: SmartGuard 600 DeviceNet

Documentation: Catalog #: 1752-L2488B  
http://ab.com/en/epub/catalogs/12762/2181376/2416247/7448535/

Document: Open

Clipboard: SB

**SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications v1.0.5**

File Edit View Help

New Open... Save Close Project Library Print... Help Wizard

Forms Report

Subsystem

Documentation: PL Category MTTFd DCavg CCF Blocks

Enter PL/PFH directly (refer also to Category tab)

Determine PL/PFH from Category, MTTFd and DCavg

Performance Level (PL): e+ PFH [1/h]: 3.89E-10

Documentation/reasoning:

4

Safety PLC: SmartGuard For the designated architectures a typical mission time of 20 years is assumed. This block has a mission time of 10 years (see register MTTFd), which falls below this value. Please assure to change this block in time.

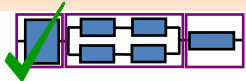
Clipboard: X

15.10.2010



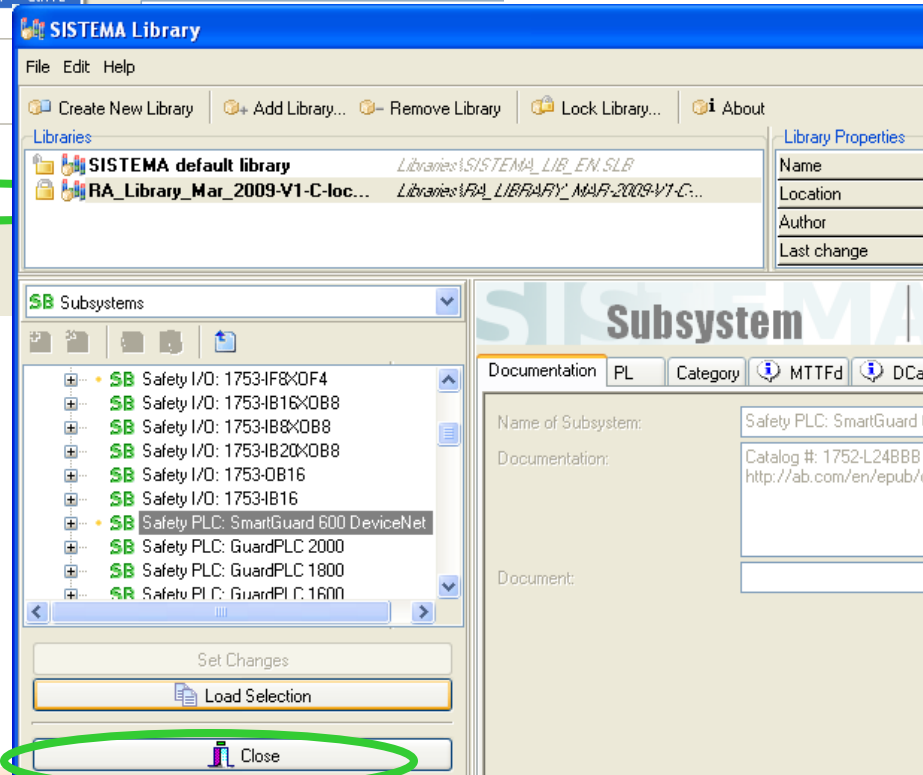
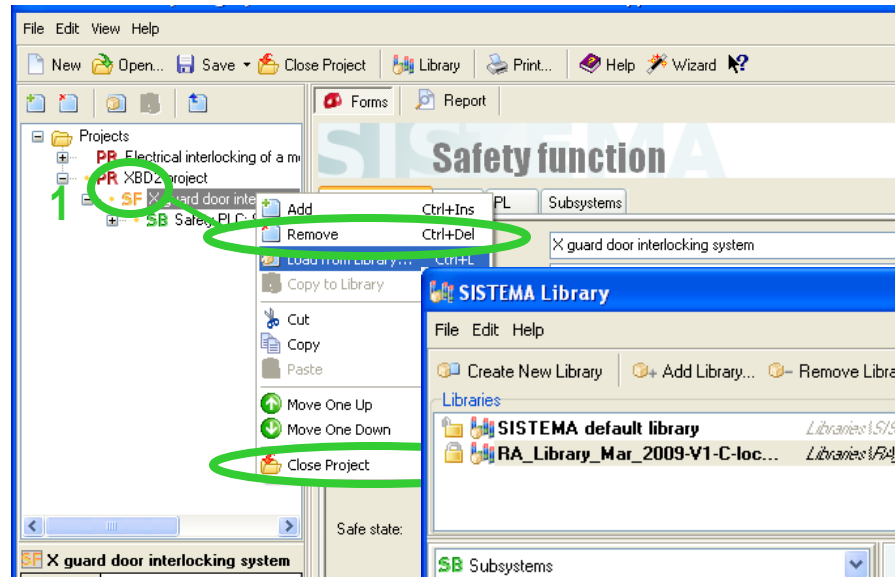
# SISTEMA

## KROK 2 Vytváření typického projektu



### Tipy

1. Můžete použít hierarchický strom pro rychlou navigaci uvnitř SISTEMY. Pokud potřebujete zavřít projekt nebo odstranit **Safety function**, **Subsystem**, **Block** nebo **Element** – nejrychlejším způsobem je kliknout pravým tlačítkem na příslušnou úroveň a vybrat příslušnou položku z pop-up menu.
2. Pokud je otevřené okno knihovny, v hlavním okně SISTEMY můžete číst, nikoliv psát. Pokud potřebujete psát text, klikněte v knihovně na tlačítko "Close". Toto je bezpečnostní opatření, nikoliv chyba programu.



15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu

### Vytvoření subsystému vstupů a aktuátorů

1. S vybraným "SF X guard door" klikněte na záložku "Subsystems".
2. Klikněte na tlačítko "Add" pro přidání subsystému do hierarchie.
3. Pojmenujte subsystém "Input and Actuation". Jakákoliv důležitá informace bude přidávána do pole "Documentation".
4. Klikněte na záložku "Category Tab" pro zobrazení okna s kategoriemi.
5. Pomocí rolovací lišty najděte kategorii 3 a vyberte ji.
6. Později se vrátíme ke kategorii, rovněž ke "CCF" pro doplnění detailů. Tuto informaci nám potvrzuje panel zpráv.

The screenshots illustrate the following steps:

1. Selecting the "Subsystems" tab in the project tree.
2. Clicking the "Add" button to create a new subsystem.
3. Naming the subsystem "Input and Actuation" in the "Subsystem" dialog box.
4. Selecting the "Category" tab in the dialog box.
5. Scrolling through the list of categories to find "3".
6. Viewing the "Documentation/reasoning" field and the "Messages" panel at the bottom.

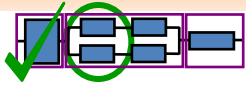
**Tip** – Barevné body v hierarchickém stromu nám dávají rychlou informaci o stavu bezpečnostní funkce či subsystému.

- **Zelená** = znamená žádné chyby, nebo nesplněné podmínky
- **Yellow** = žádné chyby, je nutné splnit dodatečné požadavky z informačního panelu
- **Red** = alespoň jedna chyba, nedůslednost nebo nesplněná nutná podmínka

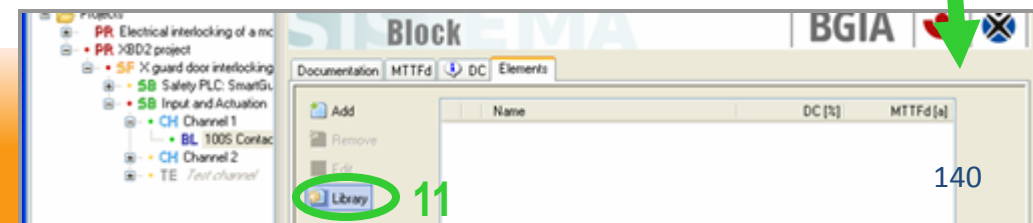
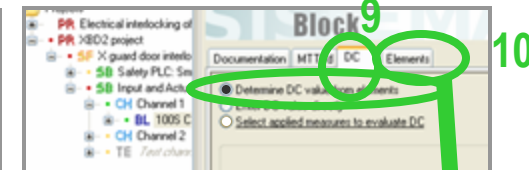
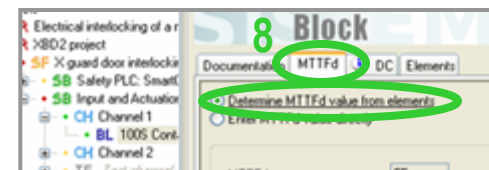
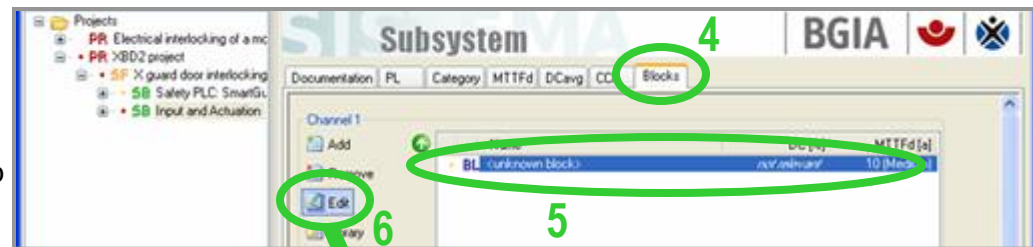
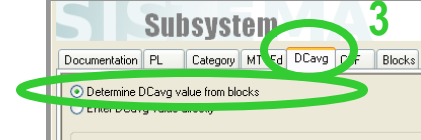
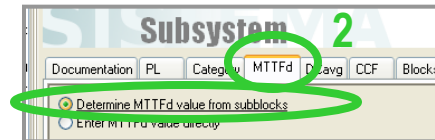
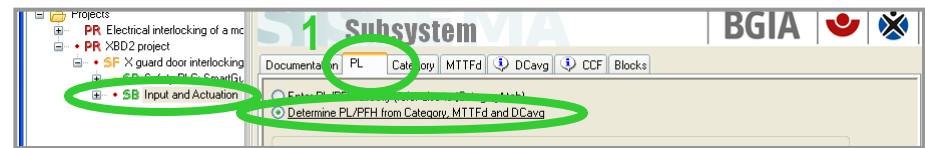


# SISTEMA

## KROK 2 Vytváření typického projektu



### Vytváření bloku stykače 100S



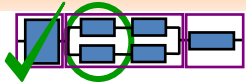
1. S vybraným blokem "SB Input and Actuation" klikněte na záložku "PL" a ujistěte se, že je vybráno "Determine the PL/PFH from Category, MTTFd and DCavg".
2. Klikněte na záložku "MTTFd" a ujistěte se, že je vybráno "Determine the MTTFd value from subblocks".
3. Klikněte na záložku "DCavg" a ujistěte se, že je vybráno "Determine DCavg value from blocks".
4. Klikněte na záložku "Blocks".
5. V panelu kanálu 1: klikněte na "BL <unknown block>" pro jeho výběr
6. Klikněte na „Edit“
7. Zadejte do pole jméno "100S Contactor"
8. Klikněte na záložku "MTTFd" a ujistěte se že je vybráno "Determine the MTTFd value from elements"
9. Klikněte na záložku "DC" a ujistěte se, že je vybráno "Determine the DC value from elements"
10. Klikněte na "Elements"
11. Klikněte na "Library"

15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu



### Nahrávání elementů stykače 100S Contactor “Elements” do bloků

1. Ujistěte se, že máte vybránou knihovnu RA.
2. Vyberte z combo-boxu “EL Elements”
3. Klikněte na “Output Contactor: 100S-C”
4. Klikněte na tlačítko „Load selection“ – Okno knihovny se zavře.
5. Klikněte na “Save”
6. Rozklikněte hierarchii “BL 100S Contactor” a poté klikněte na “EL Output Contactor 100S-C”
7. Pole “Documentation” informuje o hodnotách MTTFd a B10d (protože se jedná o elektromechanické zařízení)
8. Klikněte na záložku “MTTFd”
9. Ujistěte se, že je vybráno “Determine the MTTFd value from B10d value”

The screenshots show the following steps:

1. Selecting the RA library in the library list.
2. Selecting 'EL Elements' in the dropdown menu.
3. Selecting 'Output Contactor: 100S-C' in the element list.
4. Clicking the 'Load Selection' button.
6. Expanding the 'BL 100S Contactor' hierarchy to show 'EL Output Contactor 100S-C'.
7. Viewing the 'Documentation' field for the selected element, which contains technical data.
8. Switching to the 'MTTFd' tab in the documentation window.
9. Selecting the option 'Determine MTTFd value from B10d value' in the documentation window.

### Information

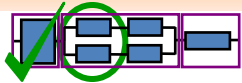
Electromechanical devices have B10d values - Electronic devices will either be “Subsystems” or the MTTFd will be entered directly at the “Element” or “Block” level

15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu



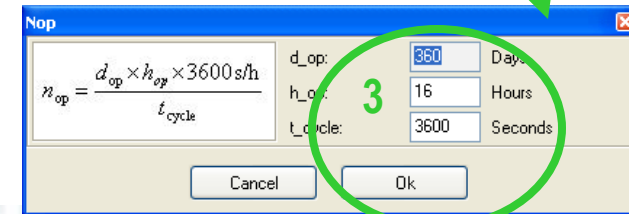
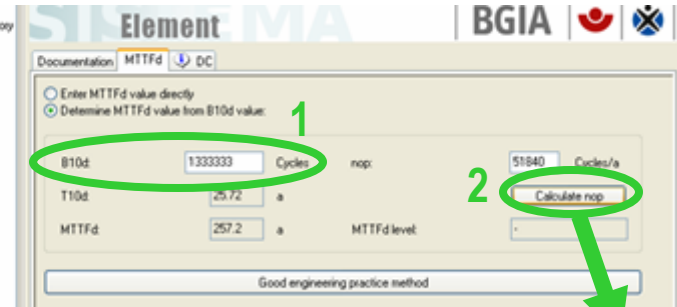
### Určování MTTFd z B10d pro elementů stykače

Hodnotka MTTFd stykače 100S-C vychází z hodnoty **B10d** a **cyklů** (počet operačních cyklů). Budeme předpokládat, že stroj pracuje **360 dní** za rok, **16 hodin denne** a ochranný kryt je otvírán průměrně jedenkrát za hodinu (tzn každých **3600 sekund**).

1. Hodnota B10d stykače 100S-C je 1.333.333
2. Klikněte na tlačítko "Calculate nop"
3. Zadejte 360 (dní - days), 16 (hodin – hours), 3600 (sekund - seconds) a klikněte na "OK"
4. Pole "Cycles/a", "T10d" a "MTTFd" budou automaticky přepočítána.
5. Klikněte na záložku "DC"

**DŮLEŽITÉ** – pro "Elements" s hodnotou **B10d** (nahranou z knihovny), a výchozí hodnotou 51840 je dána pro počet cyklů/rok. Reálná hodnota musí být přepočítána výše popsaným postupem pro každou aplikaci.

Technical interlocking of a movable guard - Category X2 project  
 X2 guard door interlocking system  
 SB Safety PLC: SmartGuard 600 DeviceNet  
 SB Input and Actuation  
 CH Channel 1  
 BL 100S Contactor  
 EL Output Contactor: 100S-C  
 CH Channel 2  
 TE Test channel





# SISTEMA

## KROK 2 Vytváření typického projektu

Pro stovnáni:

### Okno elementů MTTFd

MTTFd bude zadáno přímo pro elektronické komponenty

Hodnota B10d je pro elektromechanické elementy a ostatní „pohyblivé části, jako hydraulika či pneumatika. Je nahrána automaticky, když je element nahráván z knihovny

MTTFd bude určeno z hodnoty B10d pro elektromechanické elementy (nebo ostatní „pohyblivé části“ technologie, jako hydraulika či pneumatika).

The screenshot shows the 'Element' software interface for MTTFd calculation. The interface includes the following fields and controls:

- Documentation:** MTTFd, DC
- Options:**
  - Enter MTTFd value directly
  - Determine MTTFd value from B10d value:
- Input Fields:**
  - B10d: 2000000
  - T10d: 347.22
  - MTTFd: 3472.22
  - Mission time: 39
- Output Fields:**
  - Cycles nop: 5760
  - MTTFd level: .
- Buttons:** Calculate nop
- Dropdown:** Good engineering practice method

Pole počtu operačních cyklů

Tlačítko pro výpočet počtu operačních cyklů z počtu předpokládaných užití systému. Jedná se o součást převodi B10d na MTTFd.

Hodnota MTTFd v letech

Tlačítko "Good engineering practice method" dovoluje zadávat hodnoty komponentů z EN ISO 13849-1 tabulky C1. Užití není součástí této prezentace.

Hodnota **mission time** odkazuje na dobu limitující použitelnost komponentu. Aktuální doba použití komponentu nesmí tuto hodnotu **mission time** překročit. Pokud hrozí překročení této hodnoty, komponent musí být zaměněn **za stejný typ** před uplynutím doby. Hodnota pro elektronické zařízení je finální hodnota udávaná výrobcem. Hodnota u mechanických a elektromechanických prvků je založena na hodnotě T10d.

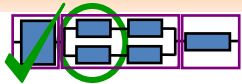
**T10d value** se uplatňuje u elementů s mechanickou charakteristikou. Uvádí operační dobu jejich použití v závislosti na aplikaci. Hodnota je založena na hodnotě B10d. Aktuální operační doba nesmí nikdy překročit hodnotu T10d. Pokud hrozí překročení hodnoty, komponent musí být vyměněn za stejný typ před uplynutím doby. Hodnota ukazuje požadovanou dobu T10d pro komponenty.

15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu

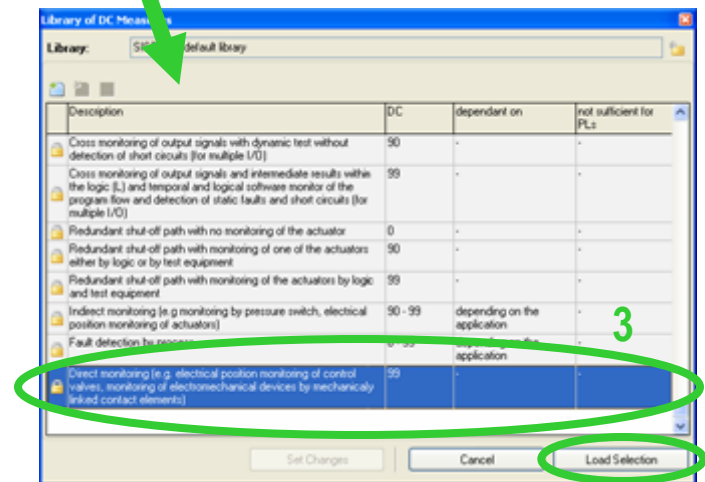
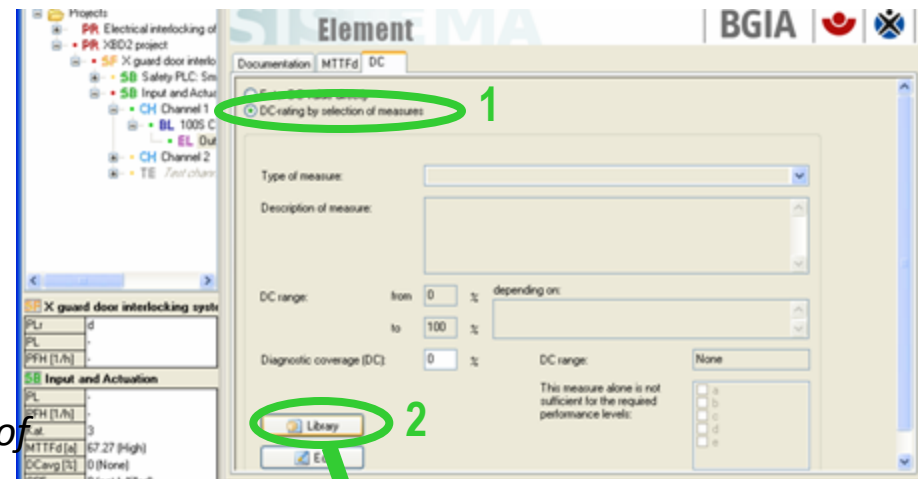


### Určování DC pro elementy stykačů

SISTEMA poskytuje přístup k tabulkám opatření EN ISO 13849-1 pro diagnostické monitorování, které může být určeno pro stanovení DC (Diagnostic Coverage – diagnostické pokrytí).

**DŮLEŽITÉ** výběr určení pro stykače bere v úvahu architekturu kategorie 3, např. redundantní konfigurace s monitorováním pomocí bezpečnostní PLC SmartGuard. Jeden ne-monitorovaný stykač (kategorie 1) bude mít DC rovnou nule.

1. Ujistěte se, že je zvoleno “DC-rating by selection of measures”
2. Klikněte na tlačítko “Library” pro získání přístupu do tabulky opatření
3. Posuvníkem naleznete “Output device” a vyberte “Direct monitoring (e.g. electrical position monitoring....)”
4. Klikněte na tlačítko “Load Selection” – DC je nyní 99% (High - vysoká)
5. Klikněte na “Save”

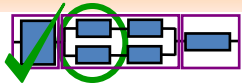






# SISTEMA

## KROK 2 Vytváření typického projektu

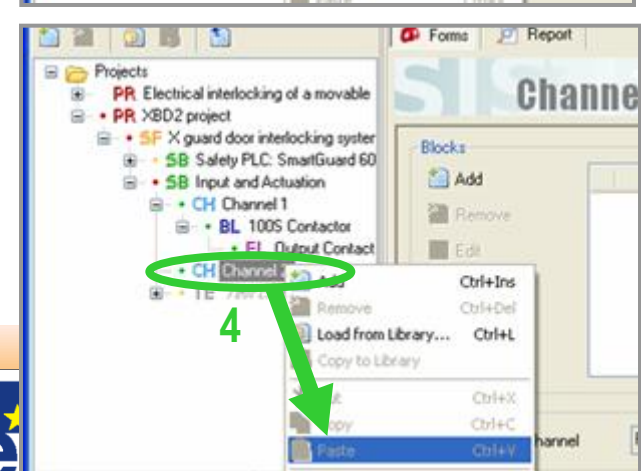
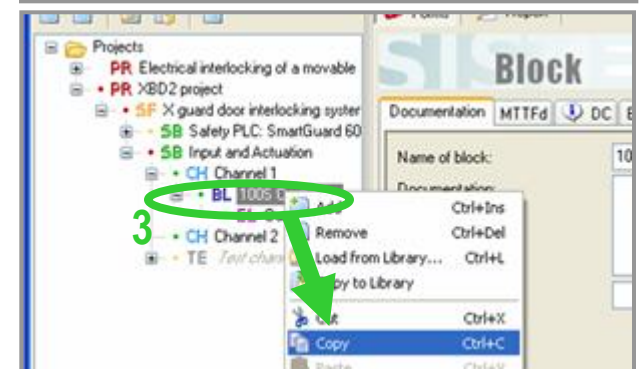
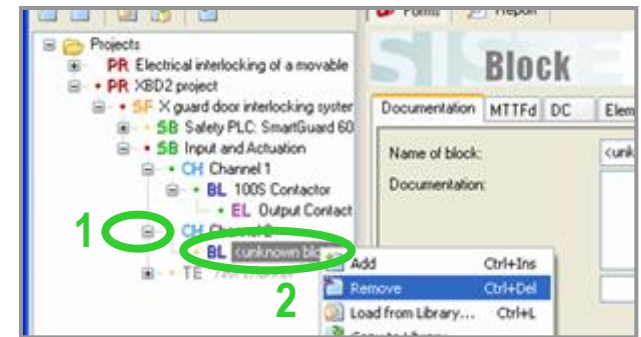


### Zadávání dat pro element stykače v kanálu 2

Před chvílí jste dokončili zadávání dat elementu stykače v kanálu 1.

Mohli bychom jít zpět o několik kroků a použít stejný proces pro druhý kanál. Jelikož pracujeme se SW a nikoliv manuálně, máme možnost použít rychlejší způsob:

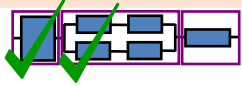
1. V hierarchickém stromu rozklikněte “**Channel 2**” až na úroveň bloků
2. Klikněte pravým tlačítkem na „BL <unknown block>“ a vyberte položku “remove” (pokud bude třeba potvrzení, potvrďte krok – v závislosti na nastavení)
3. Klikněte pravým tlačítkem na “BL 100S Contactor” pod “**Channel 1**” a vyberte “Copy”
4. Klikněte pravým tlačítkem “CH Channel 2” a vyberte “Paste”
5. Klikněte na “Save”





# SISTEMA

## KROK 2 Vytváření typického projektu



Data pro stykače jsou kompletní v obou kanálech

1. Žádná data nejsou vyplňována do “TE test channel”. Tento se používá pouze pro architektury druhé kategorie.
2. Data zadaná pro elementy stykače jsou poskytnuta blokům stykače a poté do vstupu a ovládání subsystému. Toto může být kontrolováno v panelu zobrazení sumárních dat.

Dalším krokem je zadání dat pro kanály spínače Trojan. Mohli bychom rovněž přidat Trojan na úrovni elementů, pro komplexnost prezentace však zkusíme vložit prvek jako blok.

**NEZAPOMEŇTE:** Stále musíme dokončit doplnění “Category” a “CCF” údajů. Odložíme ale tento krok na později a vložíme data na úrovni subsystémů, protože budou stejná pro všechny bloky vstupů a ovládání u celého subsystému.

The screenshot shows the SISTEMA software interface. The top menu bar includes File, Edit, View, and Help. Below the menu is a toolbar with icons for New, Open, Save, Close Project, Library, Print, and Help. The main window is divided into several panes. On the left, a tree view shows the project structure: Projects > PR Electrical interlocking of a movable > PR XBD2 project > SF X guard door interlocking system > SB Safety PLC: SmartGuard 60 > Input and Actuation > CH Channel 1 > BL 100S Contactor > EL Output Contact. A green circle labeled '1' highlights the 'TE Test channel' entry in the tree. Below the tree, there are three data entry panels. The first panel is for the 'X guard door interlocking system' with fields for PLr (d), PL (e), and PFH (1/h) (2.47E-8). The second panel is for 'Input and Actuation' with fields for PL (e), PFH (1/h) (2.47E-8), Kat. (3), MTTFd (a) (100 (High)), DCavg (%) (99 (High)), and DCF (0 (not fulfilled)). The third panel is for 'BL 100S Contactor' with fields for MTTFd (a) (2314.81 (-)), DC (%) (99 (High)), and EL (-). A green circle labeled '2' highlights the 'Input and Actuation' panel. On the right side of the interface, there is a 'Block' panel with fields for Name of block (100S Contactor), Documentation, and Document.

15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu



### Vytváření bloku Trojan

1. Vyberte “SB Input and Actuation”. Klikněte na záložku “PL” a ujistěte se, že je vybráno “Determine the PL/PFH from Category, MTTFd and DCavg”
  2. Klikněte na záložku “MTTFd” a ujistěte se, že je vybráno “Determine the MTTFd value from subblocks”
  3. Klikněte na záložku “DCavg” a ujistěte se, že je vybráno “Determine DCavg value from blocks”
  4. Klikněte na záložku “Blocks”.
- Poznámka:** Pokud vkládáte nejprve bloky z knihovny do subsystému: nejprve vyprázdňte výchozí “BL <unknown block>” – klikněte na něj pravým tlačítkem a vyberte “Remove” pro smazání.
5. V panelu „Channel 1“: klikněte na “Library” pro zobrazení dostupných bloků
  6. Klikněte na “Interlock Switch: Trojan 5” poté “Load Selection” pro přidání bloku do kanálu 1
  7. Rozklikněte “Channel 1” v hierarchickém stromu a vyberte nově přidáný blok „Trojan 5“

The screenshots show the following steps:

1. Selecting the 'SB Input and Actuation' block in the project tree, with the 'PL' tab active and 'Determine the PL/PFH from Category, MTTFd and DCavg' selected.
2. Switching to the 'MTTFd' tab and selecting 'Determine MTTFd value from subblocks'.
3. Switching to the 'DCavg' tab and selecting 'Determine DCavg value from blocks'.
4. Switching to the 'Blocks' tab.
5. Clicking the 'Library' button in the 'Channel 1' panel.
6. Selecting 'BL Interlock Switch: Trojan 5' in the library and clicking 'Load Selection'.
7. The 'BL Interlock Switch: Trojan 5' block is now listed in the 'Channel 1' panel.

15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu

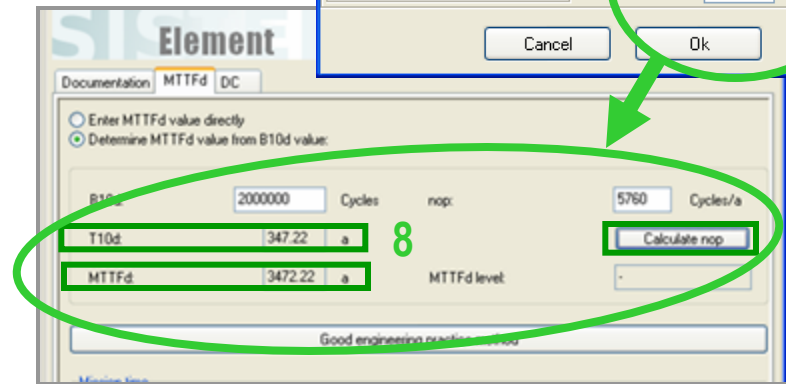
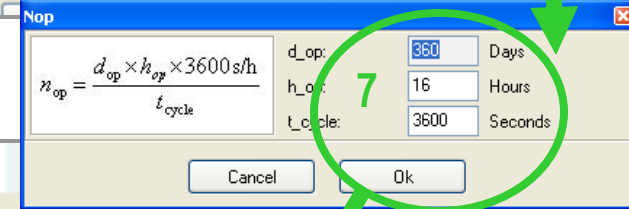
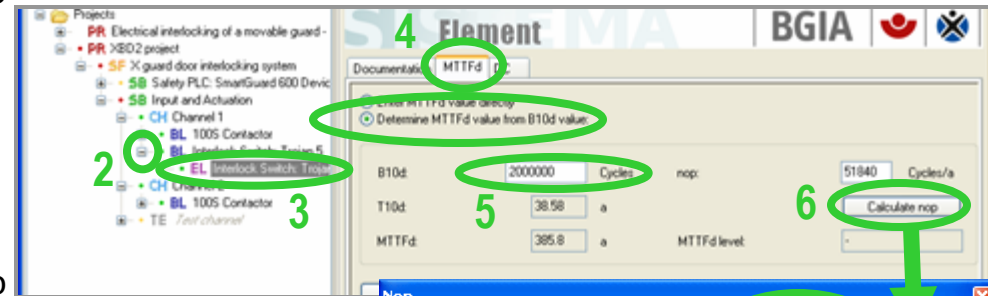
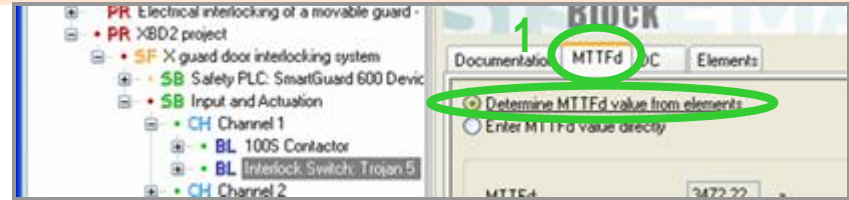


### Určení MTTFd z B10d pro Trojan 5

Stejně jako u stykačů, MTTFd Trojanu 5 je založena na jeho hodnotě B10d a počtu cyklů. Potřebujeme jít na úroveň elementů pro výpočet MTTFd z reálného použití.

1. Klikněte na záložku "MTTFd" a ujistěte se, že je vybráno "Determine the MTTFd value from elements"
2. Rozklikněte "BL Interlock Switch: Trojan 5" na úroveň elementů
3. Klikněte na "EL Interlock Switch: Trojan 5"
4. Klikněte na záložku "MTTFd" a ujistěte se, že je vybráno "Determine the MTTFd value from B10d value"
5. Trojan 5 B10d hodnota je 2000000
6. Klikněte na tlačítko "Calculate nop"
7. Zadejte 360 (days - dní), 16 (hours – hodin), 3600 (seconds - sekund) a klikněte na "OK"
8. Pole "Cycles/a", "T10d" a "MTTFd" budou přepočítány. – klikněte na "Save"

**DŮLEŽITÉ** – pro "Blocks" s hodnotou B10d (nahrané z knihovny) je výchozí hodnota 51840 pro počet operačních cyklů. Reálná hodnota musí být přepočítána přes tlačítko "Calculate nop" na úrovni elementů pro každou aplikaci.



15.10.2010



# SISTEMA

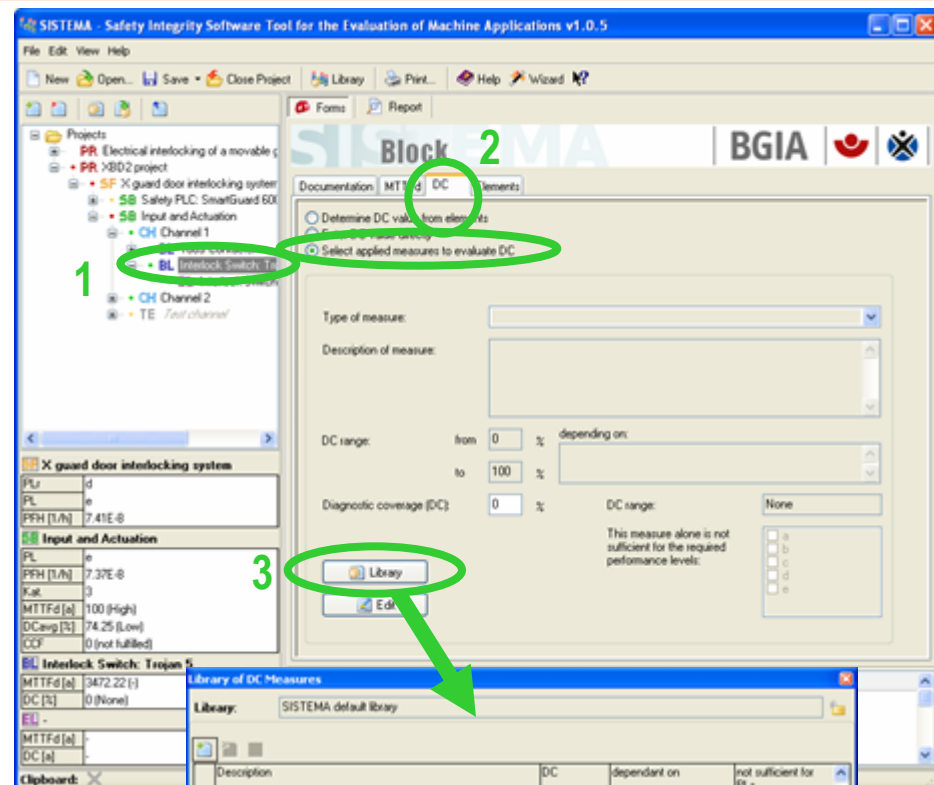
## KROK 2 Vytváření typického projektu



### Určení "DC" pro blok Trojan 5

Půjdeme zpět na úroveň bloků pro zadání "DC"

1. V hierarchickém stromu klikněte na "BL Interlock Switch: Trojan 5"
2. Klikněte na záložku "DC" a ujistěte se, že je vybráno "Select applied measures to evaluate DC"
3. Klikněte na "Library" pro otevření tabulky opatření
4. Posuňte se na "Input device" a vyberte "Direct monitoring (e.g. electrical position monitoring...)"
5. Klikněte na tlačítko "Load Selection" DC je nyní nastaveno na 99% (High-vysoké)
6. Klikněte na "Save"



Description	DC	dependant on	not sufficient for PLs
Input device			
Plausibility check, e.g. use of normally open and normally closed mechanical linked contacts	99	-	-
Cross monitoring of inputs without dynamic test	0-99	depending on how often a signal change is done by the application	-
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90	-	-
Cross monitoring of input signals and intermediate results within the 99 logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99	-	-
Indirect monitoring (e.g. position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99	Application	-
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99	-	-
Fault diagnosis (e.g. monitoring of sensor response time)	0-99	depending on the application	-
Monitoring some characteristics of the sensor (response time)	90	-	-

**DŮLEŽITÉ** výběr opatření pro Trojan 5 má vlivna architekturu kategorie 3, např. redundantní konfigurace s monitorováním, které je zajištěno bezpečnostním PLC SmartGuard. Ne-monitorovaný Trojan 5 (kategorie 1) by měl DC rovnou nule.



# SISTEMA

## KROK 2 Vytváření typického projektu



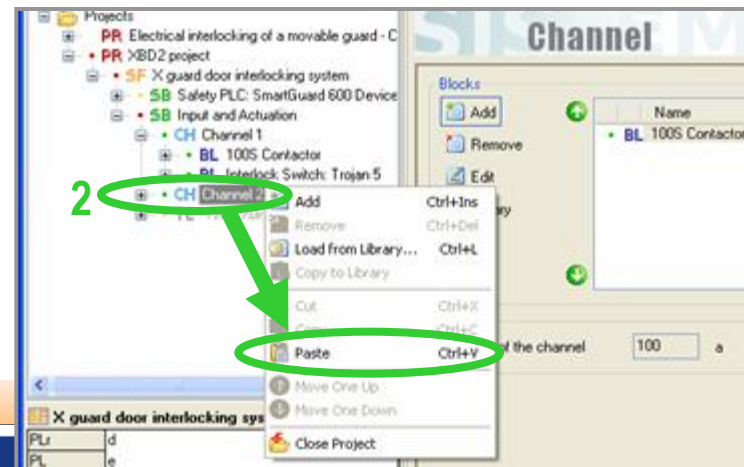
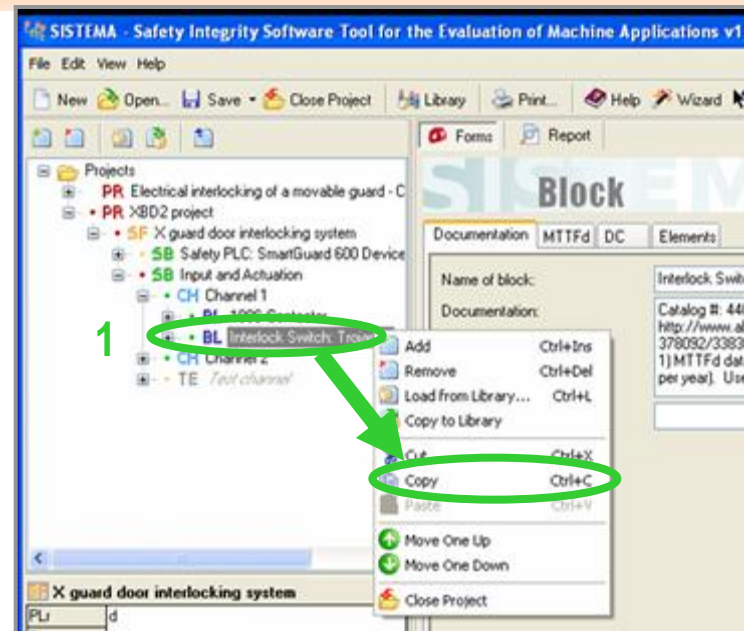
### Zadání dat bloku Trojanu 5 v kanálu 2

Právě jste dokončili zadávání dat blku Trojan 5 Block v kanále 1. Přestože se jedná o jeden spínač, má 2 oddělené elektrické kanály. Každý z nich musí být zadáván samostatně.

Protože jsou oba kanály identické, použijeme techniku “copy and paste”.

1. V hierarchické struktuře klikněte pravým tlačítkem na “BL Interlock switch: Trojan 5” v kanálu 1 a vyberte “Copy” – kopírování.
2. Klikněte pravým tlačítkem na “CH Channel 2” a vyberte “Paste” – vložit.
3. Klikněte na “Save”

**Poznámka:** Pokud kopírujete první blok do subsystému: vyprázdněte výchozí “BL <unknown block>”. Klikněte pravým tlačítkem na tuto položku a vyberte “Remove” pro smazání.

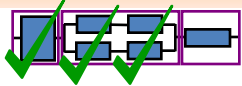


15.10.2010



# SISTEMA

## KROK 2 Vytváření typického projektu



Data Trojanu 5 jsou kompletní pro oba kanály

1. Žádná data nebyly zadávány do “TE test channel”. Toto je použitelné pouze pro architektury kategorie 2.
2. Data zadaná pro bloky Trojanu 5 jsou poskytnuta vstupům a ovládání subsystému. Toto může být zkontrolováno na panelu souhrnu dat.

Stále musíme dovyplnit “CCF” a “Category”. Uděláme to nyní na úrovni subsystému, protože data jsou stejná pro všechny bloky u vstupů i ovládání.

**1** TE Test channel

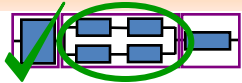
SF X guard door interlocking system	
PLr	d
PL	e
PFH [1/h]	2.47E-8
Input and Actuation	
PL	e
PFH [1/h]	2.47E-8
Kat.	3
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	0 (not fulfilled)
BL Interlock Switch: Trojan 5	
MTTFd [a]	3472.22 (-)
DC [%]	99 (High)
EL	-
MTTFd [a]	-
DC [a]	-

Clipboard: BL



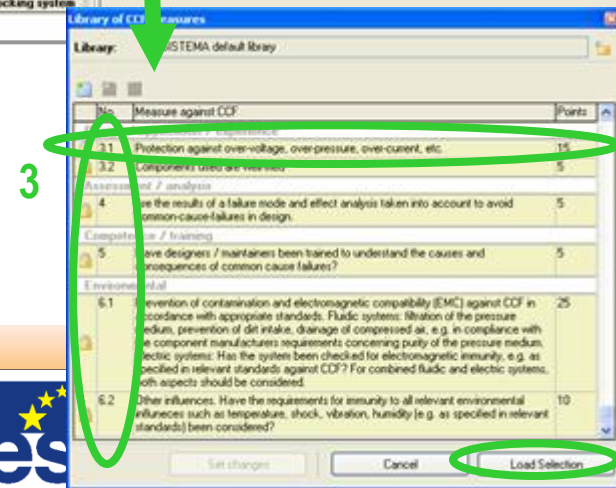
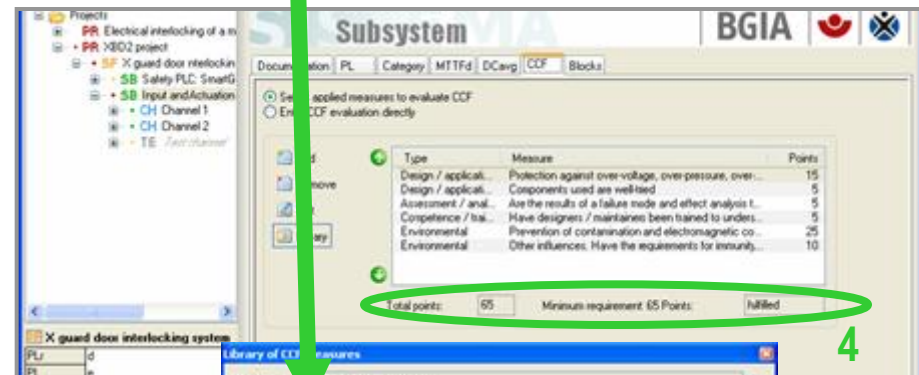
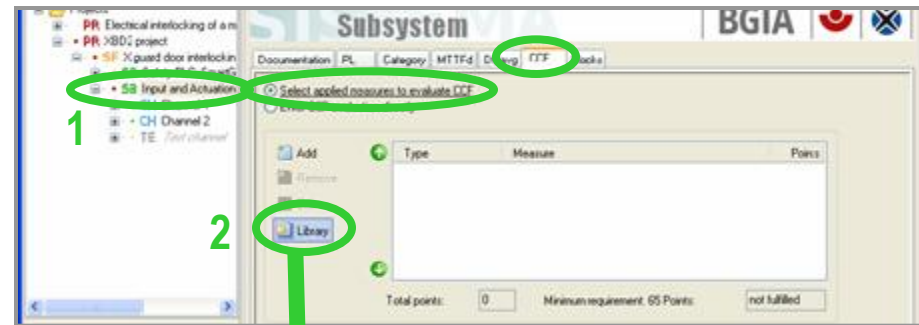
# SISTEMA

## KROK 2 Vytváření typického projektu



### Zadávání CCF dat vstupů a ovládání

1. Klikněte na “SB Input and Actuation”.  
Klikněte na záložku “CCF” a ujistěte se, že je vybráno “Select applied measures to evaluate CCF”
2. Klikněte na tlačítko “Library” pro zobrazení tabulky dostupných opatření
3. Každé opatření musí být vybráno a nahráno individuálně. Nahrajte opatření 3.1, 3.2, 4, 5, 6.1, 6.2.
4. Součet bodů aplikovaných opatření musí být minimálně v hodnotě 65, aby byl splněn status “fulfilled” - splněno

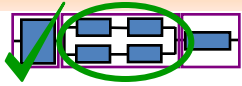






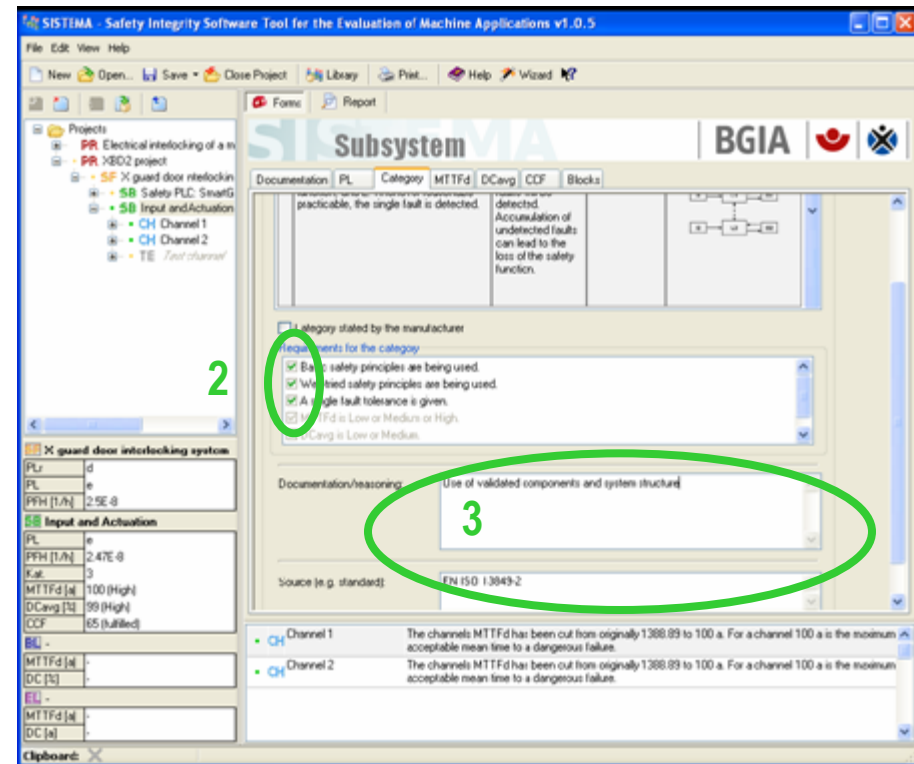
# SISTEMA

## KROK 2 Vytváření typického projektu



### Zadávání informací o kategorii vstupů a ovládání

1. Vyberte "SB Input and Actuation". Klikněte na záložku "Category"
  2. Zkontrolujte zatržení požadovaných políček k potvrzení, že byly splněny požadavky příslušné kategorie.
  3. Odůvodnění spojené s deklarací kategorie může být uvedeno do polí "Documentation" and „Source". SISTEMA by bez vyplnění polí byla schopna vypracovat report, nicméně dříve či později byste informace museli doplnit pro zkompletování dokumentace stroje.
- Indikační bod pro vstupní a ovládací subsystém změnil barvu na zelenou. Všechny data jsme tedy zadali správně.

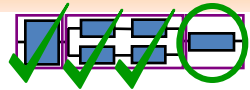


Nyní musíme dokončit celý subsystém



# SISTEMA

## KROK 2 Vytváření typického projektu



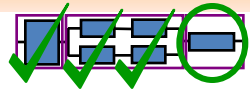
### Vytváření mechanické části subsystému Trojanu 5 - vysvětlení

- Dokumenty pro Trojan 5 vysvětlují, že je použito vyloučení chyby pro některé body jejichž porucha může způsobit poruchu celého zařízení. Tato konstrukce je použita u většiny elektromechanických komponentů, jako např. tlačítka E-Stop, koncové spínače, jazýčkové spínače apod.
- Trojan 5 má dva elektrické kanály a může být použit jako součást zapojení kategorie 3 pro dosažení **PLd** pokud může být uvedeno příslušné vyloučení chyby mechanických vazeb jako nebezpečných bodů zařízení. Pokud jsou podmínky použití Trojanu 5 v rámci daných hranic, vyloučení chyby může být vyžadováno.
- Pro **PLe** bude obvykle nutné pro splnění požadavků použít technologii, která vyloučí možnost použití zařízení s jedním nebezpečným místem, jako například některé typy bezkontaktních dveřních spínačů. Alternativně může být použito dvojice oddělených zařízení pro dvojici kanálů.
- Mechanické vedení může být považováno za část struktury kategorie 3, protože jsme použili vyloučení chyby. Bude přidáno jako separátní subsystém, protože má jinou strukturu, než ostatní subsystémy. Porot můžeme použít kategorii 3, ale pouze ve spojení s vyloučením chyby.
- **Subsystém s vyloučením chyby nemá vliv na výpočty, jeho zmínění v projektu však zaručí zmínku o něm v reportu, na základě kterých mohou být přijaty odpovídající opatření (častější kontroly).**
- Tento subsystém označíme jako „Mechanical FT 0: Trojan 5”



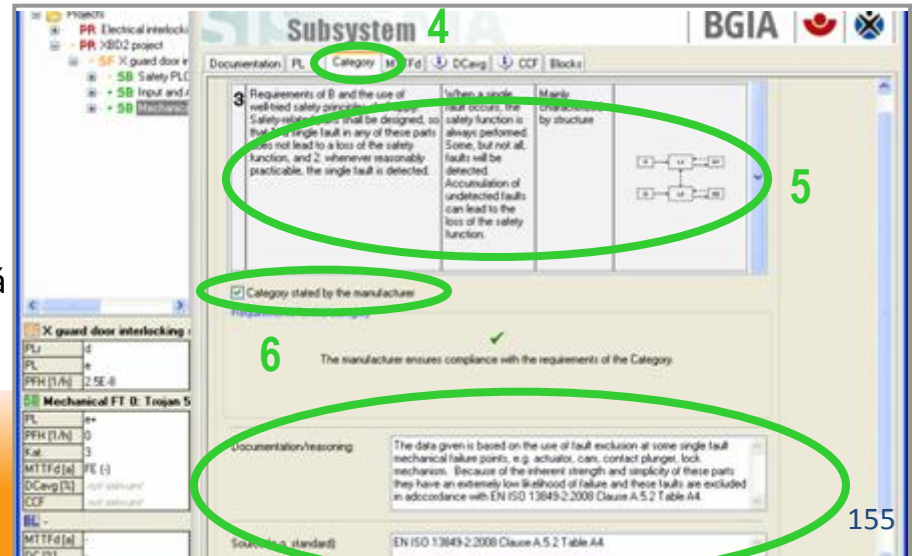
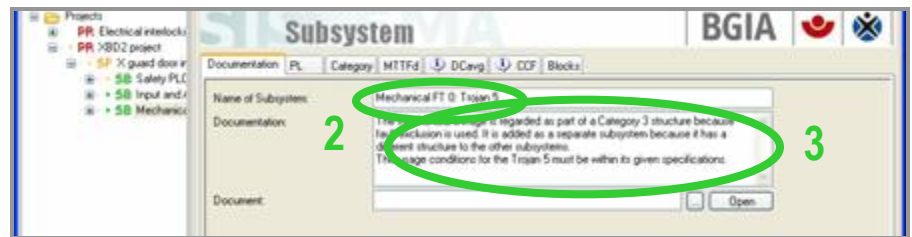
# SISTEMA

## KROK 2 Vytváření typického projektu



### Vytváření subsystému “Mechanical FT 0”

1. Klikněte pravým tlačítkem na “SF X guard door” a vyberte “Add” pro vytvoření nového subsystému.
2. Jméno subsystému nastavte “Mechanical FT 0: Trojan 5”.
3. Jakákoliv relevantní informace pro použití vyloučení chyby by měla být uvedena v poli “Documentation”.  
Např.: “Mechanická vazba je považována jako část struktury 3. kategorie, protože je použito vyloučení chyby. Je přidáno jako oddělený subsystém, protože má rozdílnou strukturu vzhledem k ostatním subsystémům.” – Použití je možné za podmínek splnění specifikací Trojany 5.  
V záložce PL budou již zaškrtnuty políčka „Determine PL/PFH from Category, MTTFd and DCavg”
4. Klikněte na záložku “Category” pro zobrazení okna kategorií
5. Najděte a vyberte kategorii 3
6. Zkontrolujte zatržení “Category stated by the manufacturer”. Výrobce prohlašuje, že podmíněně vyloučení chyby může být použito, které dovoluje použití jako část architektury kategorie 3 v systémech s PLd. Odpovídající informace o Trojany 5 obsažená v knihovně může být zkopírována z knihovny do pole “Documentation”.



15.10.2010

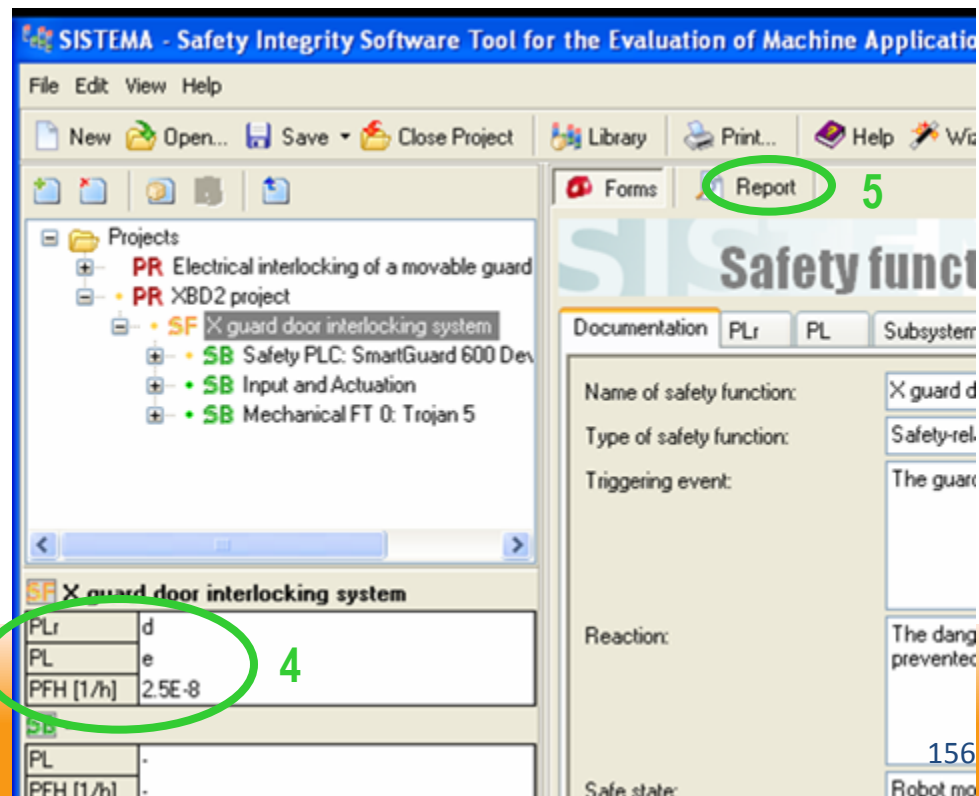
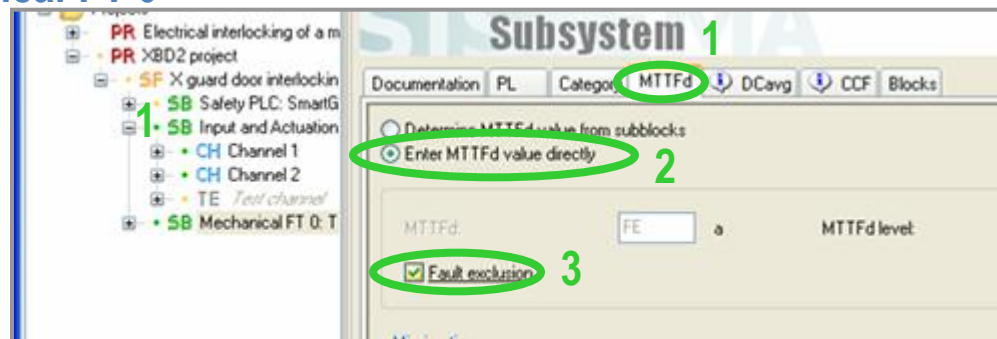


# SISTEMA

## KROK 2 Vytváření typického projektu

### Vytváření subsystému "Mechanical FT 0"

1. Klikněte na záložku "MTTFd"
2. Ujistěte se, že je vybráno "Enter MTTFd value directly"
3. Zatrhněte políčko "Fault Exclusion"
4. Právě jste dokončili zadávání dat do SW SISTEMA. U bezpečnostní funkce bylo dosaženo PLe s PFH  $2,5 \times 10^{-8}$
5. Klikněte na "Report" pro generování koncové zprávy (reportu).





# SISTEMA

## KROK 2 Vytváření typického projektu

### Report - Zpráva

**SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications v1.0.5**

File Edit View Help

New Open... Save Close Project Library Print... Help Wizard

Forms Report

**SISTEMA - Sicherheit von Steuerungen an Maschinen**  
Report of project: "XBD2 project"

Report date: 01.05/2009  
File date: 01.05/2009

**BGIA** Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

**PROJECT STATUS**

Status: yellow

Note: There are warnings with yellow status listed for this project (or it's subordinate basic elements). Please consider these hints.

**OVERVIEW**

**PR Projectname:XBD2 project**  
Machine: X robot access gate - Also other hazard points liste SISTEMA version: 1.0.5  
Author: D Jones Standard version: ISO 13849-1:2006, ISO 13849-2  
Safetyfunctions:

**SF Name:Xguard door interlockingsystem**  
Type: Safety-related stop function initiated by safeguard  
PL: e PFH [1/h]: 2.5E-8  
PLr: d  
Subsystems:

**SB Name:Safety PLC: SmartGuard 600 Devicelet**  
PL: e+ PFH [1/h]: 3.89E-10  
DCavg [%]: not relevant MTTFd [a]: not relevant  
CCF Points: not relevant Category: 4

**SB Name:Input and Actuation**

Page 1 of 29 Zoom: 90%

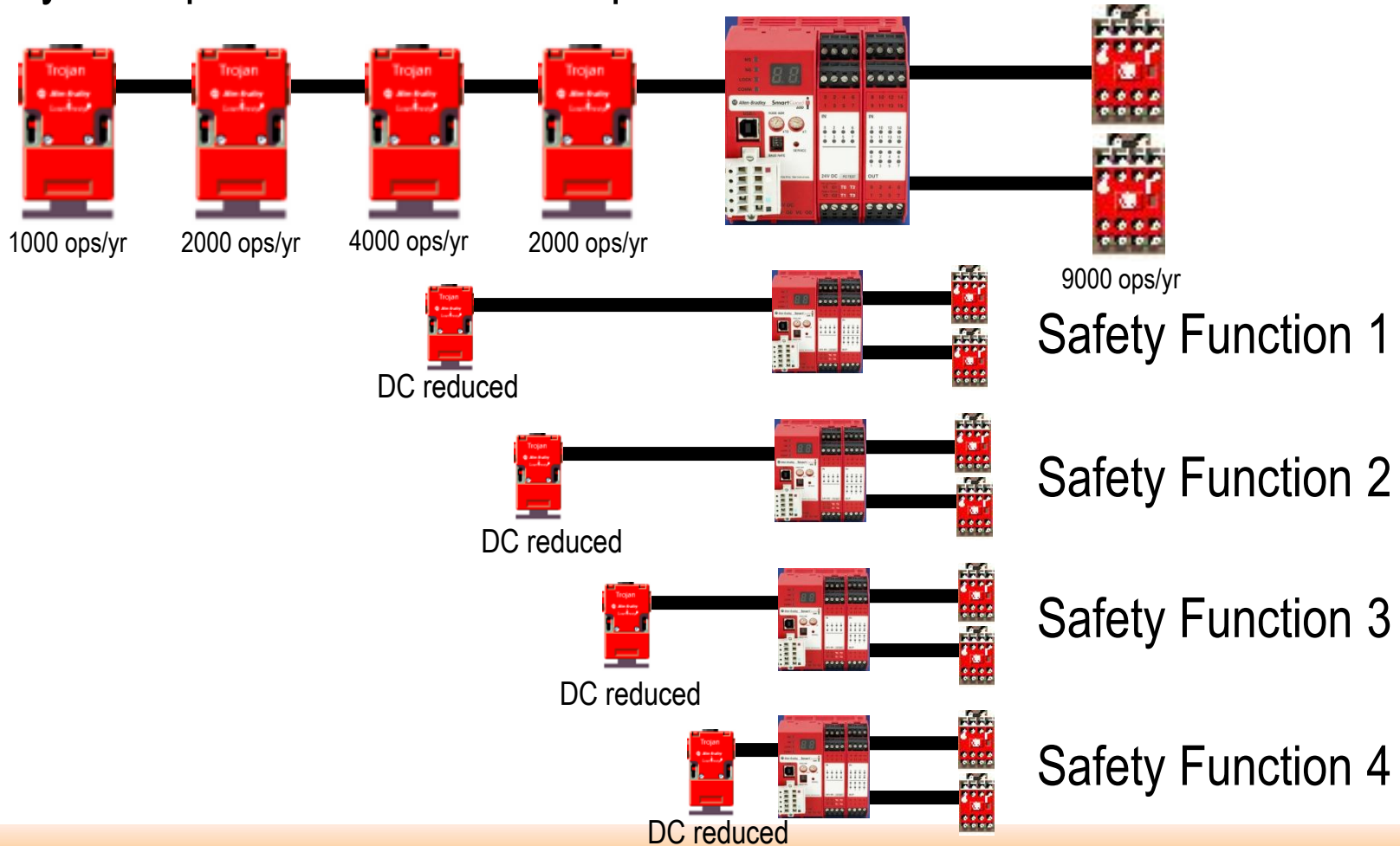
Clipboard: X

15.10.2010



# Práce s rozdílnými architekturami

Jak byste uspořádali architekturu pro SISTEMU?



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Práce s rozdílnými architekturami

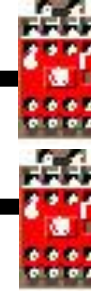
Jak byste uspořádali architekturu pro SYSTEMU?



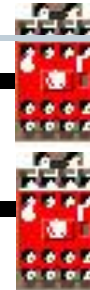
**TLS**  
Guard locking  
Interlocking Switch



**SmartGuard**  
Safety Controller



**100S**  
Safety Contactors



Safety Function 1  
Prevention of unexpected start-up



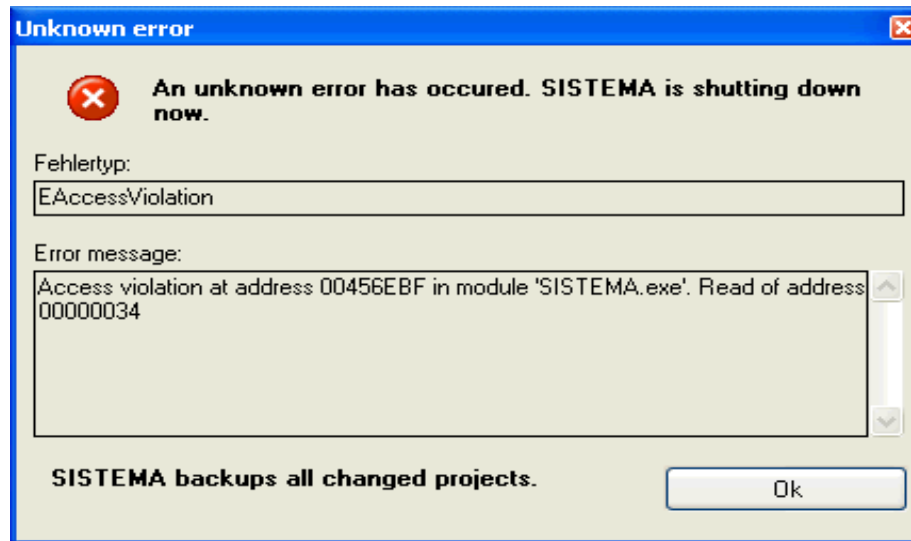
Safety Function 2  
Guard locking

15.10.2010



- **Q: SISTEMA způsobí občas nestabilitu systému, je nějaký způsob, jak vyřešit problém?**

- A: Anglická verze SW má někdy problémy s přístupem do knihoven opatření CCF nebo opatření DC. Toto je způsobeno vadou v překladu SW, nikoliv knihoven samotných. Chyba se vyskytuje dnes již v zastaralé verzi SW (nižší než verze 1.1 z července 2009). Pro vyřešení problému si stáhněte novou verzi.







- Q: Proč mají některé prvky v knihovně produktů RA označení „PLe+” ohodnocení?
  - A: Když hodnota PFH subsystému překročí PLe (např. je méně než  $10^{-8}$ , která je nutná pro požadavky PLe), SISTEMA označí subsystém hodnocením „PLe+”

The screenshot shows the SISTEMA software interface. At the top, there is a navigation bar with the following tabs: Documentation, PL (selected), Category, MTTFd, DCavg, CCF, and Blocks. Below the navigation bar, there are two radio buttons for determining PL/PFH: "Enter PL/PFH directly (refer also to Category tab)" (selected) and "Determine PL/PFH from Category, MTTFd and DCavg". The main form area contains the following fields:

- Performance Level (PL): A dropdown menu showing "e+" (circled in blue).
- PFH [1/h]: A text input field containing "3.89E-10".
- Documentation/reasoning: A large text area for entering details.



# FAQ

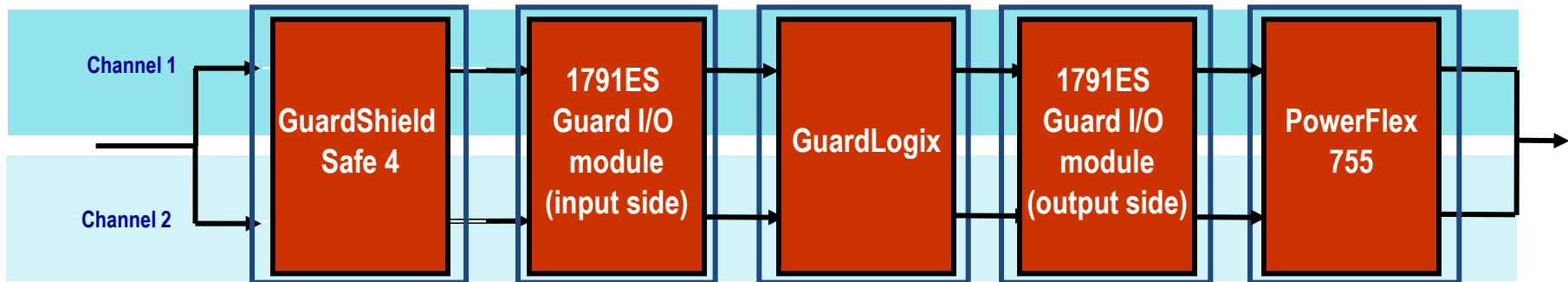
- **Q: Když nahrávám některé subsystemy z knihoven, obdržím varování, že subsystemy mají kratší dobu použití (mission time), než typických 20 let. Je to důvod k obavám?**
  - A: Ne. Mission time nebo „proof test interval“ je teoretická hodnota času, po kterou může být subsystem používán, po jejímž uplynutí musí být vyměněn. Většina subsystemů v knihovnách má Mission time 20 let a více, u výrobců se však vyskytují výrobky s nižším MT. Neměňte hodnotu z té, kterou jste nahráli z knihovny. Podle hodnoty (i když je nízká) byly výrobky certifikovány.

For the designated architectures a typical mission time of 20 years is assumed. This block has a mission time of 10 years (see register MTTFd), which falls below this value. Please assure to change this block in time.



## • Q: Jak bych zadal do **SISTEMY** vzdálené bezpečnostní I/O na sběrnici?

- A: Řešením je rozdělit systém až na jádro bezpečné informace, jak je zobrazeno na obrázku. Uvědomte si, že vzdálené I/O a bezpečnostní PLC musí být do **SISTEMY** nahrány jako 2 separátní subsystémy s přihlédnutím na k PFHd na straně vstupů, stejně jako na straně výstupů.



Příklad bezpečnostní funkce implementované s bezpečnostním systémem GuardLogix (povšimněte si, že vzdálené moduly 1791ES Guard I/O jsou na straně vstupů i výstupů).



# FAQ

- **Q: Je SISTEMA omezená počtem subsystémů, které mohou obsluhovat jednu bezpečnostní funkci?**
  - A: Ne, hranice jsou závislé pouze na parametrech počítače.



Mgr. Karel Stibor

# SNÍMÁNÍ PŘÍTOMNOSTI OSOB

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Důvody

Tato funkce je důležitá všude tam, kde musíme vyloučit přítomnost osob v době běhu strojního zařízení.

Méně častou aplikací bývá přítomnost obsluhy právě na některém z míst (u ovládacího pultu apod.), bez které stroj nebude pracovat.

Jako u většiny bezpečnostních funkcí máme k dispozici na výběr elektrické nebo elektromechanické zařízení.

Zařízení elektrická:

- světelné bariéry
- laserové scannery
- 3Dkamery

Zařízení elektromechanická:

- bezpečnostní hrany
- nášlapné rohože



# Normy pro optické bariéry

Je záležitostí výrobce, aby zaručil splnění norem EN IEC 61496-1 a -2 pro evropské prostředí a UL 1998 pro Severní Ameriku

Rovněž musí být certifikovány dle norem EN IEC 61496 a EN 954-1, EN 61508 nebo dle EN ISO 13849-1 a zatříděna do bezpečnostní kategorie, SIL nebo PL.

Optické závory (či bariéry) svou konstrukcí mohou splňovat podmínky 2. nebo 4. kategorie (PLd/PLe, SIL 2/3).

Laserový scanner může díky své konstrukci požadavky 3.kategorie, PLd nebo SIL2



# Jak vytipovat vhodnou světelnou závoru ?

Špatně umístěné závory jsou u 84% případů aplikací a to včetně nových strojů a zařízení!!!

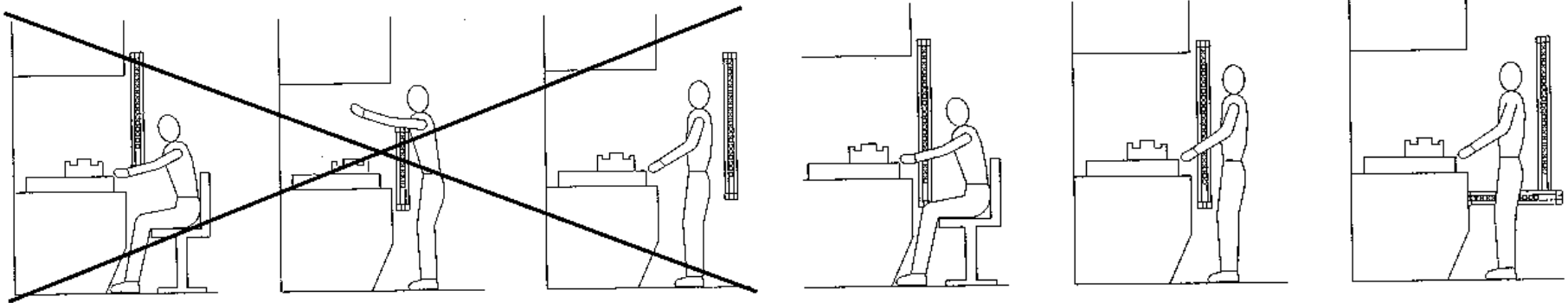
**Správně umístěná závora může ušetřit velikou část nákladů!**

- 1) Rozlišení                    14mm ochrana prstů  
                                      30mm ochrana ruky  
                                      1, 2, 3 paprskové pro ochranu těla, kontrolu přístupu atd.
- 2) Kategorie                    TYP 2 pro aplikace kategorie 2 / SIL 1  
                                      TYP 4 pro aplikace kategorie 3,4 / SIL 3
- 3) Hlídaná výška                min. 160mm, max.1910mm
- 4) Potřebná rozteč            max. 70m
- 5) Speciální funkce            Muting (řízené odpojení závory)  
                                      Blanking (řízené zaslepení jednoho/více paprsků)
- 6) Připojení                    Délka připojovacího vodiče





# Kam umístit světelnou závoru ?



$$S = K(t_1 + t_2 + t_3) + C$$

<b>S</b>	<i>Minimální bezpečná vzdálenost</i>	mm
<b>K</b>	<i>Rychlost přibližování obsluhy k nebezpečnému místu</i>	mm/sec
<b>t<sub>1</sub></b>	<i>Reakční doba světelné závory v sekundách</i>	sec
<b>t<sub>2</sub></b>	<i>Reakční doba bezpečnostního vyhodnocovacího přístroje v sekundách (např. PLC nebo bezpečnostní modul)</i>	sec
<b>t<sub>3</sub></b>	<i>Reakční doba stroje v sekundách, tzn. čas, který stroj potřebuje k přerušení nebezpečného pohybu od okamžiku převzetí signálu k zastavení od vyhodnocovacího přístroje</i>	sec
<b>C</b>	<i>Přídavná vzdálenost</i>	mm



# Podmínky použití



Bezpečnostní systém smí být použit pouze jako odpínací zařízení a ne jako povelový přístroj.



Pohyblivá část stroje lze elektricky ovládat.



Jakýkoli pohyb uvádějící stroj do pohybu je možné okamžitě přerušit. Obzvláště musí být znám čas do zastavení stroje: eventuálně je nutné ho změřit!



Stroj nevytváří nebezpečné situace na základě vyhazování nebo padání předmětů. V opačném případě je nutné zavést přídatná mechanická opatření – kryty.



Minimální zjišťovaná velikost objektu musí být stejná nebo větší než rozlišení určitého modelu optické bariéry.



Chraňte vysílač i přijímač před zdroji světla, jejichž intenzita osvětlení by mohla překročit odolnost vůči falešnému světlu.



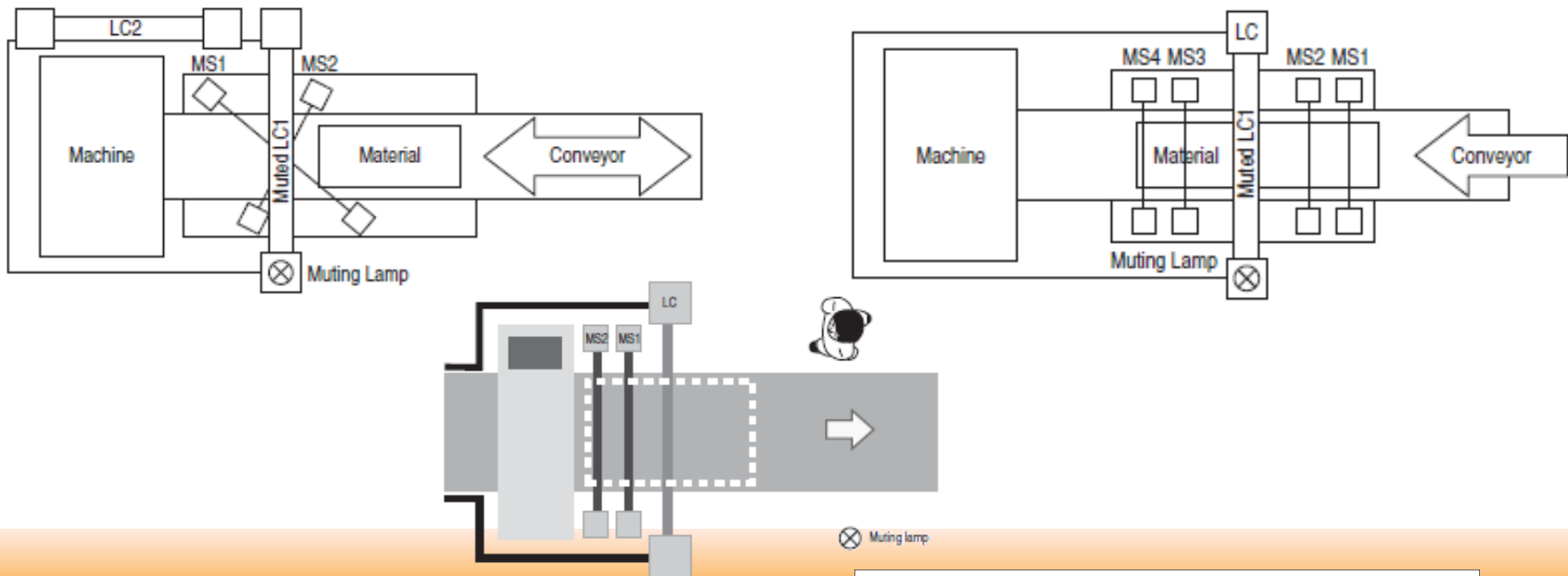
# Speciální druhy provozu - Muting

Muting je řízené, dočasné odpojení vyhodnocování funkce světelné závory.

Muting se používá tam, kde chceme nechat vstoupit polotovary či vystoupit výrobky z nebezpečného procesu a přitom nechceme dovolit vstoupit obsluze či jiné osobě.

Pokud vstoupí do ochranného pole osoba, optická závora vypne nebezpečný pohyb.

Existují 3 typy funkce muting. 2T-obousměrný, 4T-jednosměrný a 2L jednosměrný.



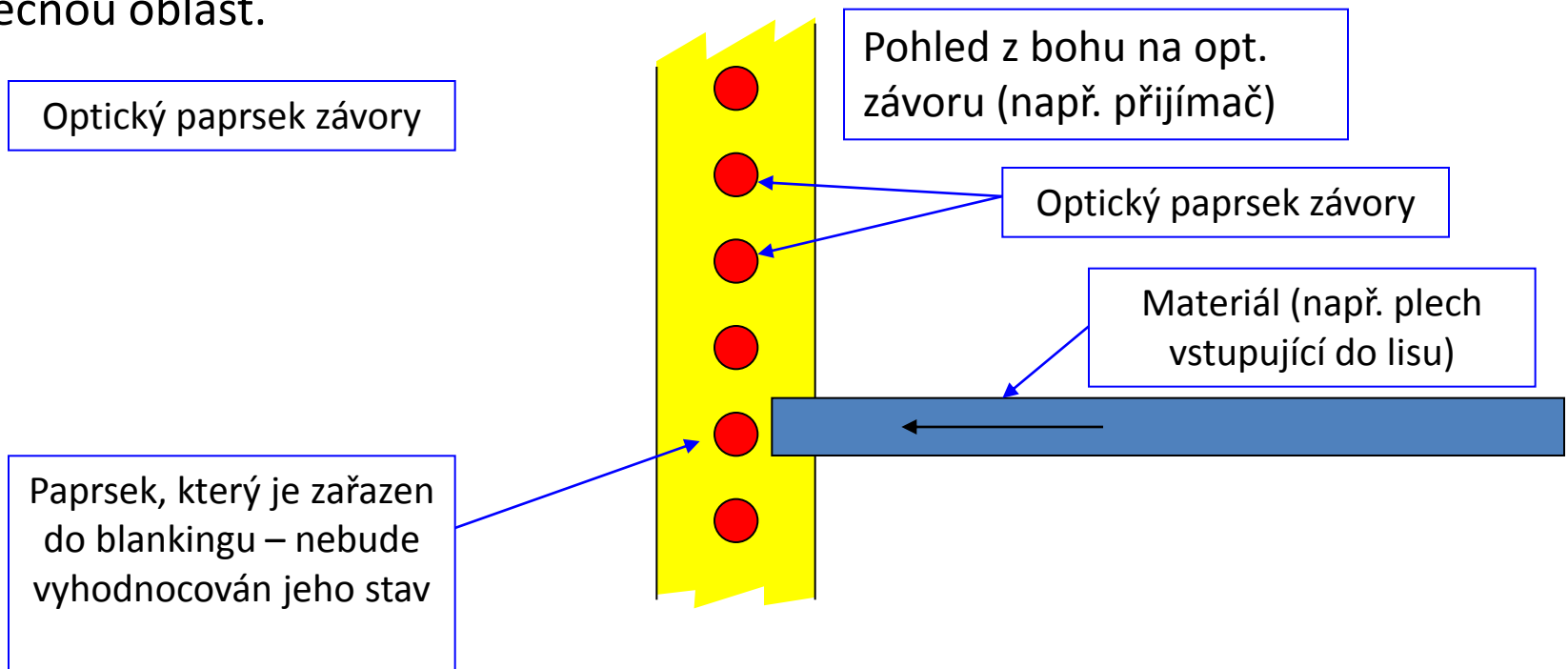
15.10.2010



# Speciální druhy provozu - Blanking

Blanking je řízené, trvalé odpojení vyhodnocování jednoho z optických paprsků světelné závory.

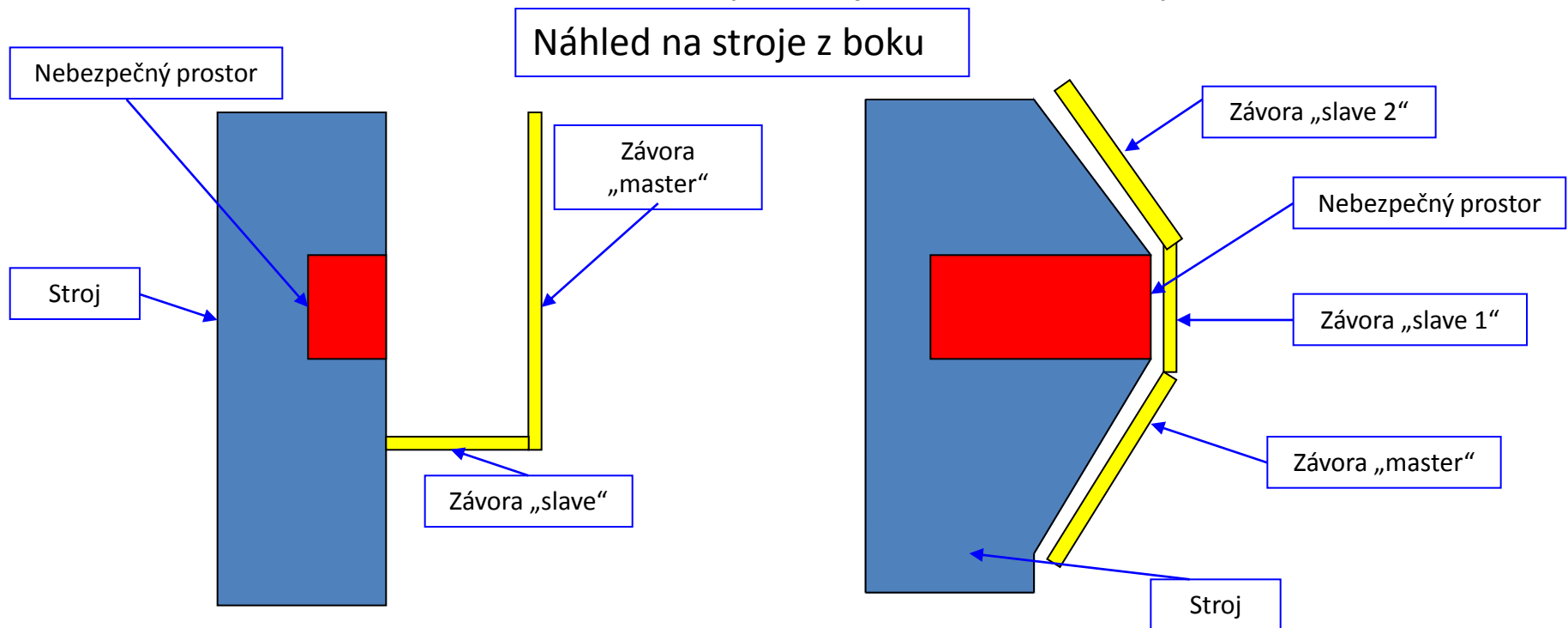
Blanking se používá tam, kde chceme nechat vstoupit či vystoupit materiál z nebezpečného procesu a přitom nechceme dovolit obsluze dosáhnout na nebezpečnou oblast.





# Speciální druhy provozu - Kaskádování

Kaskádování je zapojení optických závor do sekvencí, které má za cíl například kopírovat složité tvary stroje, zabezpečení složitých prostor a podobně. Jeho výhodou je zapojení zapojených závor ja jeden vstup bezpečnostní logiky, nevýhodou je většinou delší reakční doba celé kaskády (sčítají se reakční doby všech závor).



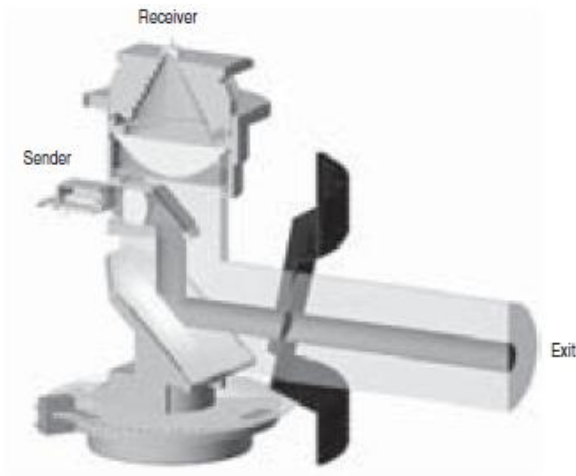
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

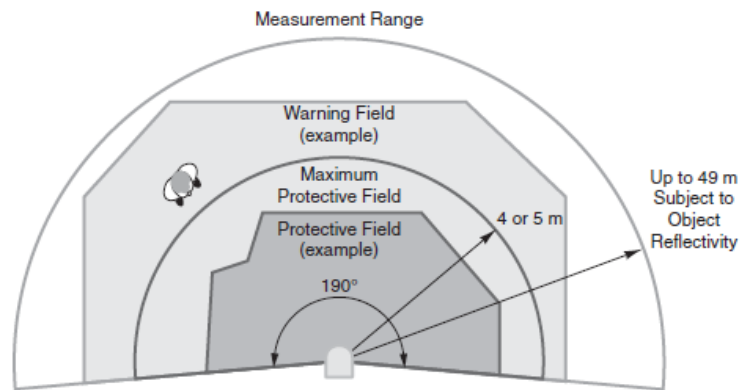
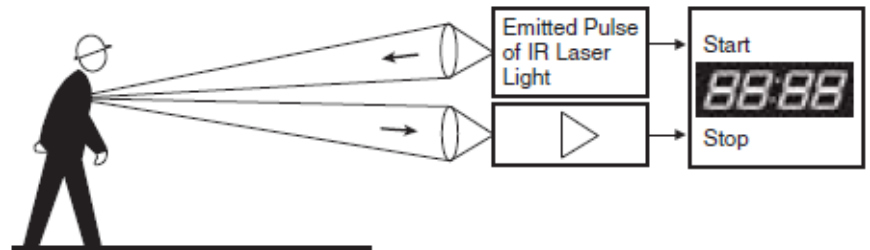




# Laserové scannery



- Sender Path
- Receiver Path



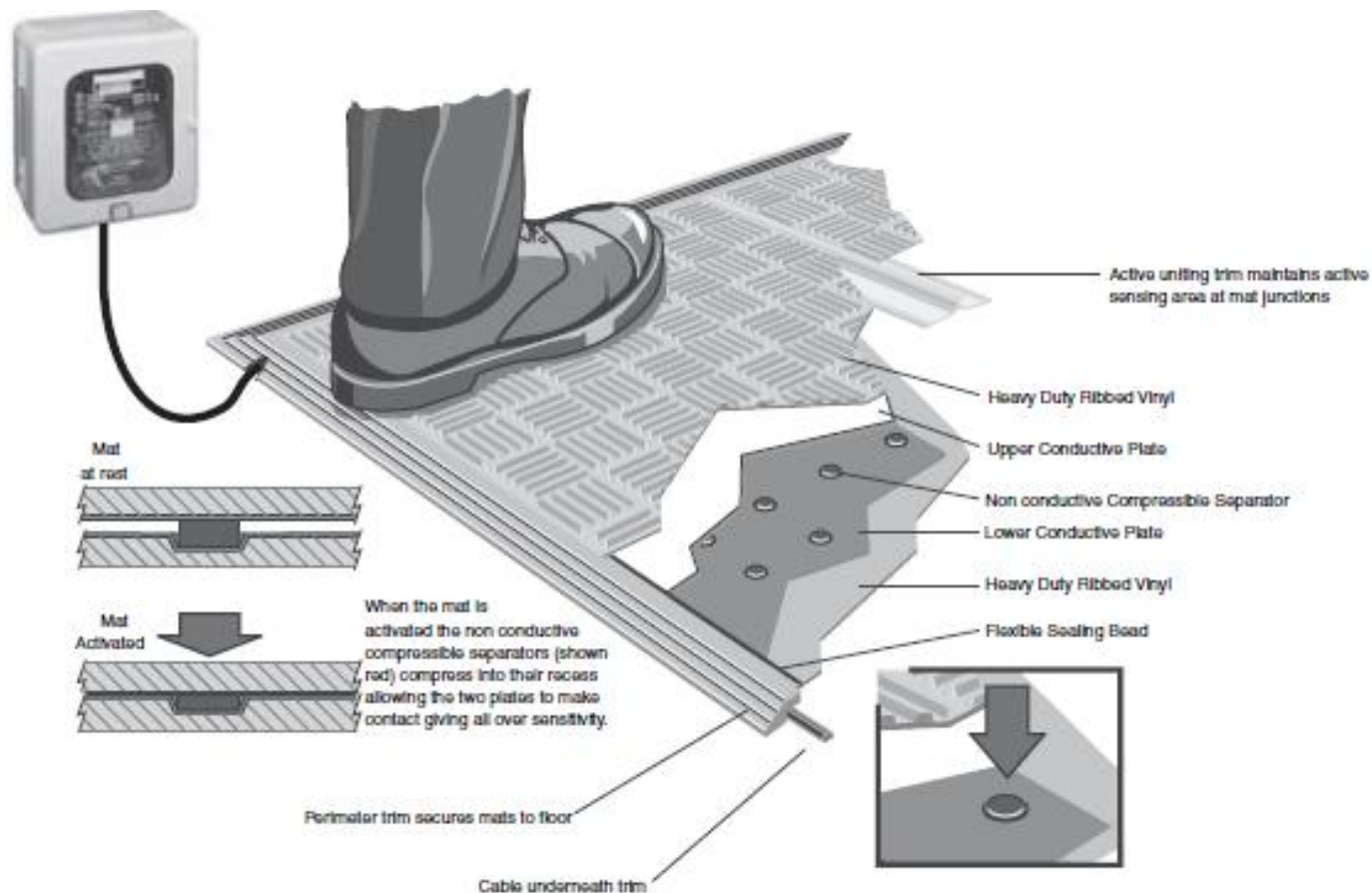
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Nášlapné rohože



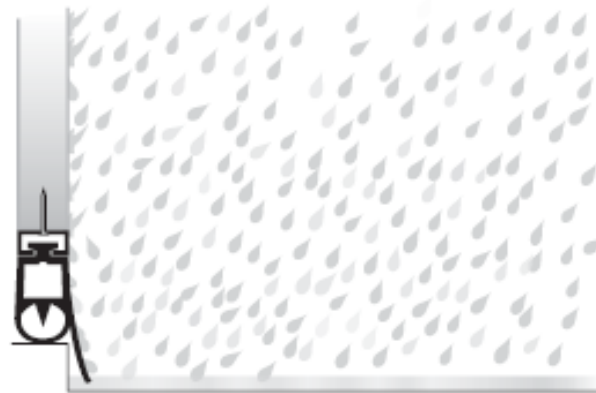
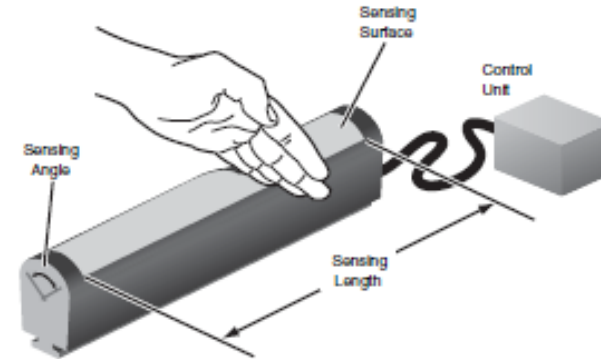
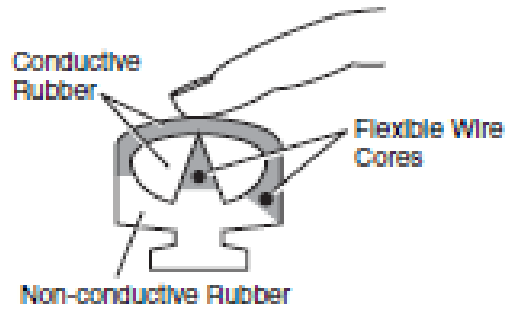
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Bezpečnostní hrany



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ







Mgr. Karel Stibor

# BEZPEČNOSTNÍ KRYTY

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Podmínky

Podmínky aplikace bezpečnostních krytů se řídí normou EN 1088.

Základní dělení krytů je na kryty pevné a pohyblivé. Kryty pevné musí být uchyceny tak, aby nešly snadno odejmout. Kryty pohyblivé se dělí na kryty s blokováním a bez blokování. Kryty pohyblivé musí být monitorovány, popřípadě zajištěny. Monitorování či zajišťování probíhá pomocí elektronických nebo elektromechanických komponent.

Blokování krytu může být pomocí pružiny, motoricky, elektromagnetem či jinou silou přímým silovým působením. Každopádně při otevřeném krytu je třeba, aby byl znemožněn nebezpečný provoz stroje (za určitých podmínek je možno stroj provozovat za snížené rychlosti).

Čidla snímající polohu krytu musí být upevněna spolehlivě, jejich uvolnění musí vždy vyžadovat nářadí, omezení drážek musí být omezeno na prvotní seřízení, po prvotním seřízení musí být poloha aretována tak, aby výměna čidla mohla být provedena bez nutnosti seřízení. Další mechanické požadavky naleznete v článku 5 normy EN 1088.



# Podmínky

Musí být minimalizována možnost vyřazení monitorovacího / blokovacího zařízení.

Veškerá elektrická instalace musí být v souladu s normou EN 60204-1.



# Typy

Monitorování krytů může splňovat všechny typy kategorií a SIL.

Princip snímání polohy je běžný na principu:

- magnetickém (jednoduché pro překonání)
- magnetickém s kódováním (obtížnější, ne nemožné, většinou speciální logika)  
RFID (téměř nemožné překonat, ne všichni výrobci nabízí ve spojení s blokováním)
- elektromechanické (cenově výhodné, nejjednodušší k překonání, nejvyšší přídržná síla aktuátoru+spínače, nevýhoda použití pro nejnebezpečnější provozy)



Mgr. Karel Stibor

# LOGICKÉ PRVKY BEZPEČNOSTNÍCH OBVODŮ

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Podmínky

Logické prvky musí splňovat podmínky použití alespoň jedné z možností:

- |                               |                        |
|-------------------------------|------------------------|
| - EN 954-1                    | bezpečnostní kategorie |
| - EN ISO 13849-1 (+ EN 62061) | Performance Level      |
| - EN 61508                    | Safety Integrity Level |

Logické prvky se dělí dle možností na:

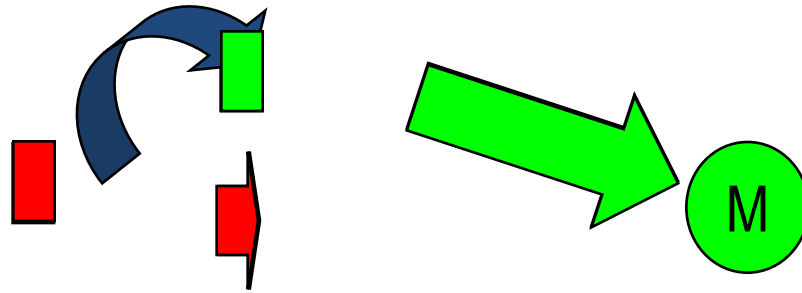
- diskrétní bezpečnostní moduly (někdy označovaná za bezpečnostní relé)
- bezpečnostní PLC (ať už s bezpečnostní sběrnicí, nebo bez)
- bezpečnostní integrované systémy



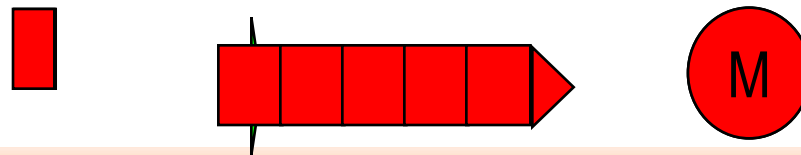
# High availability X safety

- Základním pravidlem rozhodování je stav zjištění CHYBY systému (nikoliv např. tlačítko nouzového zastavení, ale např. přerušení vodiče k němu)

HIGH AVIABILITY (též Fault tolerant systémy) přepnou řízení na druhou větev – jsou na tuto činnost určeny – aby se pokud možno předešlo zastavení výroby.



SAFETY systémy uvedou při detekci chyby celý systém do bezpečného stavu – dle vypínací sekvence se snaží co nejdříve dosáhnout stavu se všemi výstupy v logické 0 – bez výjimky následuje zastavení části výroby (stroje a strojní zařízení)





# Cíl bezpečnostní logiky

- 1) Číst informace / monitorování z bezpečnostních vstupních zařízení (tlačítka, rohože, opt. závory, zpětná vazba atd.)
- 2) Tyto získané informace zaručeně a spolehlivě vyhodnotit dle vzorových scénářů
- 3) Na základě vzorových scénářů reagovat pomocí ovládacích prvků (aktuátorů). V některých případech může být vyžadováno monitorování skutečného stavu aktuátorů.





# Bezpečnostní moduly

- V minulosti (do roku 1986) se používaly pouze stykačové kombinace a to pouze u strojů, které konstruktérům připadaly nebezpečné. V roce 1986 byl na trh uveden první bezpečnostní modul určený pro nouzové zastavení. Finančně tento prvek nebyl vůbec výhodný, ušetřil ale dramaticky místo v rozvaděči (namísto 4 stykačů postačilo zapojit 1 modul o šířce 80mm).
- + finanční výhodnost u malých aplikací, není potřeba hlubších znalostí, jednoduchost údržby, ...
  - finanční náročnost u velkých aplikací, jednoduchost nedovoleného překonání, ...



# Bezpečnostní PLC

- První bezpečnostní PLC certifikováno v roce 1996. Vyvinuto na základech programovací řeči S5, nicméně se nejednalo o Simatic. V minulosti byly problémy s použitím bezpečnostního PLC kvůli nepružnosti normy EN 954-1. Vlivem finanční náročnosti „velkých“ systémů dochází k postupnému přechodu výrobců do oblasti malých systémů.
- + finanční výhodnost u středních aplikací, možnost tvoření designu „za běhu“, výhodnost použití pro modulární použití, pro většinu „nezasvěcených“ se jedná o černou krabičku, do které se bojí zasahovat
  - pro údržbu a diagnostiku je třeba SW a odborného pracovníka,



# Bezpečnostní integrované systémy

Bezpečnostní integrované systémy spojují výhody bezpečnostních PLC a klasických systémů. Na trhu se začaly objevovat na přelomu tisíciletí. Jsou nejpokročilejším, co současná technika nabízí.

- + možnost integrovat nejen standardní a bezpečnostní řízení, ale i polohování a pohony, možnost použít decentrální architekturu, integrace do programovacího prostředí, čím více funkcí a větším množstvím integrují, tím cenově výhodnější
- pro údržbu a diagnostiku je třeba SW a odborného pracovníka



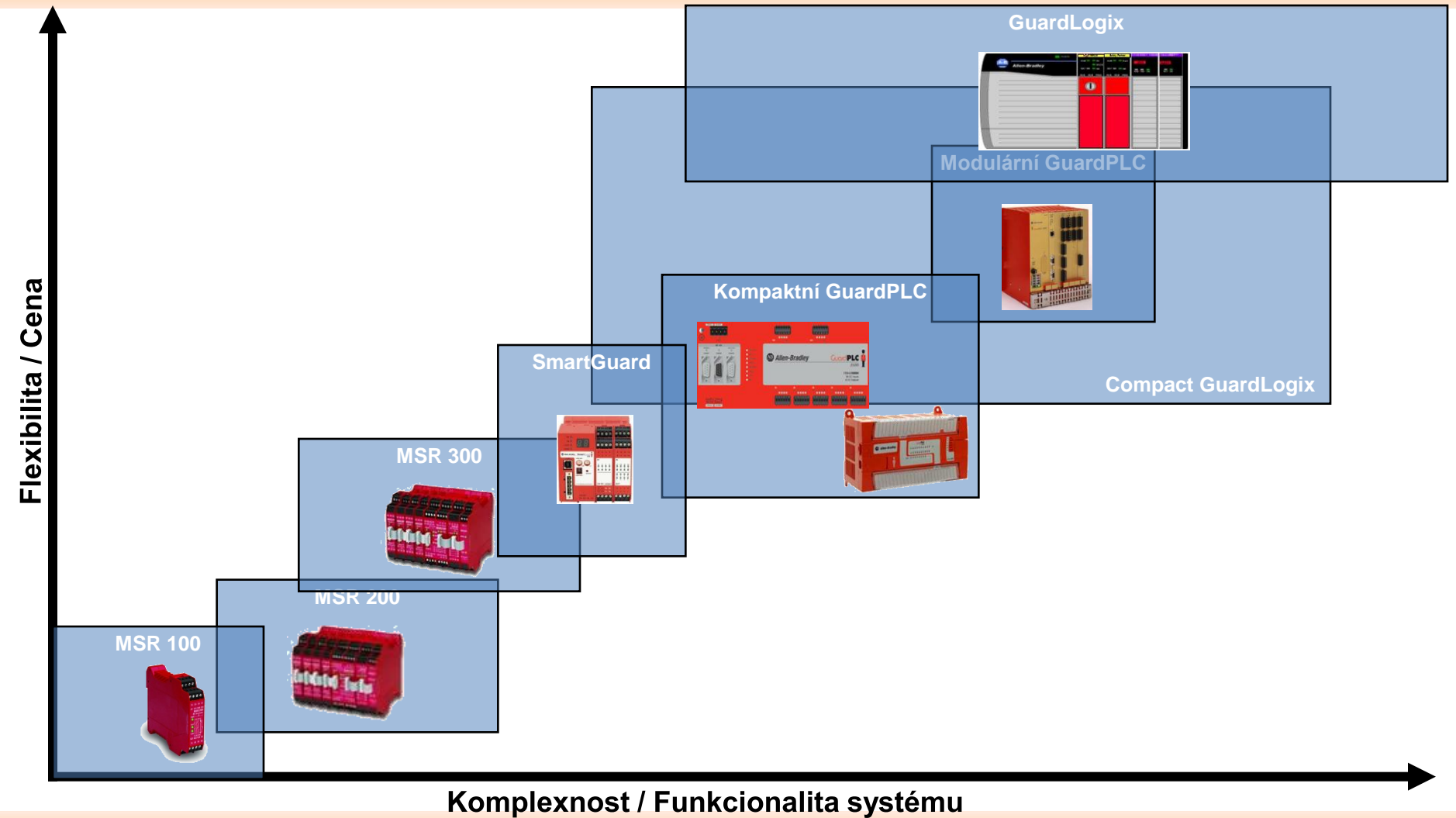
# Redundantní systémy

Cílem systémů je pokračovat v činnosti po případné poruše části či částí architektury. Tento typ řízení se používá zejména v procesním řízení, kde nenadálé odstavení systému může způsobit materiální škody, nebo dokonce poškození zdraví či ztrátu na životech. Většinou je možnost použít redundantní napájení, systém, sběrnice, vstupy a výstupy, vizualizaci i historizaci dat

- + splňují často požadavky na bezpečnost i redundanci, extrémně spolehlivé, možnost výměny částí za běhu
- značná finanční náročnost, nejlepší systémy vyrábí relativně málo specializovaných firem, pro diagnostiku a údržbu je nutná vysoce školeného odborníka



# Přehled logických prvků



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





Mgr. Karel Stibor

# SYSTÉMY LOTO

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Co to je LOTO

Slovo LOTO je zkratkou anglického „Lock-out, tag-out“.  
Výraz by se dal přeložit jako „žádost o vstup“.

Logická sekvence potom může vypadat takto:

- žádost o vstup do nebezpečného prostoru
- dokončení nebezpečných pohybů
- pokud je třeba, odepnutí silových obvodů
- odemčení nebezpečného prostoru
- práce údržby (seřizování apod.)
- zamčení nebezpečného prostoru
- zapnutí silových obvodů
- připravenost k zapnutí stroje



# Jak na LOTO

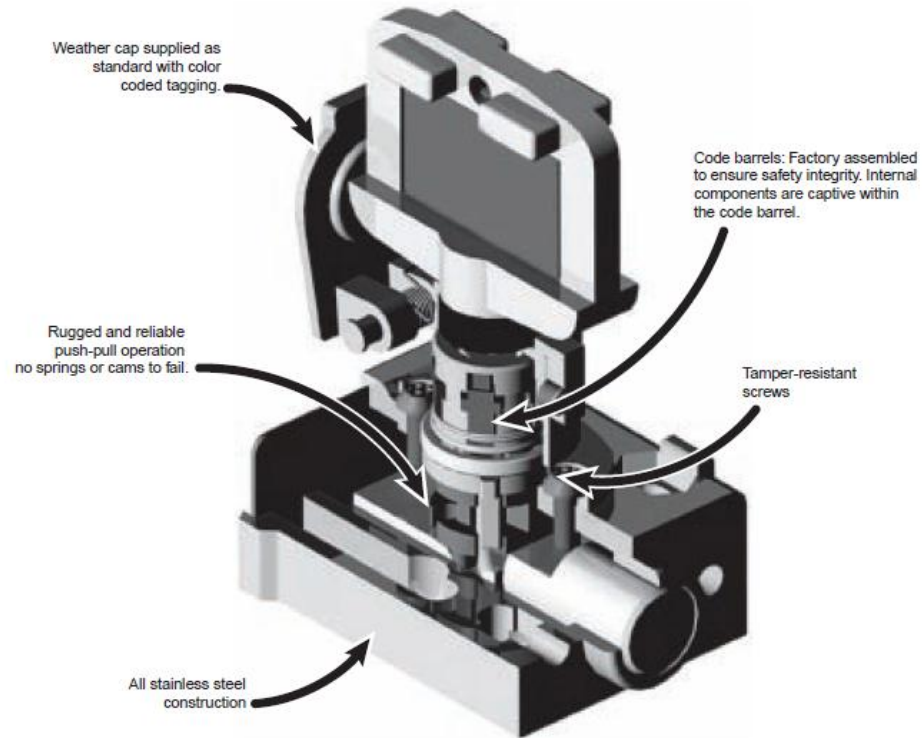
V minulosti byly systémy LOTO obsluhovány pomocí vačkových vypínačů a vysacích zámků. Nevýhodou tohoto systému je vysoká zmetkovost. Proto jsou v současnosti nasazovány elektronické nebo elektromechanické systémy.

Po stisku tlačítka řídicí systém ukončí výrobu posledního kusu, předá informaci bezpečnostní logice a ta vykoná kontrolu zastavení/vypnutí, načež odemčene nebezpečný prostor, pokud jsou splněny bezpečnostní podmínky. Po dokončení servisu je postup opačný. Největší výhodou je kontrolované zastavení, které nezpůsobí materiální škody. Navíc je často hlídána přítomnost osob v pracovním prostoru.





# Čím je LOTO realizováno?



## Prosafe Keys

Compact, solid and sturdy keys supplied with dust seals and coded tagging. Optional colors/text are available.





# Jaké jsou možnosti ?

## Plant and Machinery Interlocking

### Primary hazards (Power isolation)



Rotary key Switch

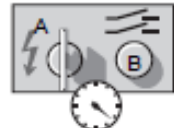


3 Port Spool valve

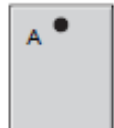
Consider removal of all power providing kinetic energy to the system i.e., electrical motors, pressurized air, etc.

Comments  
Consider factors such as run down and environmental factors such as hazardous (explosive) atmospheres. Use EEX isolator and timed delay units where necessary.

### Auxiliary hazards



Timed delay unit



Solenoid key release Unit coupled to temperature or pressure sensors

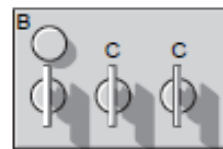


Bolt lock off device for grounding and capacitive discharge

Consider if the hazard is removed immediately i.e.,

- Machine run on due to momentum.
- Pressurization of hydraulic or pneumatic systems.
- Stored energy such as capacitance or static electricity.
- Temperature, either hot or cold, creating a hazard.

### Key control element



Required when more than one hazard element needs isolation or more than one exposure/access point interlocking.

Comments  
Consider sequentially interlocking all primary sources of hazard so all are eliminated. In turn, releasing a single key to input in key control element. Additional monitoring, isolation or control functions such as switches or solenoid locks may be incorporated at this stage to eliminate other elements.

### Guarded area access



Bolt lock for sliding guards



Access lock for general duty sliding, hinge and lift off guards



Chain interlock for large or poorly aligned sliding, hinge and lift off guards

To gain access to the danger zone.



Comments  
Consider 2 key versions to provide  
a) Personnel key exchange types to prevent operator lock-in (whole body access applications only).  
b) Lock out devices requiring 2 keys in from different sources to enable controlled access.

### Ancillary functions



Rotary key Switch



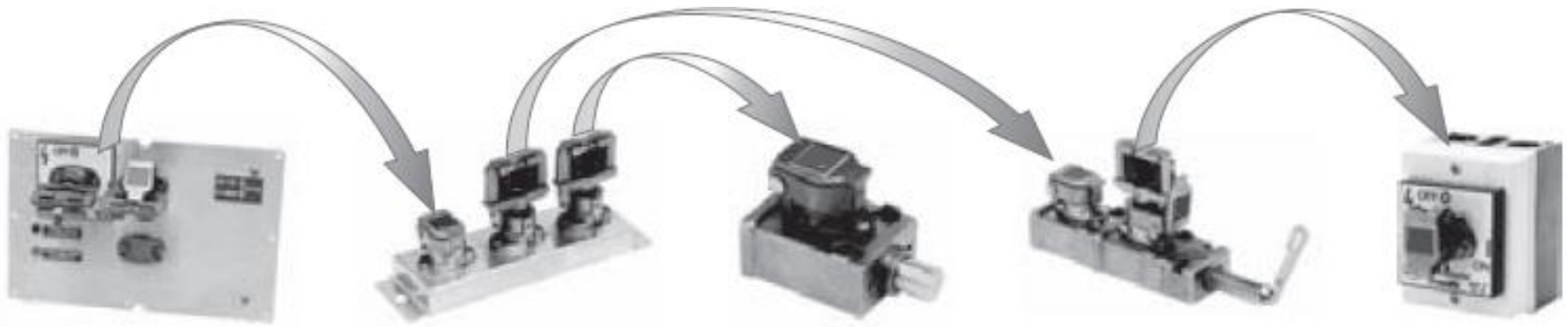
3 Port Spool valve

Required when additional functions such as programming/machine resetting are necessary.

Comments  
Two key versions required at access points to facilitate this feature.



# Ještě názorněji...



15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





Mgr. Karel Stibor

# HLAVNÍ VYPÍNAČE

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Bezpečnost a hlavní vypínač?

Použití hlavního vypínače se řídí normou EN 60204-1, článek 5.3

Hlavní vypínač musí být použit:

- na každém napájecím zdroji stroje
- pro napajeci zdroj připojeny k napajeci soustavě motoru nebo skupiny motorů tvořene připojnicovými rozvody, sestavami sběracích kroužků nebo ohebnými kabely (uloženými na bubnu nebo zavěšenými);
- pro každý vestavěný zdroj

Pokud se to žada (např. během práce na stroji nebo na elektrickem zařízení), musí tento přístroj vypnout (odpojit) elektrické zařízení stroje od napajeni.



# Jaké typy?

Jako hlavní vypínač se musí použít jeden z těchto typů :

- a) odpínač (s pojistkami nebo bez pojistek)
- b) odpojovač (s pojistkami nebo bez pojistek), který vždy zajistí přerušení proudu spínacími přístroji dříve, než se rozepnou hlavní kontakty odpojovače
- c) jistič vhodný pro odpojení podle IEC 60947-2;
- d) zásuvka s vidlicí pro stroje se jmenovitým proudem nepřekračujícím 16 A a celkovým příkonem nepřekračujícím 3 kW;
- e) zásuvka s vidlicí nebo zásuvkové spojení pro napájení pojízdných strojů ohebnými kabely

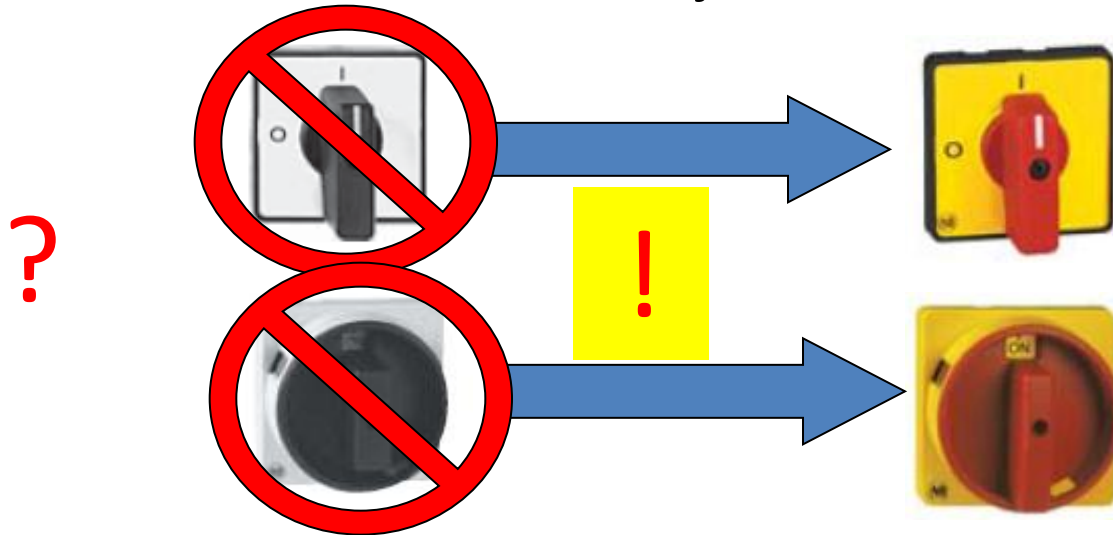
Musí být použity vypínací přístroje zabraňující neočekávanému spuštění



# Hlavní vypínač jako nouzové zastavení?

Hlavní vypínač může být použit ve funkci nouzového zastavení, pokud:

- Je snadno přístupný obsluze
- Je předepsaného typu
- Splňuje požadavky na barevnou kombinaci, tj. žluté tělo, červená ovládací rukojeť





Mgr. Karel Stibor

# NOUZOVÉ ZASTAVENÍ

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ







# Kde najdeme podklady?

Hlavní normou, při které je třeba vycházet je EN 60204-1, článek 10.7. Je ale rovněž třeba, aby E-Stop splňoval podmínky článku 9 (řídící obvody a řídící funkce).

Prvním krokem je určení typu nouzového zastavení. Může být kategorie:

- 0 – neřízené zastavení (okamžité odpojení od napájení)
- 1 – řízené zastavení (po příkazu dochází k zastavování stoje, po zastavení musí dojít k odpojení od napájení)
- 2 – řízené zastavení, kdy po zastavení zůstávají prvky napájeny

Volba kategorie vychází z analýzy rizika



# Podmínky

Nouzové zastavení musí splňovat:

- Funkce stop má prioritu před funkcí start
- Kategorie zastavení 0 a 1 musí být v činnosti nezávisle na pracovním režimu stroje, přičemž kategorie 0 má prioritu
- funkce musí být nadřazena všem ostatním funkcím a úkonnům ve všech pracovních režimech stroje
- co nejrychleji musí být přerušen přívod energie ke všem prvkům, které mohou způsobit nebezpečný stav, aniž by tím vzniklo jiné nebezpečí
- zrušení této funkce nesmí způsobit opětné spuštění stroje



# Typy ovládacích prvků

Realizovat nouzové zastavení můžeme:

- vypínač ovládaný tlačítkem
- vypínač ovládaný tažným lankem
- vypínač ovládaný pedálem bez mechanického krytu
- za určitých okolností hlavním vypínačem



+



+





# Nouzové vypnutí

Nouzové vypnutí je popsáno v normách EN 60204-1, článek 10.8 a článek 9.2.5.4.3. Funkční aspekty nouzového vypnutí je popsáno v normě EN IEC 60364-4-46.

Nouzové vypnutí má být realizováno v případech:

- ochrany osob před úrazem elektrickým proudem při dotyku živých částí
- existuje možnost vzniku jiných nebezpečných stavů, nebo poškození el. Proudem

Nouzové vypnutí je provedeno vždy odpojením od el. Zdroje a uskuteční se zastavení kategorie 0. Pokud je zastavení kategorie 0 pro stroj nepřípustné, může být ochrana před úrazem el. proudem zajištěno jinými prostředky.

Přístroje nouzového vypnutí se umísťují tam, kde je předpokládáno jejich použití. Funkce se realizuje pomocí vypínače ovládaného tlačítkem nebo vypínače ovládaného tažným lankem. Vypínač ovládaný tlačítkem je možno umístit ve skleněném krytu, který je před aktivací nutno rozbít.

Prvek musí být červený se žlutým pozadím, musí mít tvar hlavy hříbu nebo dlaně.

Po použití funkce musí dojít k ručnímu uvedení do původního stavu, až poté může být obnovena funkce obvodu.



Mgr. Karel Stibor

# OVLÁDACÍ PRVKY - AKTUÁTORY

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Podmínky použití

Je třeba, aby elektromechanické prvky splňovaly požadavky normy EN IEC 60947-5-1, kapitola 3, článek 2.2

Kontakty musí být přímo ovládány bez pružných částí tak, aby nemohl dojít k nedefinovanému stavu.

Pokud tedy použiji stykač, který má oddělitelné pomocné kontakty, jejich demontáž či samovolné odpadnutí by mohlo způsobit nebezpečný stav. Pokud použiji „klasický“ stykač či relé, je třeba, aby bylo táhlo spojující všechny kontakty z jednoho kusu a pro zpětnou vazbu mohu použít pouze pomocné kontakty na těle stykače, nikoliv pomocné.

Existují ale stykače, které mají pomocné kontakty neoddělitelné od hlavního těla. Tam mohu použít samozřejmě všechny pomocné kontakty.



# Podmínky použití - ventily

Je třeba, aby elektromechanické prvky splňovaly rovněž požadavky normy EN IEC 60947-5-1, stejně jako EN 60204-1

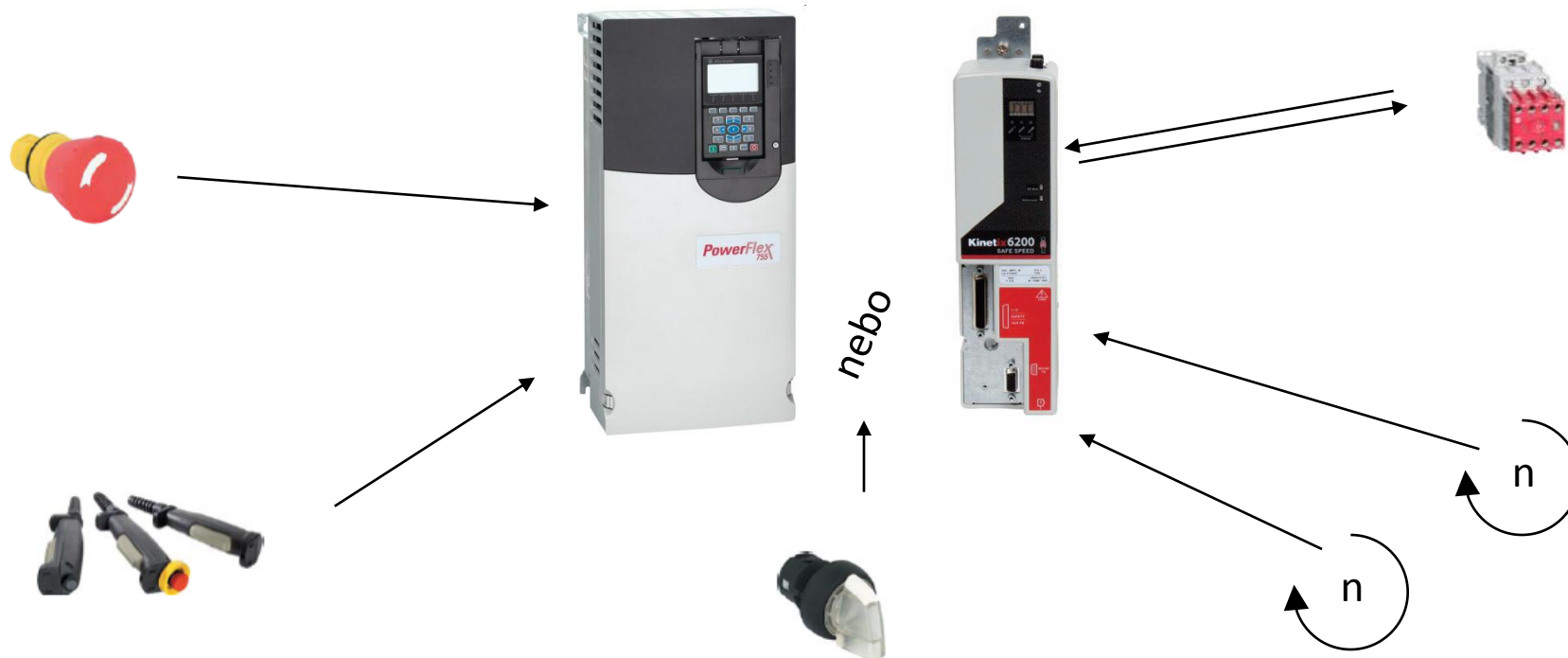
Kontakty musí být přímo ovládány bez pružných částí tak, aby nemohl dojít k nedefinovanému stavu.

Pro hydraulická vedení platí podobné podmínky, jako pro elektrická vedení (redundance, zpětná vazba apod.)



# Frekvenční měniče a serva

Pokud jsou výrobky certifikovány, mohou být použity pro řešení bezpečnostních obvodů. Jsou velice výhodné například tam, kde potřebuji zajistit bezpečně směr otáčení či nastavenou maximální hladinu otáček. Další výhodou je možnost **BEZPEČNÉ KOMUNIKACE**.







Mgr. Karel Stibor

# KLIDOVÝ STAV HŘÍDELÍ

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Proč?

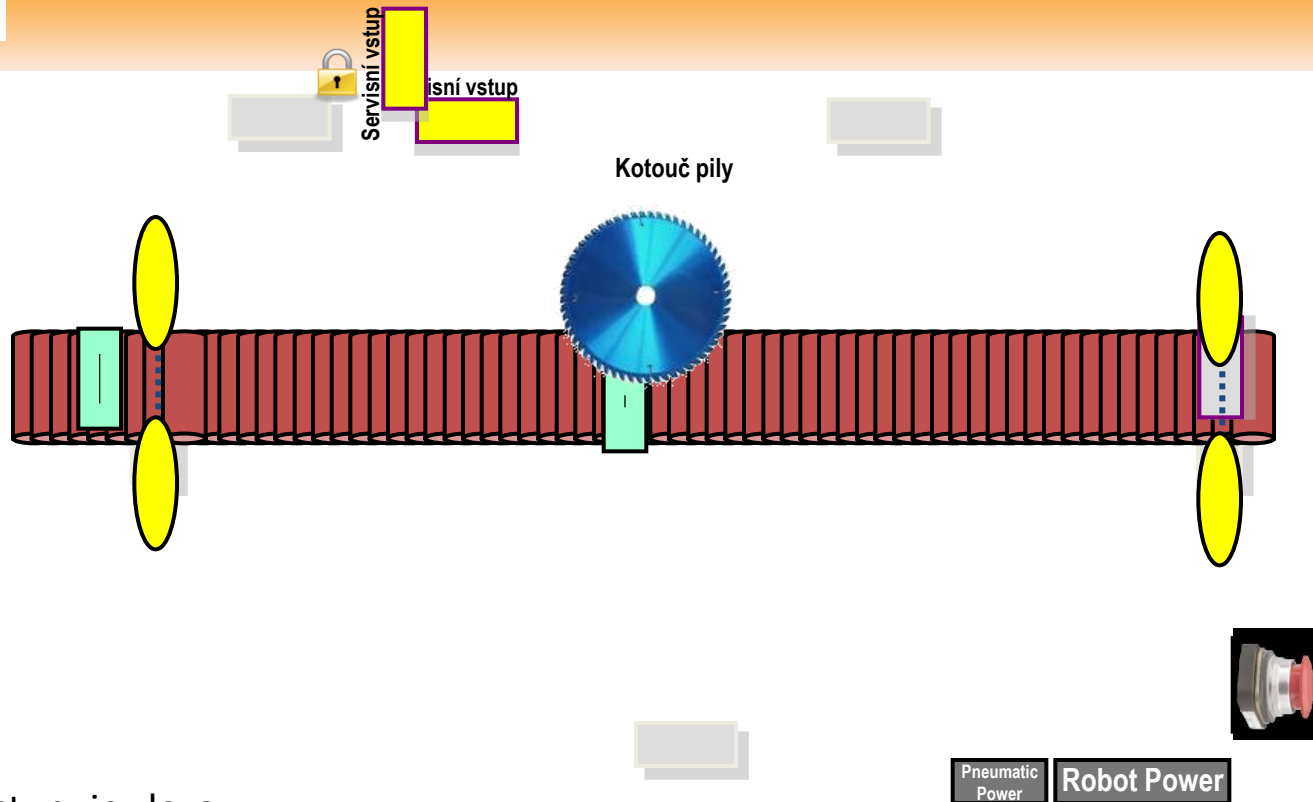
Důvodů použití monitorování os je několik:

- tam, kde konstruktér potřebuje zaručit klidový stav např. před otevřením bezpečnostního krytu
- tam, kde je třeba hlídat setrvačné síly
- tam, kde mi analýza rizika dovolí nezastavovat stroj, ale pouze zpomalit pohyb (např. kvůli seřízení, čištění apod.)
- tam, kde by nechtěnné roztočení na opačnou stranu mohlo způsobit nebezpečnou situaci (čerpadla, ventilátory, dopravníky apod.)

A samozřejmě kombinace výše jmenovaných důvodů.



# Monitorování nulové rychlosti



- Materiál vstupuje zleva
- Stroj řezá materiál
- Přítomnost osob v nebezpečném prostoru není dovolena za běhu
- Dveře jsou zajištěny pomocí bezpečnostního elektromechanického zámku

- Obsluha stiskne E-stop
- MSR57 ověřuje, zda stroj stojí
- Po zastavení odemkne zámek vchodu
- Operátor může vejít

Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

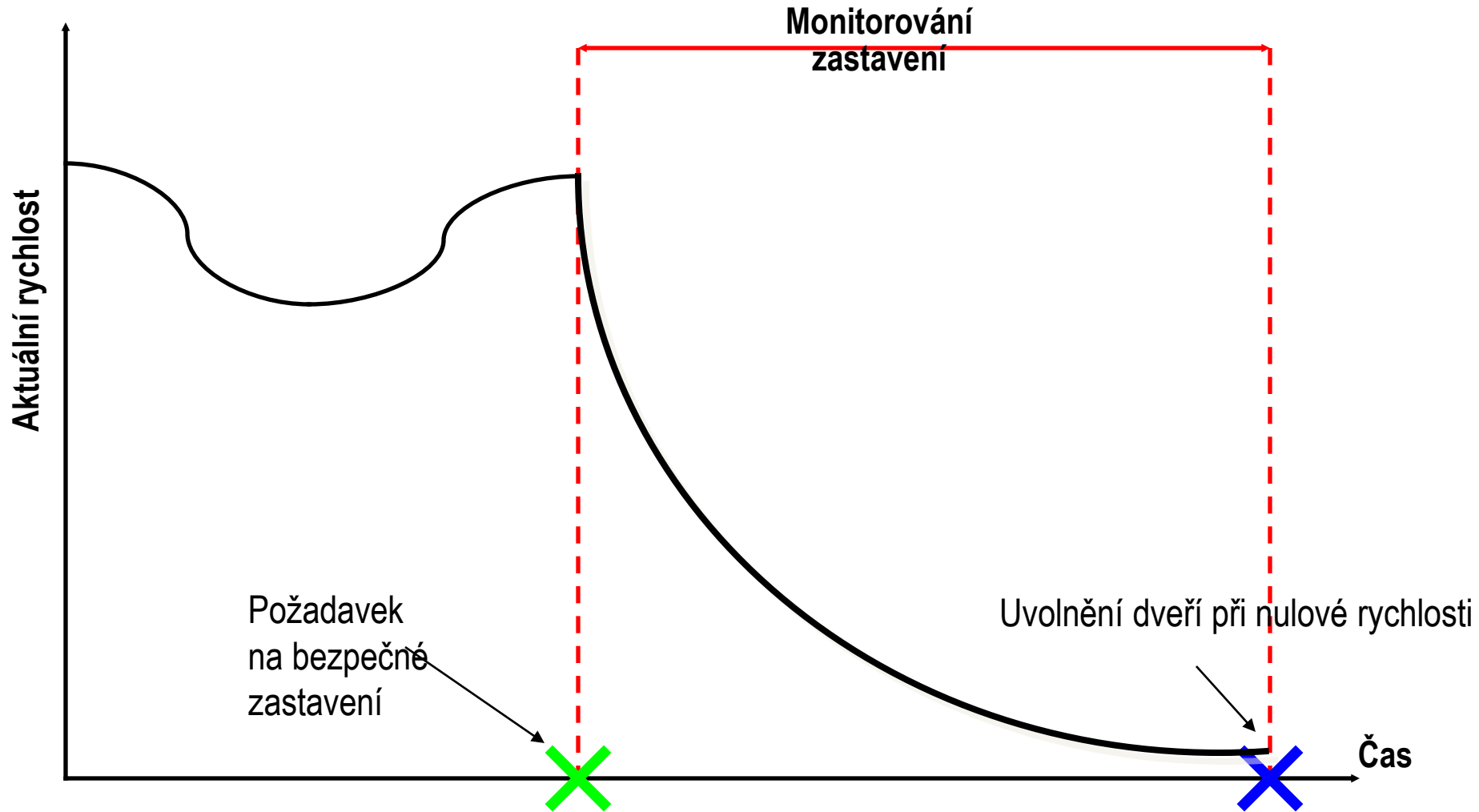
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Kategorie zastavení 0



Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

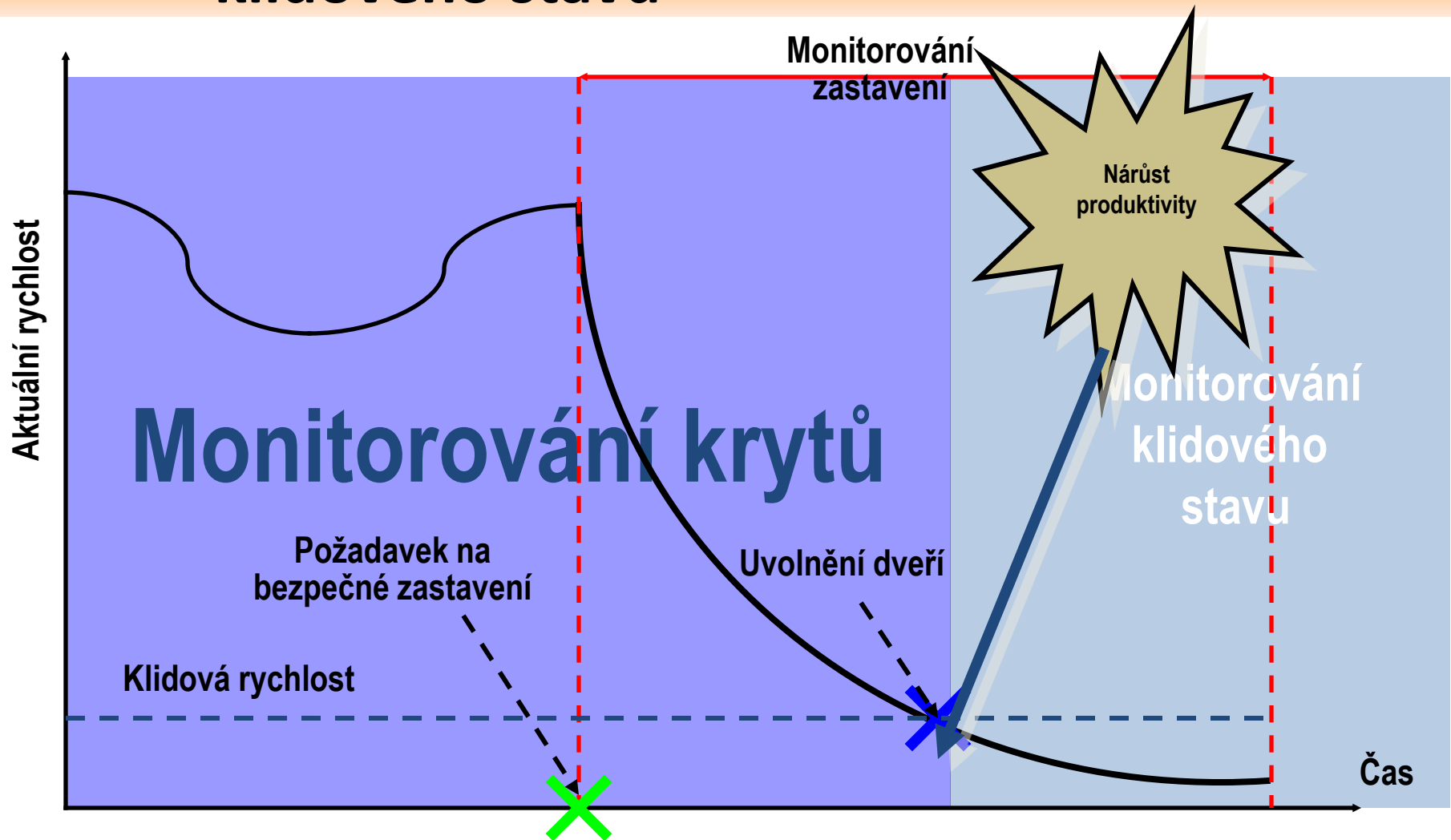
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Bezpečné vypnutí se monitorováním klidového stavu



Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

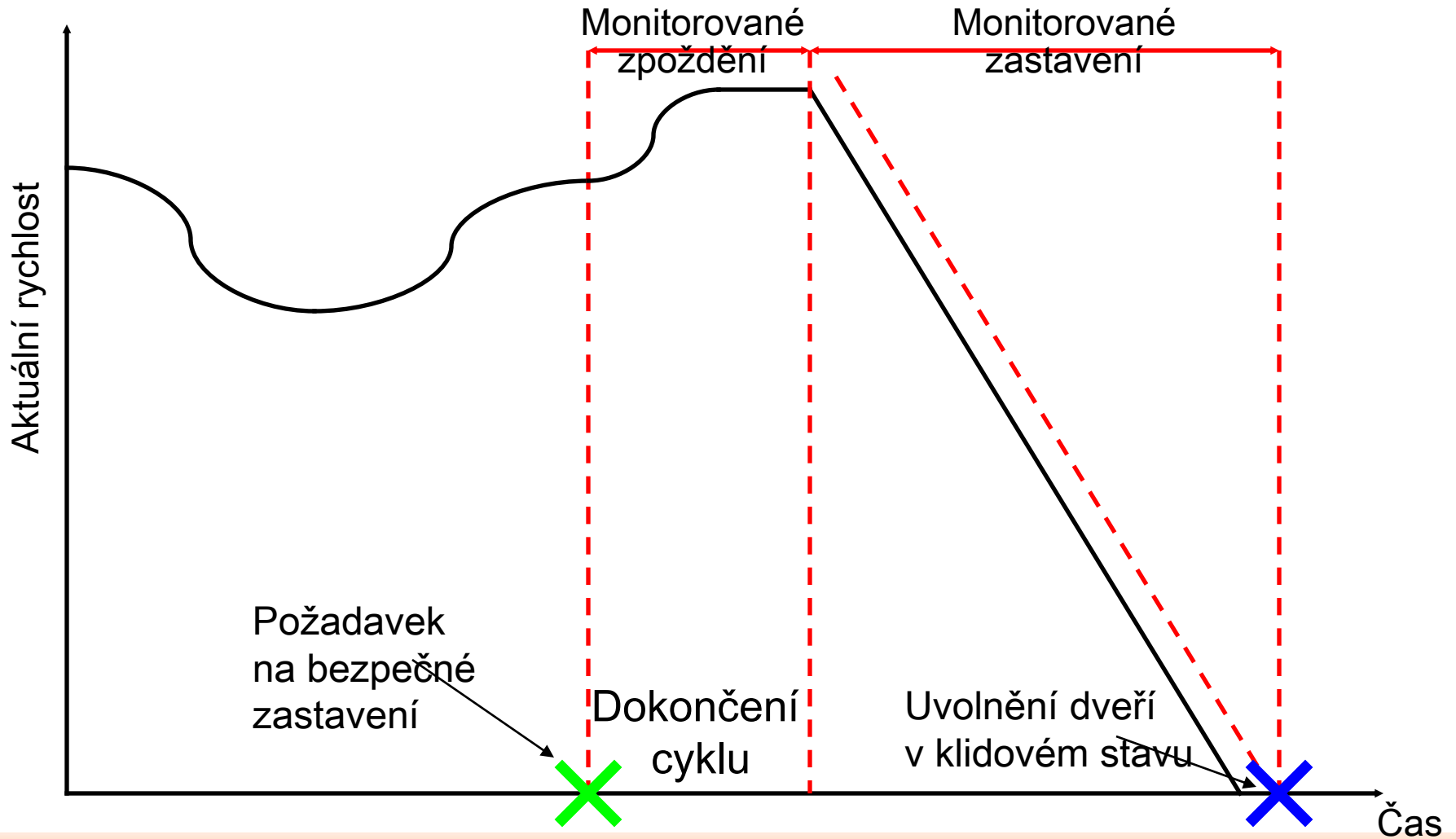
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Kategorie zastavení 1 a 2



Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

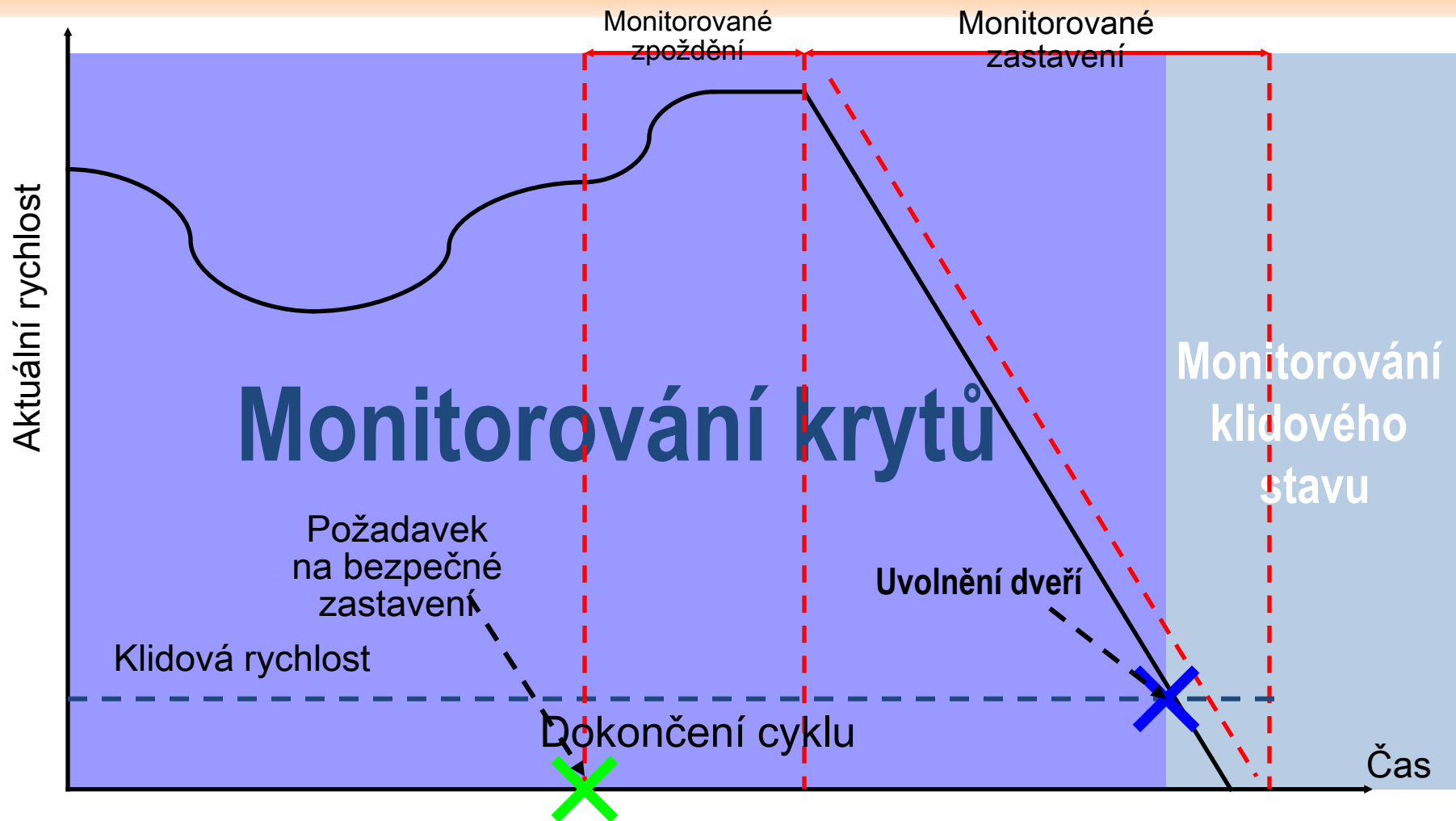
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Kategorie zastavení 1 a 2 s monitorováním



Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

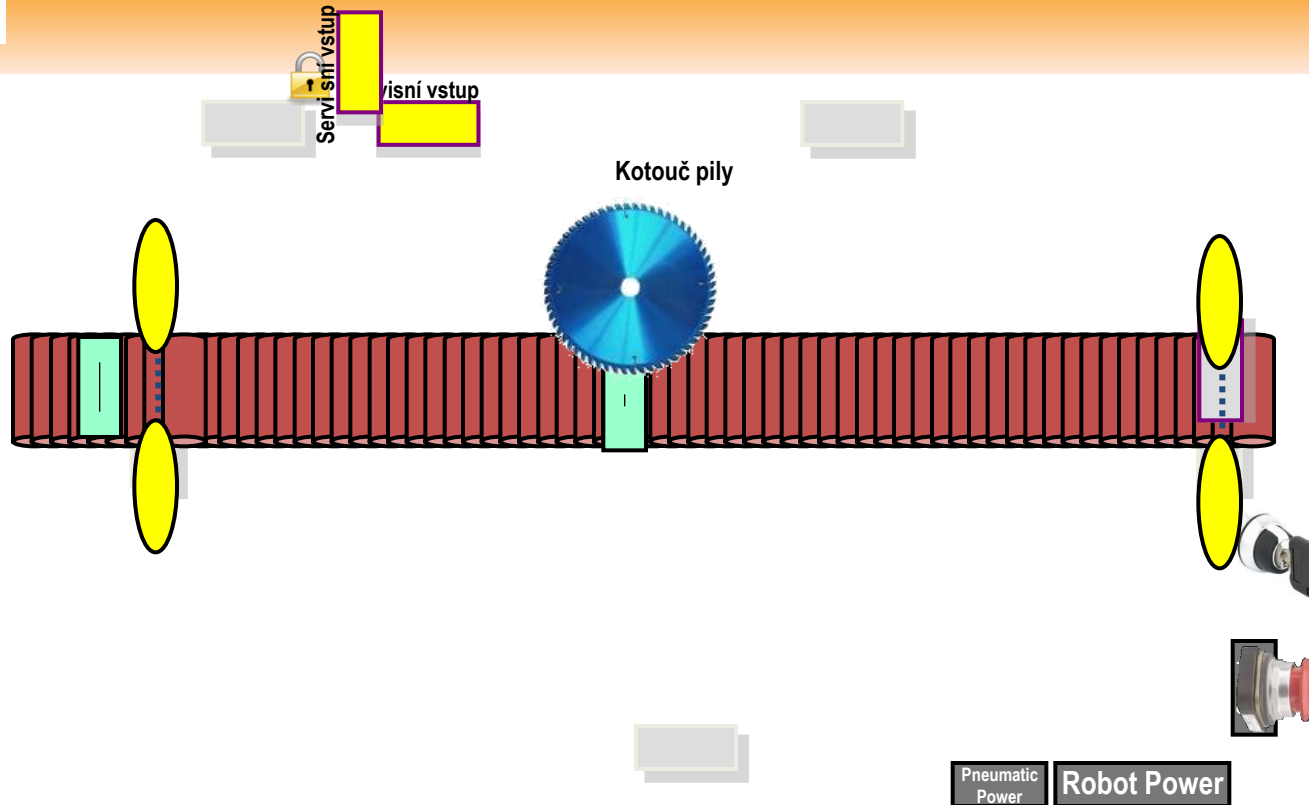


215

215



# Aplikace s limitovanou rychlostí



- Situace:

- Operátor potřebuje přístup za běhu stroje
- Nebezpečné podmínky za běhu plnou rychlostí

- Operátor stiskne požadavek na bezpečnou rychlost
- MSR57 ověří, kdy je stroj pod hranicí bezpečných otáček
- MSR57 odemkne servisní vstup
- Operátor může vstoupit za běhu stroje

Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

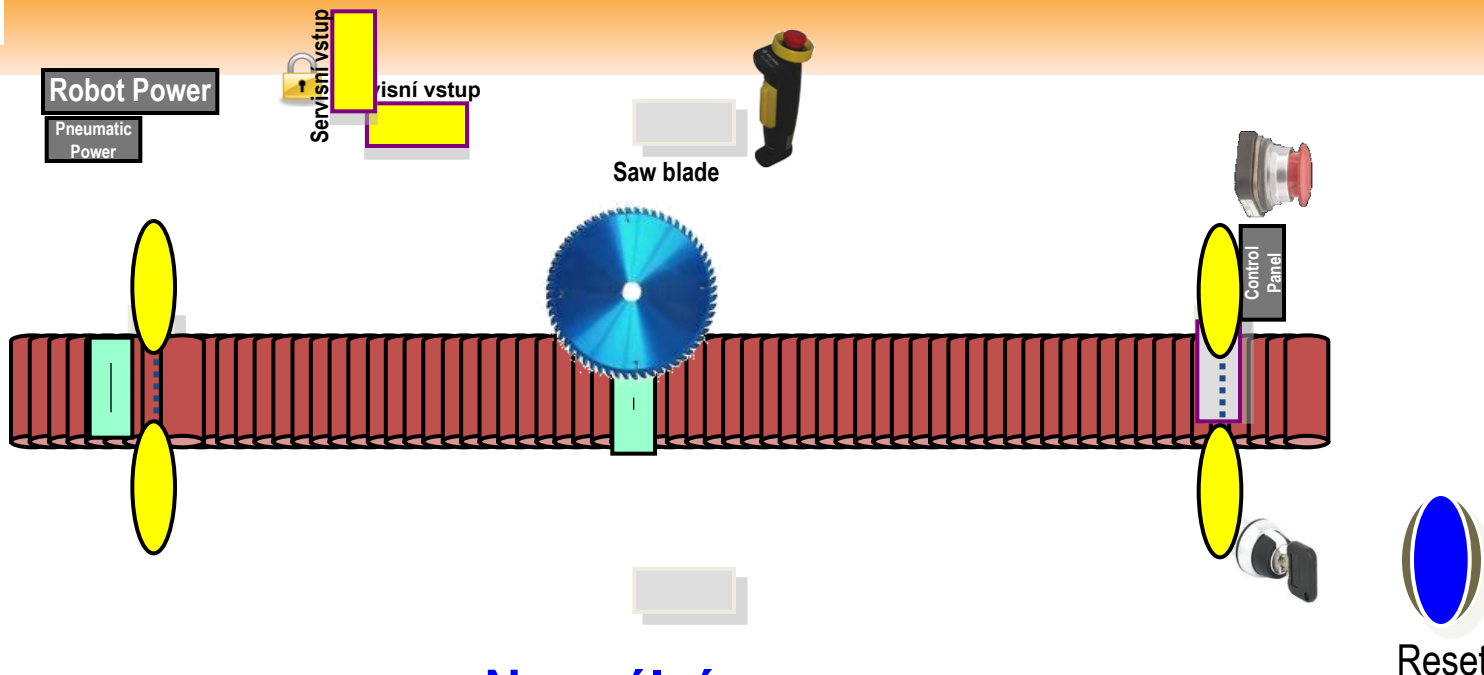
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Bezpečná rychlost s povelovým spínačem



## Normální provoz

- Operátor potřebuje vstoupit do stroje za běhu
- Nebezpečné podmínky za běhu plnou rychlostí
- Je třeba povelový spínač
- Operátor použije žádost o běh bezpečnou rychlostí

- MSR57 ověří zda je rychlost menší než nebezpečná
- MSR57 odemkne servisní vstup
- Operátor může vstoupit do stroje, dokud stroj běží a operátor drží povelový spínač

Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

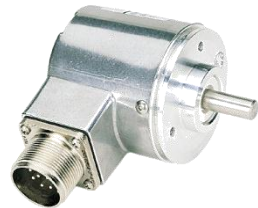


# Nejuniverzálnější způsob...

**zátěž**



**pohon**



## Door Control and Monitoring



Normální Start/Stop

E-Stop



NEBO



**E-Stop**



**Volič režimů**



**Povelový spínač  
(„tlačítko mrtvého muže“)**



Copyright © 2008 Rockwell Automation, Inc. All rights reserved.

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





Mgr. Karel Stibor

# DVOURUČNÍ OVLÁDÁNÍ

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Legislativa

Dvouruční ovládání je popsáno v normě EN 60204-1, přičemž při konstrukci se vychází z EN 574+A1.

Je třeba ho nasadit tam, kde je třeba obsluhu uchránit od nebezpečí. Dvouruční ovládání má za cíl „zaměstnan“ obsluhu na určitém místě, které je mimo nebezpečnou oblast a je součástí jiných ochranných opatření, jako například optické závory.

Používá se mimo jiné na absolutní většině lisů a to ať už excentrických, hydraulických nebo pneumatických.



# Typy

Dvouruční ovládání může být 3 základních typů:

Typ I vyžaduje:

- použití dvou ovládacích prvků, na které je třeba působit současně
- nepřetržité působení na oba prvky po celou dobu trvání nebezpečí
- pokud nebezpečný stav trvá, musí se funkce zastavit uvolněním kteréhokoliv z prvků

Typ II vyžaduje:

- ovládání stejné jako typ I
- před novým spuštěním (lisovací cyklus apod.) uvolnění obou ovládacích prvků

Typ III vyžaduje:

- ovládání stejné jako typ II
- na oba ovládací prvky je třeba zapůsobit v průběhu méně než 0,5s
- pokud je toto časové rozmezí překonáno, je třeba uvolnit oba ovládací prvky před novým spuštěním funkce



# Typy

Požadavky	Článek EN 574	Typy				
		I	II	III		
				A	B	C
Použití obou rukou (současné ovládání)	5.1	X	X	X	X	X
Vztah mezi vstupními signály a výstupním signálem	5.2	X	X	X	X	X
Přerušení výstupního signálu	5.3	X	X	X	X	X
Zamezení náhodnému spuštění	5.4	X	X	X	X	X
Zamezení vyřazení <sup>*)</sup>	5.5	X	X	X	X	X
Opětovná iniciace výstupního signálu	5.6		X	X	X	X
Synchronní ovládání	5.7			X	X	X
Použití kategorie 1 (EN 954-1:1996)	6.2	X		X		
Použití kategorie 3 (EN 954-1:1996)	6.3		X		X	
Použití kategorie 4 (EN 954-1:1996)	6.4					X



# Ověření

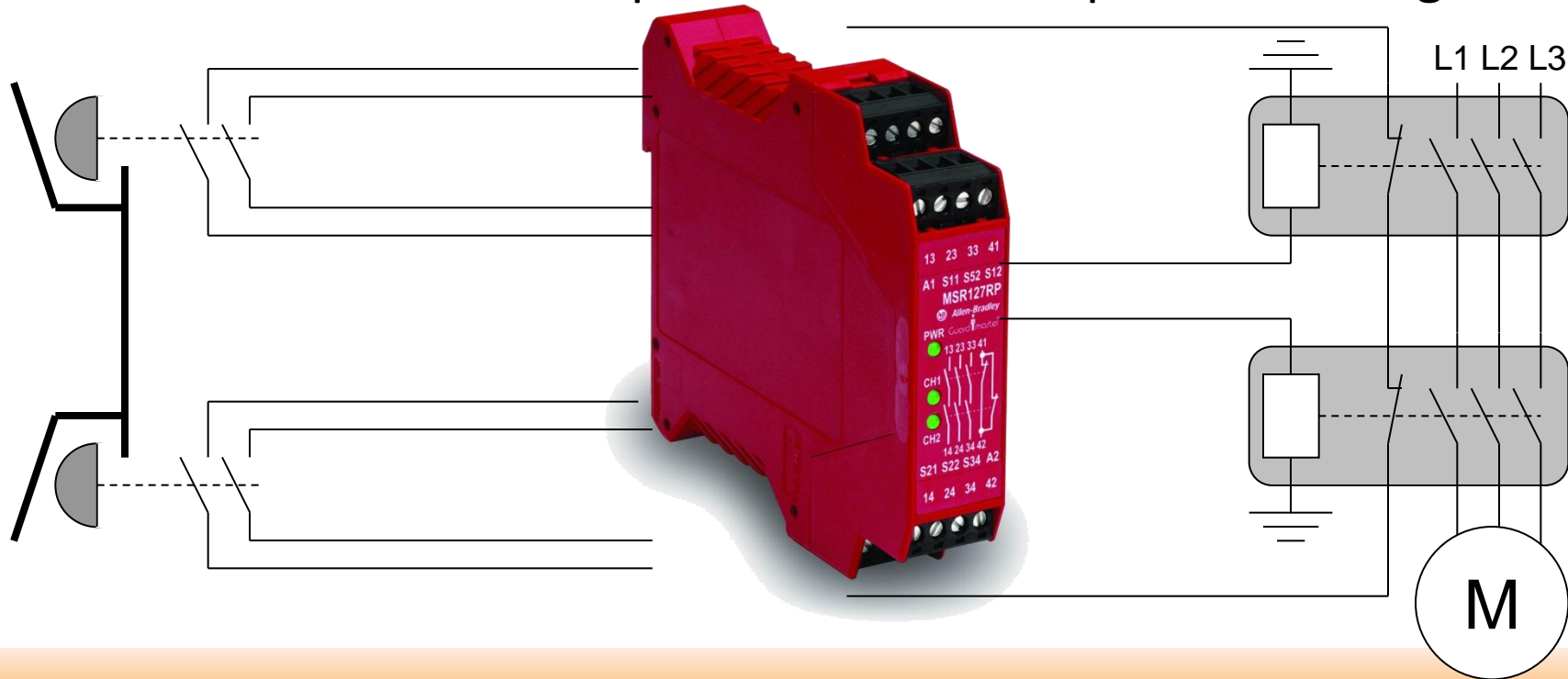
Bezpečnostní požadavky	Zkouška		
	Vizuální prohlídka	Funkční kontrola	Měření
<b>Všeobecně</b>			
Provozní podmínky, vlivy prostředí		X	X
Požadavky na zakrytí	X	X	
Volba, konstrukce a instalace ovládacího spouštěcího zařízení	X	X	X
Neúmyslný výstupní signál vyvolaný zrychlujícími silami		X	X
Neúmyslné spuštění	X	X	
Stabilita		X	
Doba reakce			X
Značení	X		
<b>Funkční vlastnosti</b>			
Použití obou rukou	X	X	
Vztah vstupního/výstupního signálu		X	
Přerušení výstupního signálu		X	
Náhodné spuštění	X	X	X
Vyřazení	X	X	X
Opětovná iniciace		X	
Synchronní ovládání		X	X
<b>Kategorie ovládání</b>			
Kategorie 1	X		
Kategorie 3		X	X
Kategorie 4		X	X



# Realizace

Realizace funkce probíhá pomocí:

- dvojice tlačítek (v předepsaném uspořádání dle EN 574)
- logického obvodu dle EN ISO 13849-1 či EN 61508
- ovládacího obvodu se zpětnou vazbou dle příslušné kategorie



15.10.2010





Mgr. Karel Stibor

# BEZPEČNOST A VÝBUŠNÉ PROSTŘEDÍ

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Legislativa

Stejně jako výchozím dokumentem pro bezpečnost je analýza rizik, pro aplikace (nejen) do výbušného prostředí se jedná o „protokol o prostředí“. Ten musí mít konstruktéři k dispozici, aby mohli řádně zpracovat svoje části projektů.

Na výběr máte dvojí postup, jak splnit legislativní požadavky:

- použít oddělovací bariéru pro splnění požadavků výbušného prostředí
- použít prvky, které splňují oba legislativní požadavky



# Možnosti

Výbušné prostředí

Nevýbušné prostředí

Bezpečnostní  
HW vstupů

Jiskrově  
bezpečné  
signály



Klasické  
signály

Bezpečnostní  
HW logiky a  
výstupů

Splňuje požadavky EN 13849-1,  
60204-1 atd.

Oddělující bariéra splňující  
požadavky prostředí i výbušnosti

- + široká univerzálnost
- cena
- certifikace

Bezpečnostní  
HW vstupů

Signály bezpečné  
jiskrově  
i bezpečnostně

Bezpečnostní  
HW logiky a  
výstupů

HW splňující požadavky prostředí i  
výbušnosti

HW splňující požadavky prostředí i  
výbušnosti

- + certifikace
- jednoduchost
- cena

15.10.2010



# Označení výrobků

Klasifikace a označení výbušných tříd a zón				
Hořlavé látky	Pravděpodobnost exploze	Určení výbušné zóny	Charakteristika produktů	
			Skupina	Kategorie
Plyny, páry, mlha	Neustálé, dlouhodobé nebezpečí	<b>zóna 0</b>	II	
	Nebezpečí se může vyskytnout	<b>zóna 1</b>	II	1G
	Může se vyskytnout, ale jen krátkodobě	<b>zóna 2</b>	II	
Prach	Neustálé, dlouhodobé nebezpečí	<b>zóna 20</b>	II	
	Nebezpečí se může vyskytnout	<b>zóna 21</b>	II	1D
	Může se vyskytnout, ale jen krátkodobě	<b>zóna 22</b>	II	
Methan	-	<b>důlní průmysl</b>	I	
	-	<b>důlní průmysl</b>	I	M1 M2

Příklad typového označení:

CE 0158



II

2G

EEx d IIC T6 PTB 99 ATEX1103

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Označení výrobků

Klasifikace zón s nebezpečím vznícení plynů, par a mlhy						
Výbušná skupina		Příklady závislé na: - skupině výbušnosti - teplotní třídě				
IIA	IIB	IIC	Amoniak	Ethylalkohol	Benzin	Acetaldehyd
			Methan	Cyklohexan	Nafta	
			Etan	Butan	Ropa	
			Propan		Hexan	
			Směs	Ethylen	Ethylglykol	Ethylether
			Acetonitril	Ethylenoxid	Karbon	
			Hydrogen	Acetylen		Karbon

T1 < 450°C    Pozor: tato tabulka slouží pouze jako příklad  
hořlavých látek u kterých hrozí bezprostřední  
nebezpečí výbuchu. Seznam není proto  
úplný!

T2 < 300°C

T3 < 200°C

T4 < 135°C

T5 < 100°C

T6 < 85°C

Produkty jsou závislé na teplotní třídě (T1 - T6).  
Tepl. třída znamená max teplotu na povrchu

Příklad typového označení:

CE 0158



II

2G

EEx d

IIC

T6

PTB 99 ATEX1103

15.10.2010



# Označení výrobků

Autorizované zkušebny		
Země	Kód	Autoriz. zkušebna
Německo	003	TÜV Hannover/Sachsen-Anhalt e.
Německo	0102	PTB
Německo	0158	IMT
Německo	0297	DOS
Německo	0588	FGA
Německo	0589	BAW
Německo	0837	IE ExU
Francie	0080	IFERIS
Francie	0081	LCIE
Holandsko	0344	EMA
Švédsko	0402	SP
V. Británie	0800	EECS BASEEFA
V. Británie	0617	

Princip ochrany - typ ochrany - norma CENELEC + základní norma EN 50014					
Oblasti použití	Typ ochrany	Kód	Symbol	Použití v zóně	CENELEC
Prevence přenesení výbuchu do okolního prostředí	<b>Pevný závěr</b>	Ex d		1, 2	EN 50018
Prevence vysokých teplot a nadměrného jiskření	<b>Zajištěné provedení</b>	Ex e		1, 2	EN 50019
Proudové a napětové okruhy	<b>Jiskrová bezpečnost</b>	Ex i		0, 1, 2***	EN 50020* EN
Přetlak	<b>Přetlakové zapouzdření</b>	Ex p		1, 2	EN 50016**
Zapouzdření	<b>Zalité zapouzdření</b>	Ex m		1, 2	EN 50028
Části ponořené do oleje jsou izolovány od zdroje zážehu	<b>Olejové zapouzdření</b>	Ex o		1, 2	EN 50015
Prevence přenesení výbuchu do okolního prostředí	<b>Pískový závěr</b>	Ex q		1, 2	EN 50017
Stejně jako výše uvedené, ale pro použití pouze v zóně 2	<b>Ochrana "n"</b>	Ex n		2	EN 50021

Další informace	
Typ použití	Kód
Pro běžné použití	-
Pro speciální použití	X
Tyto výrobky jsou jen částečně certifikovány, a proto nejsou samostatně použitelné	U

\* Produkt \*\* Systém \*\*\* ia v zónách 0, 1 a 2 ib v zónách 1 a 2

Příklad typového označení:

CE 0158 II 2G Ex d IIC T6 PTB 99 ATEX1103

15.10.2010

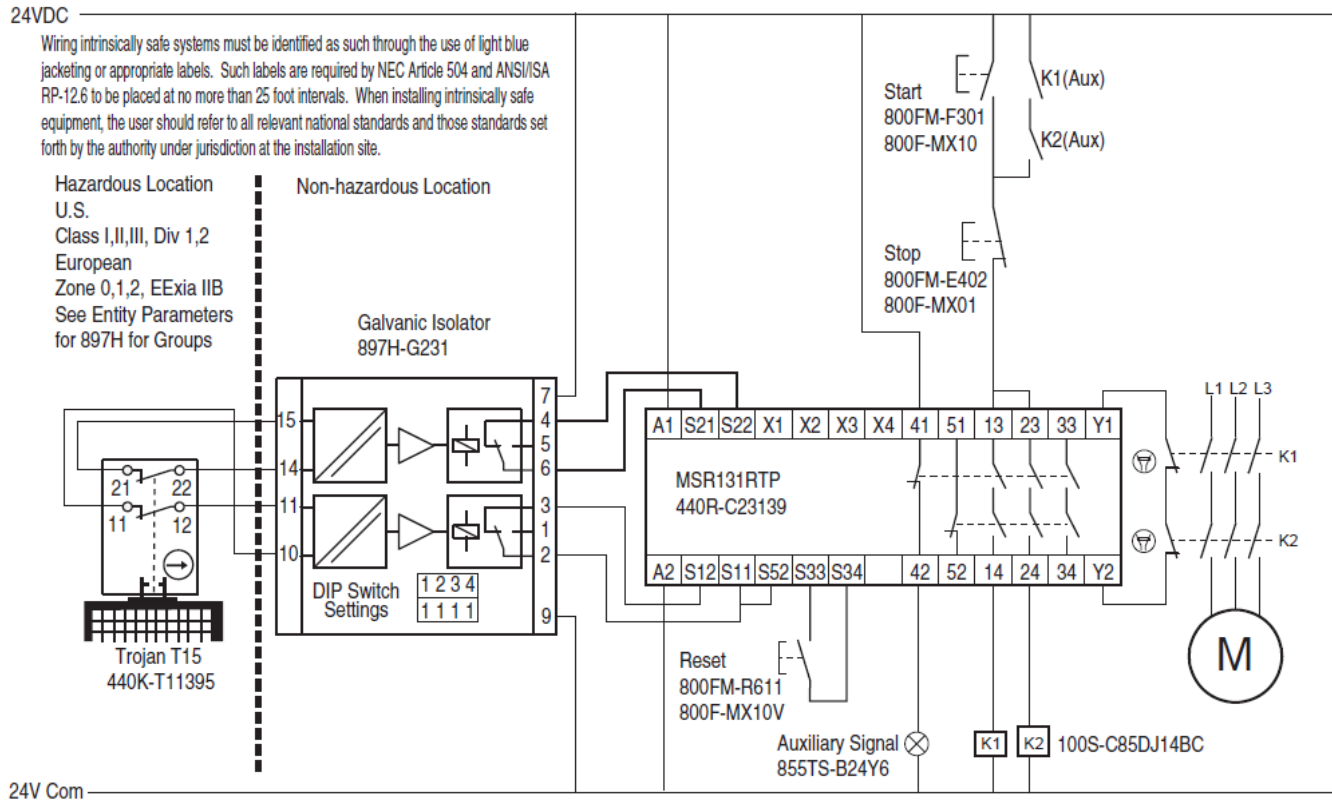
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Doporučení

Pokud je to jenom trošku možné, používejte doporučená zapojení daná výrobcem. Zjednodušíte si certifikaci zejména s ohledem na výbušné prostředí !



15.10.2010



Mgr. Karel Stibor

# ZAPOJOVÁNÍ BEZPEČNOSTNÍCH PRVKŮ

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



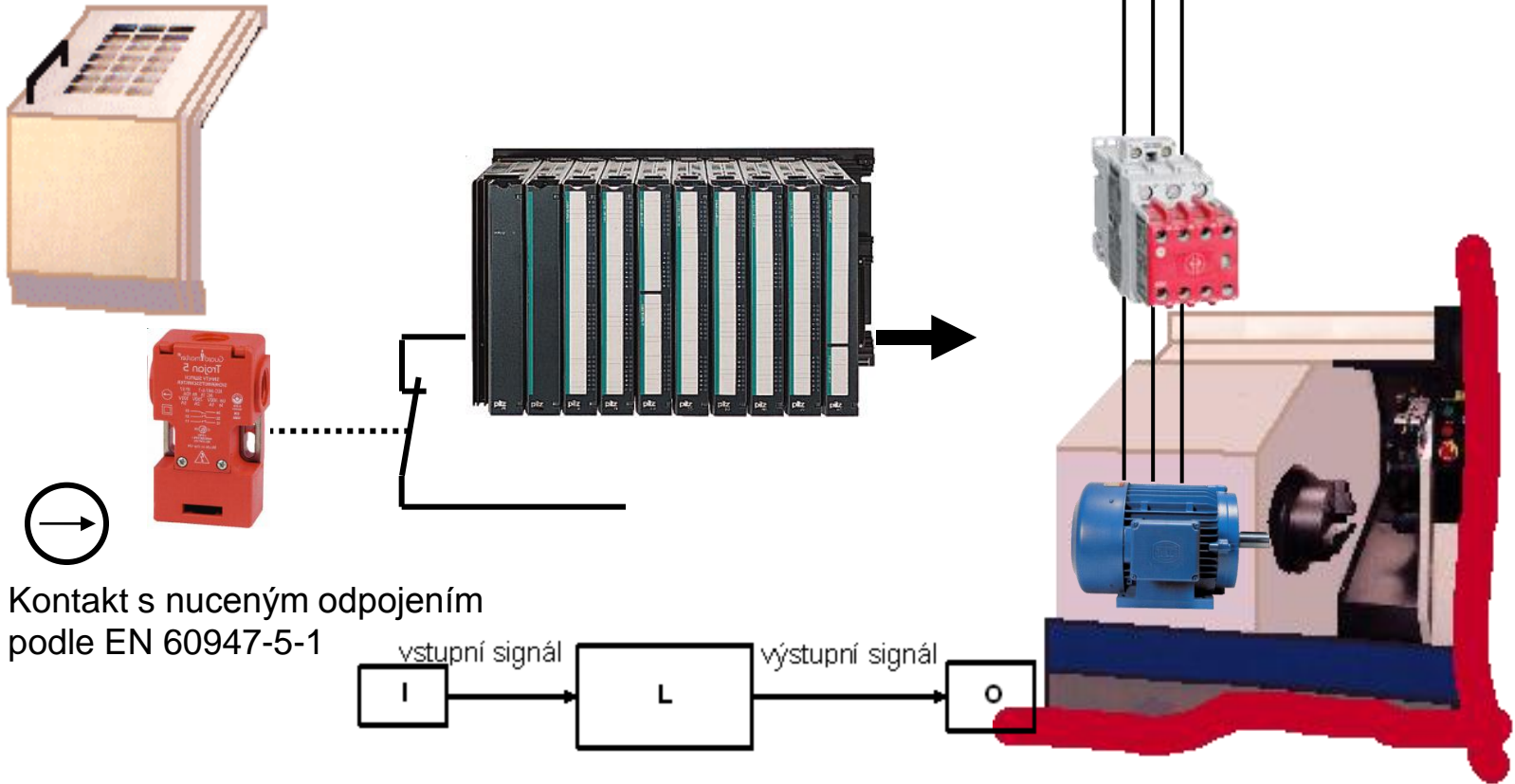




# Architektura podle EN 13849-1

## Kategorie 1

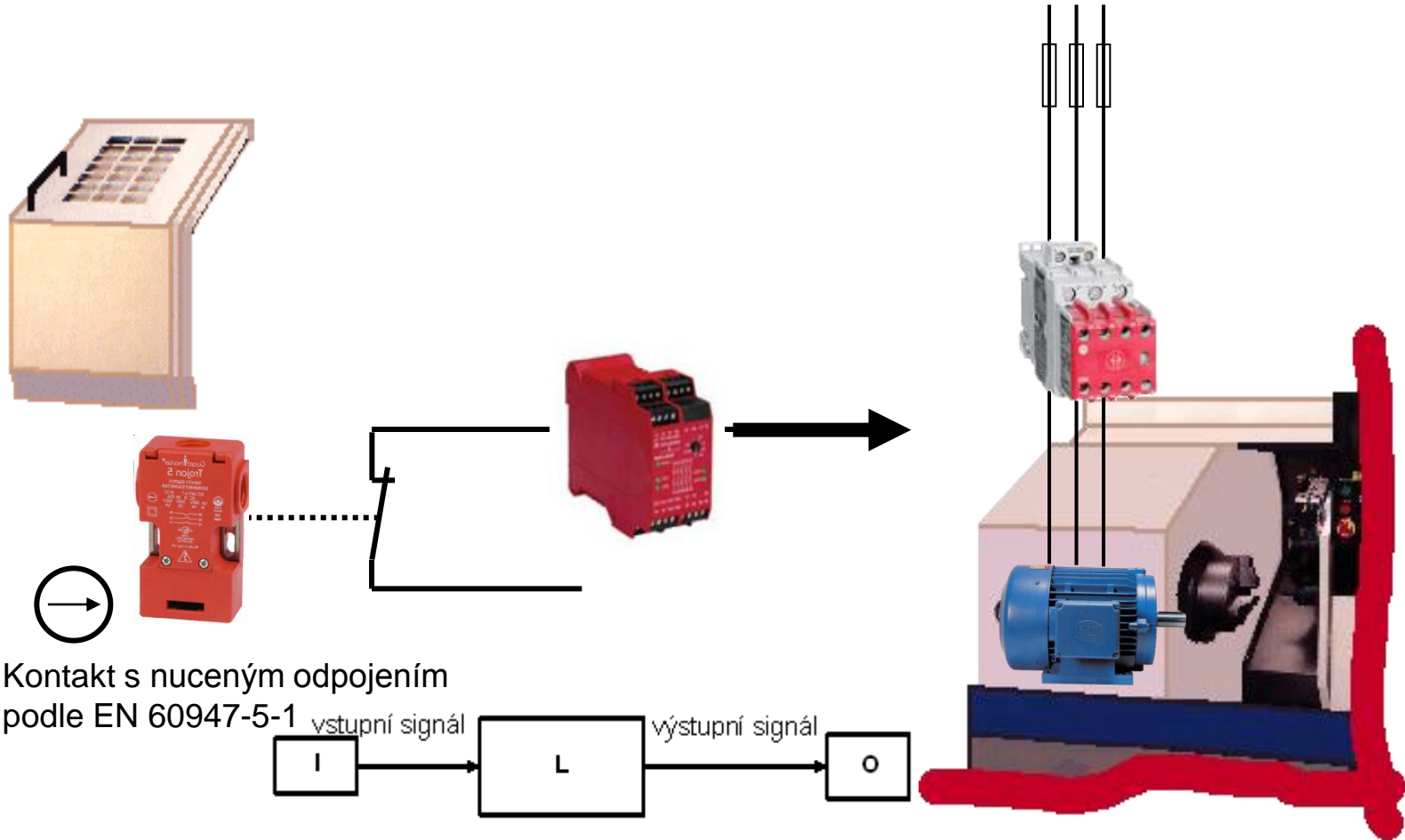
Je architektura v pořádku?





# Architektura podle EN 13849-1

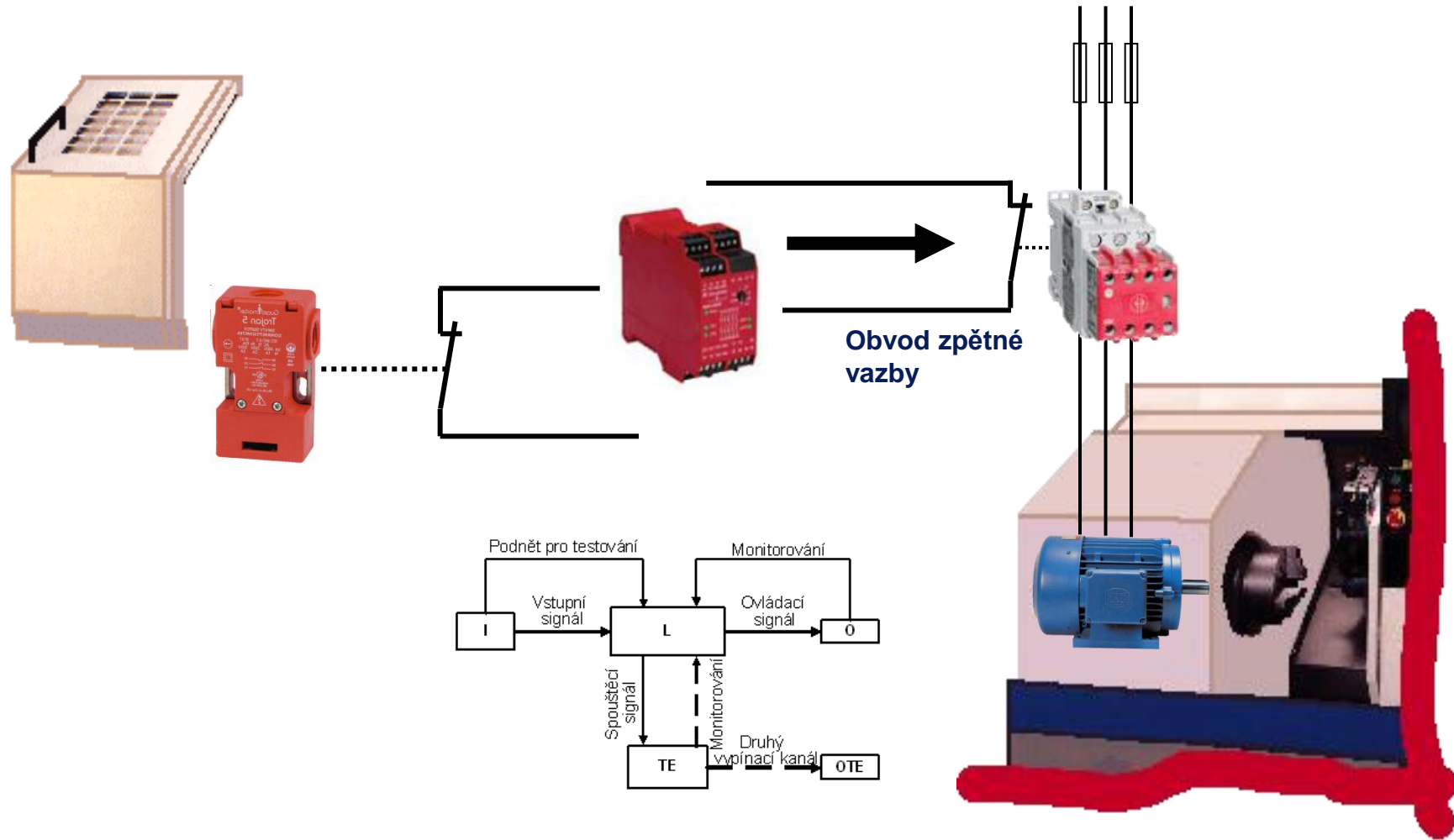
## Kategorie 1





# Architektura podle EN 13849-1

## Kategorie 2



15.10.2010

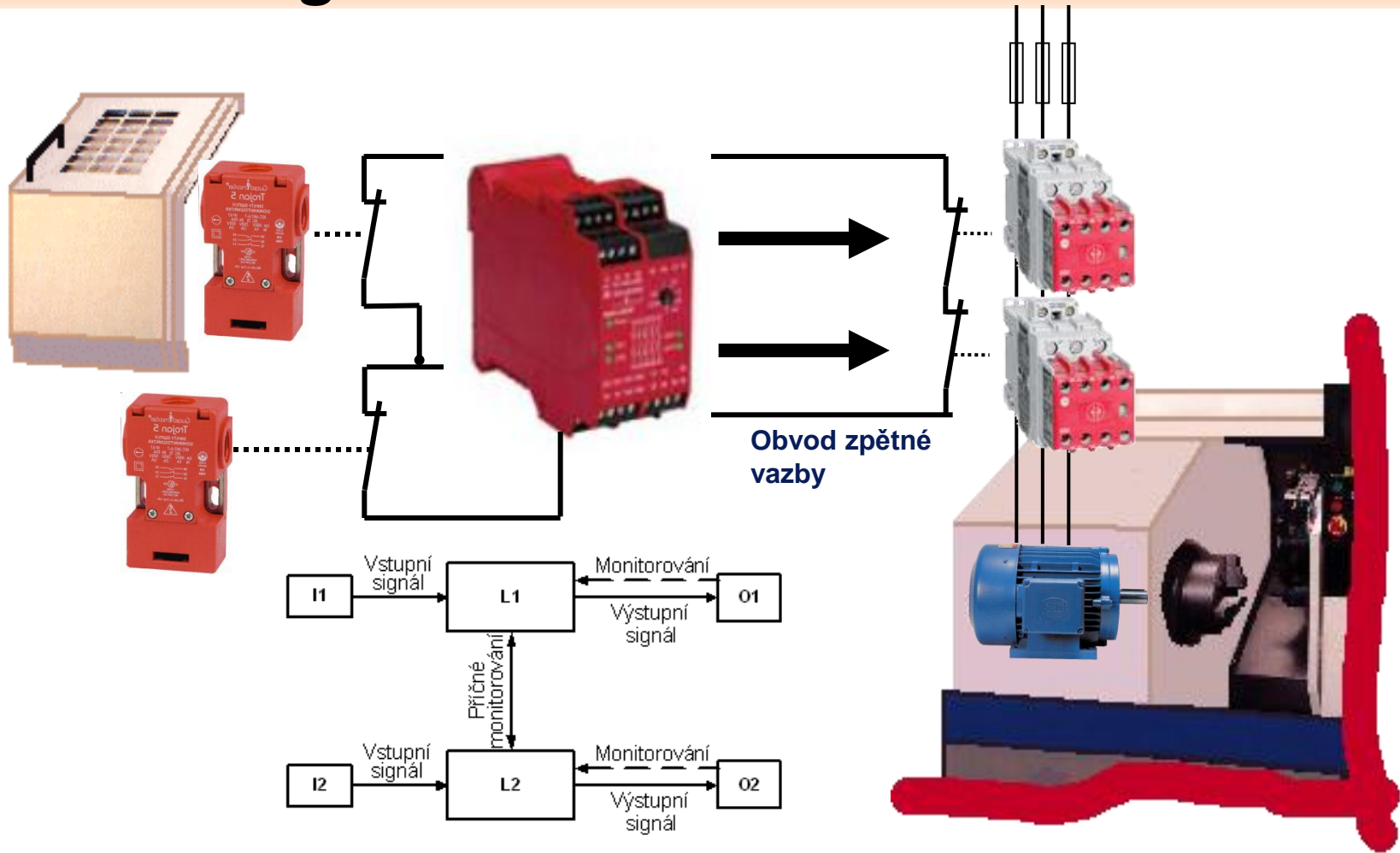
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Architektura podle EN 13849-1

## Kategorie 3



15.10.2010

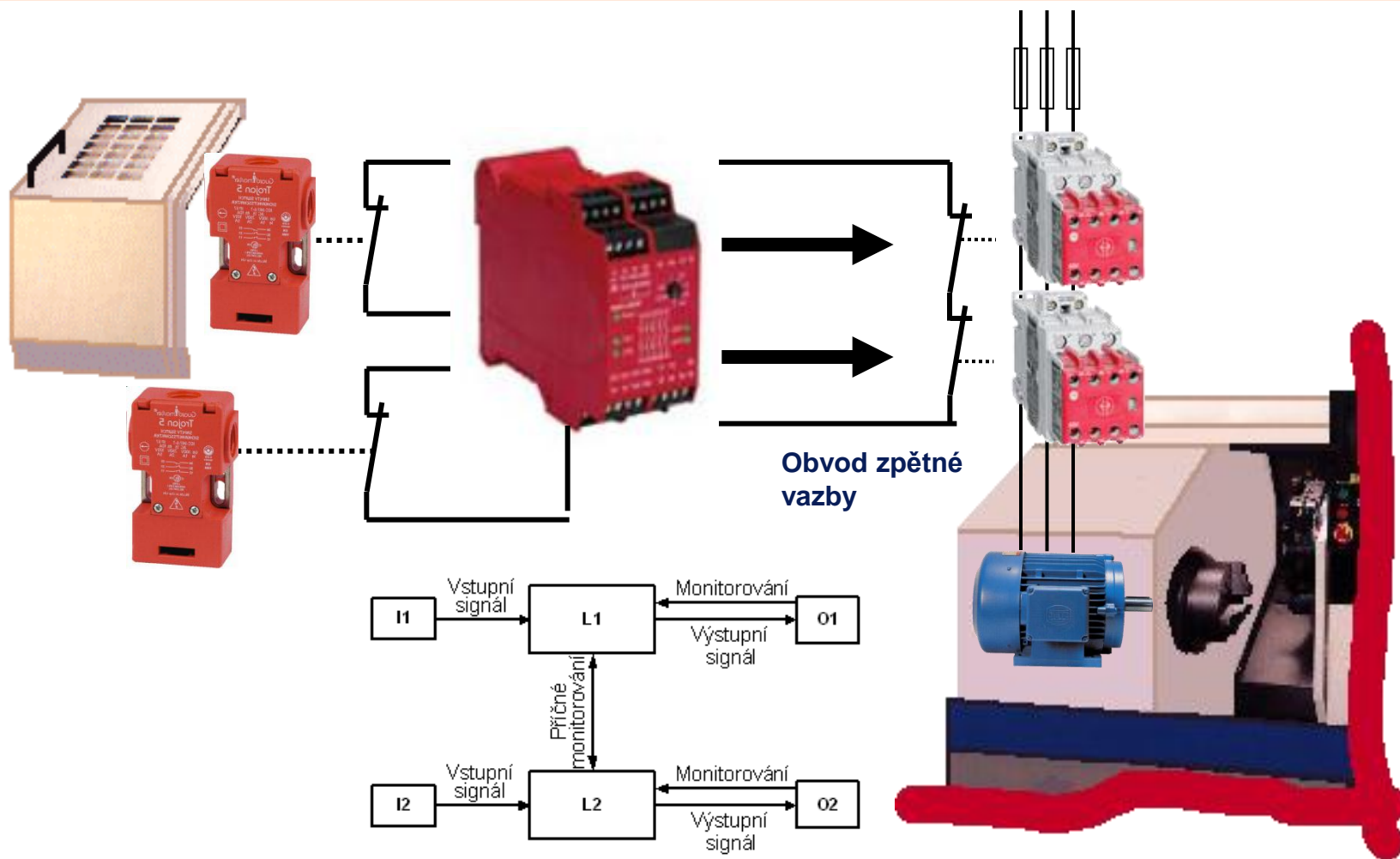
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Architektura podle EN 13849-1

## Kategorie 4



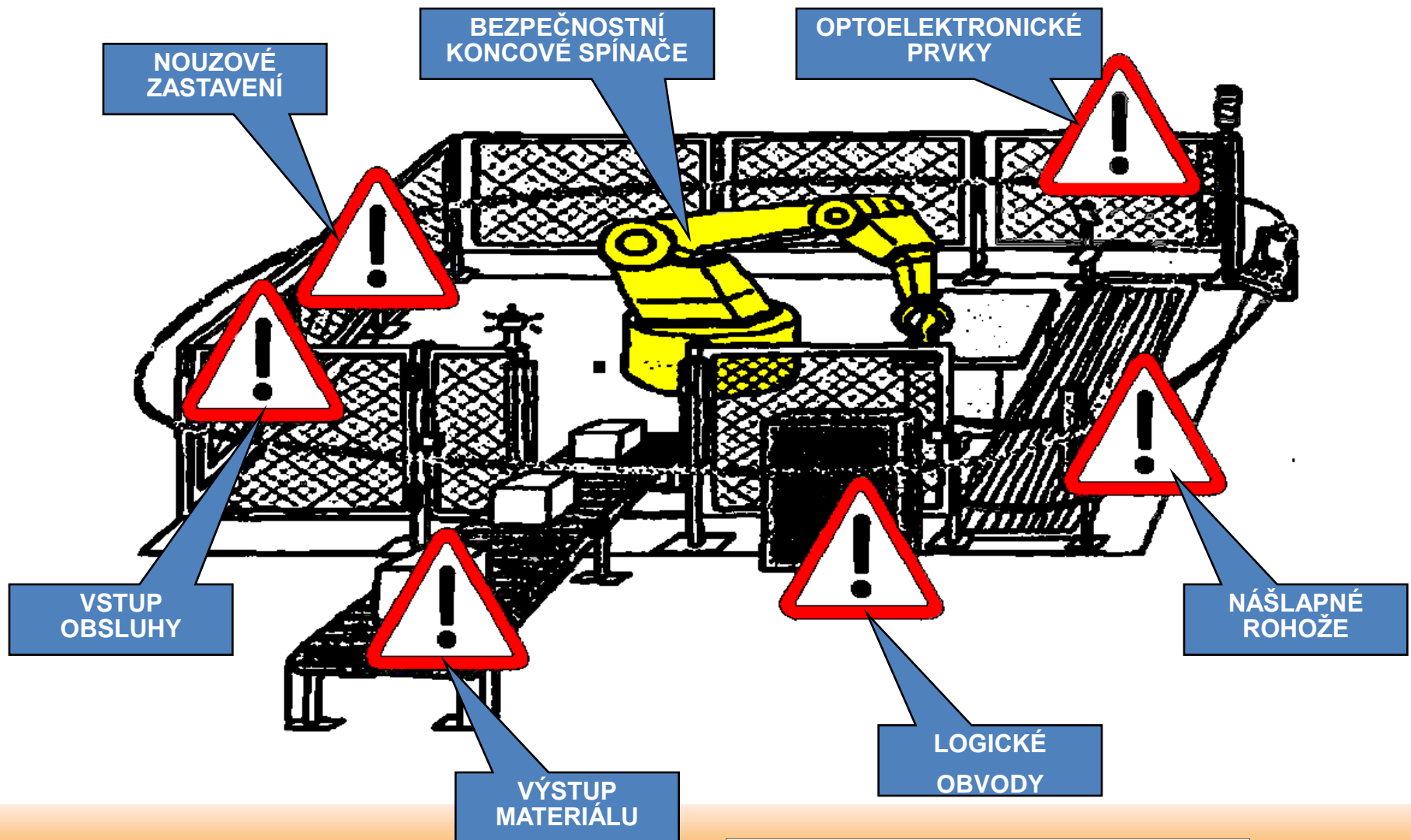
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Definujme situaci



15.10.2010

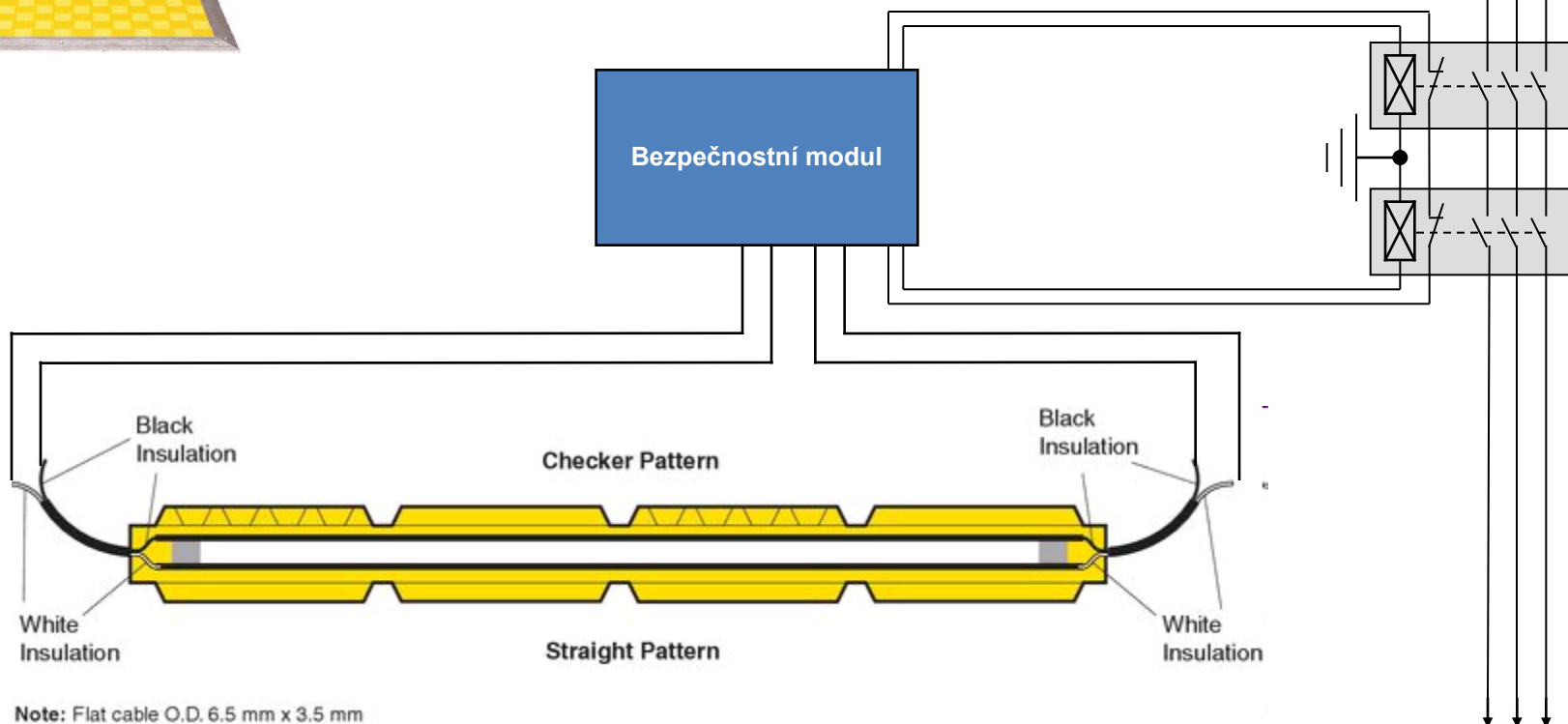
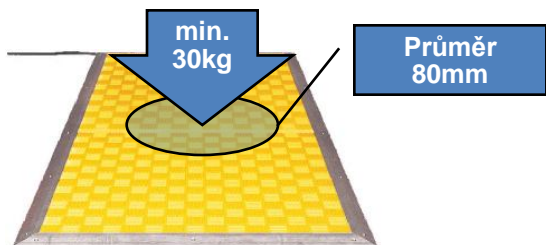


# Řešení diskrétními prvky

- + nejsou náklady na programování
- + cena
- daleko více propojování (cena, možnost chyby)
- mnoho místa v rozváděči
- možnost „zkopírovat“ aplikaci konkurencí



# Nášlapné rohože



15.10.2010

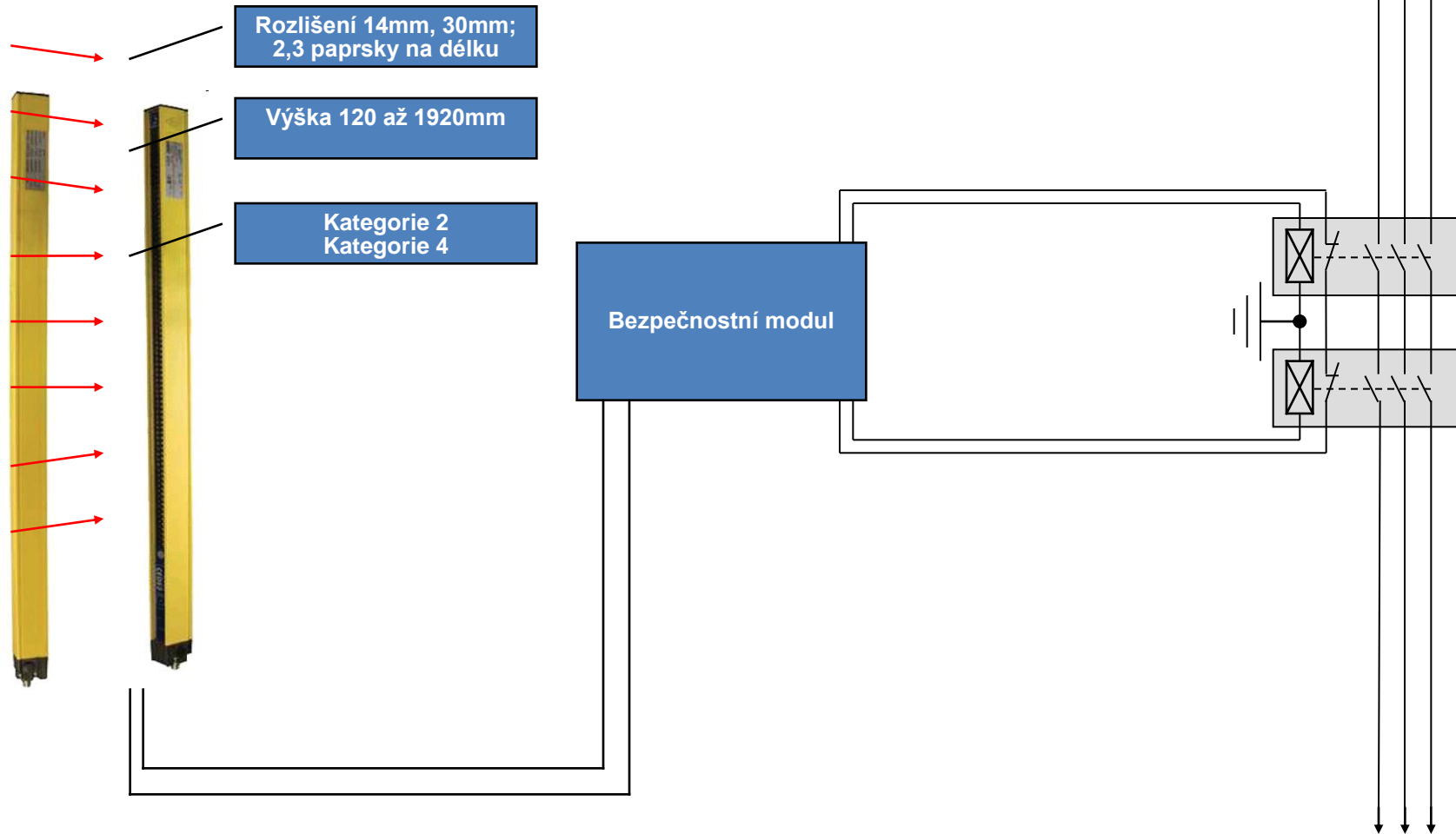
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ







# Světelné závory



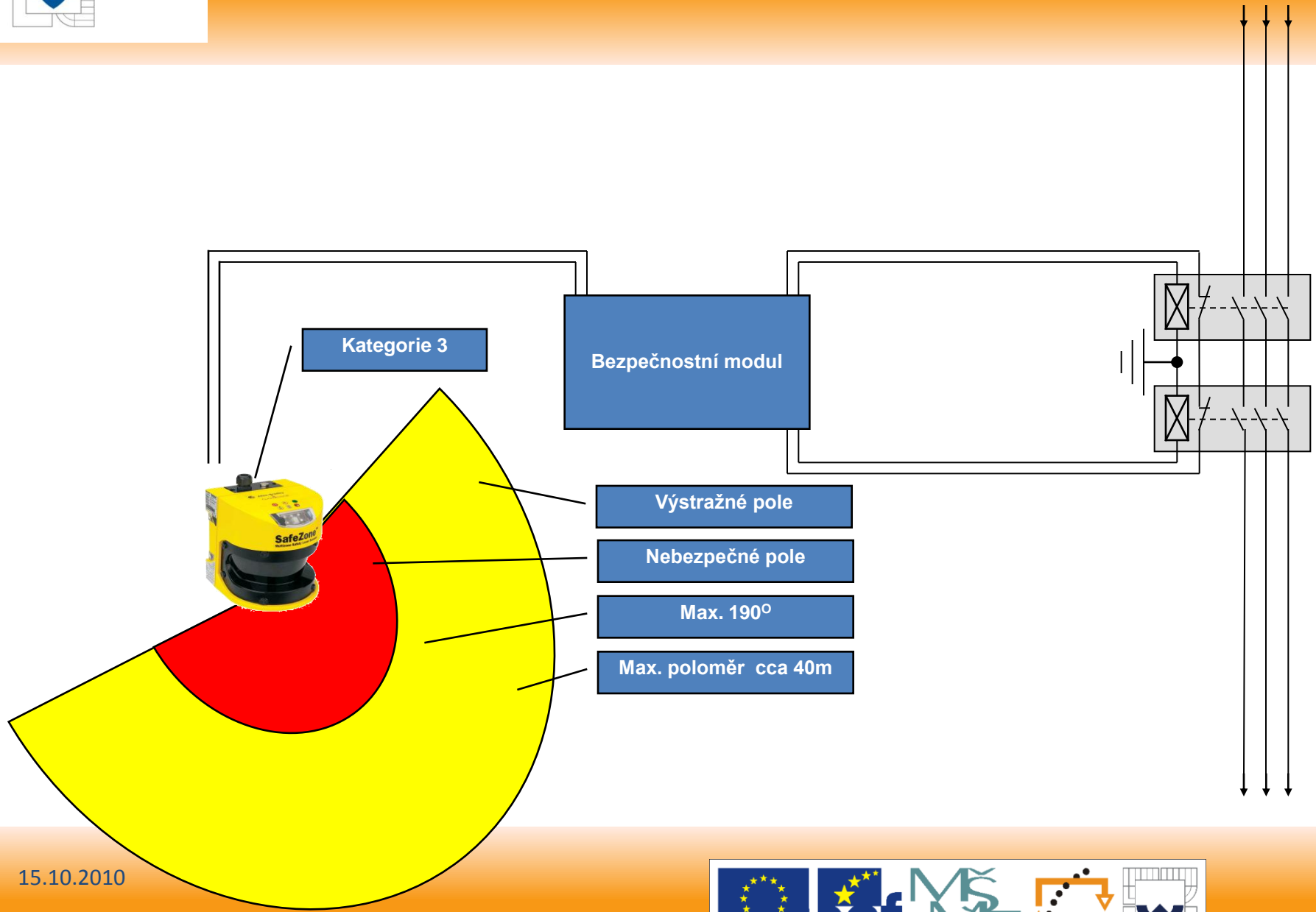
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





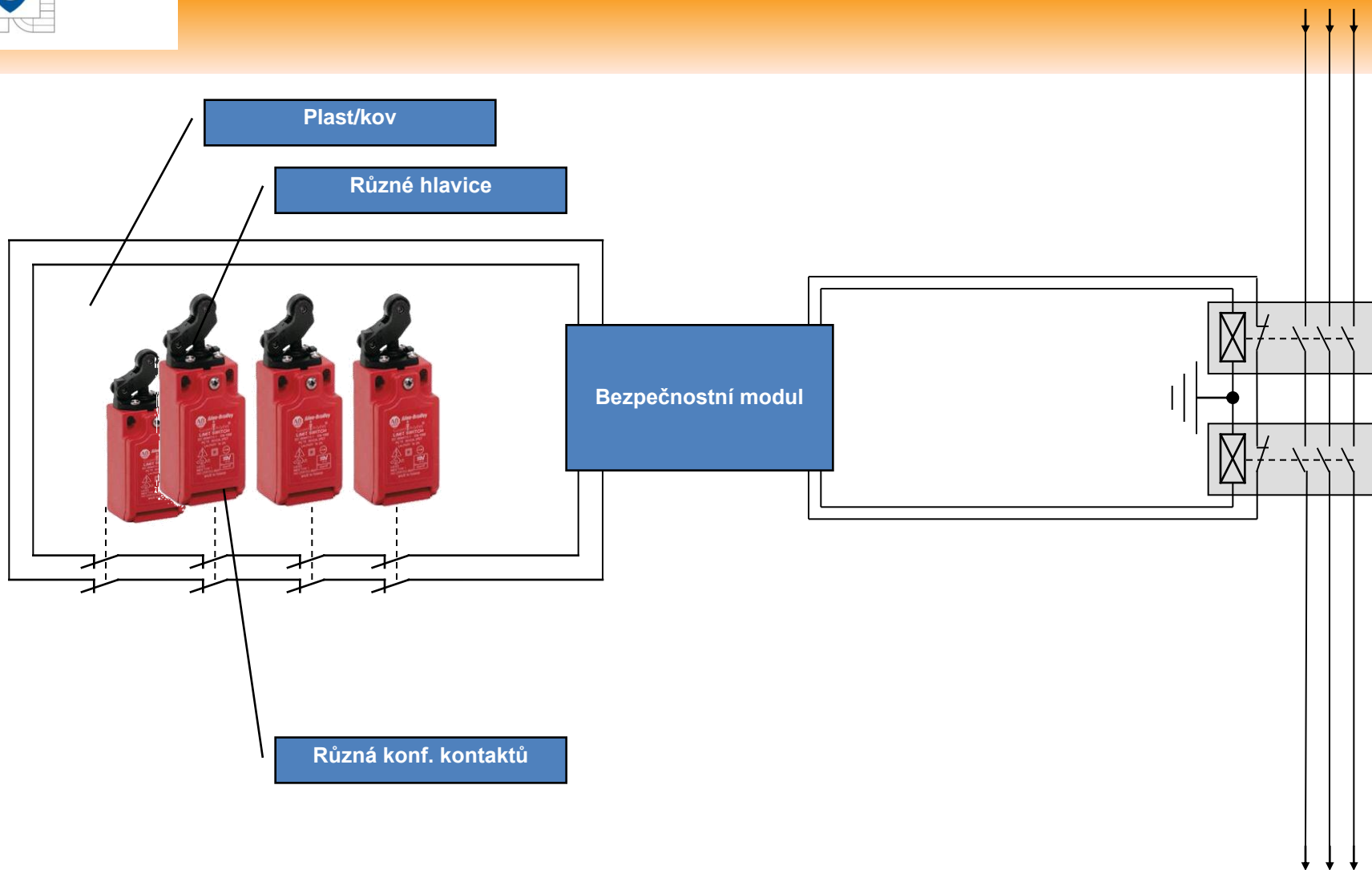
# Laserový scanner



15.10.2010



# Bezpečnostní koncové spínače



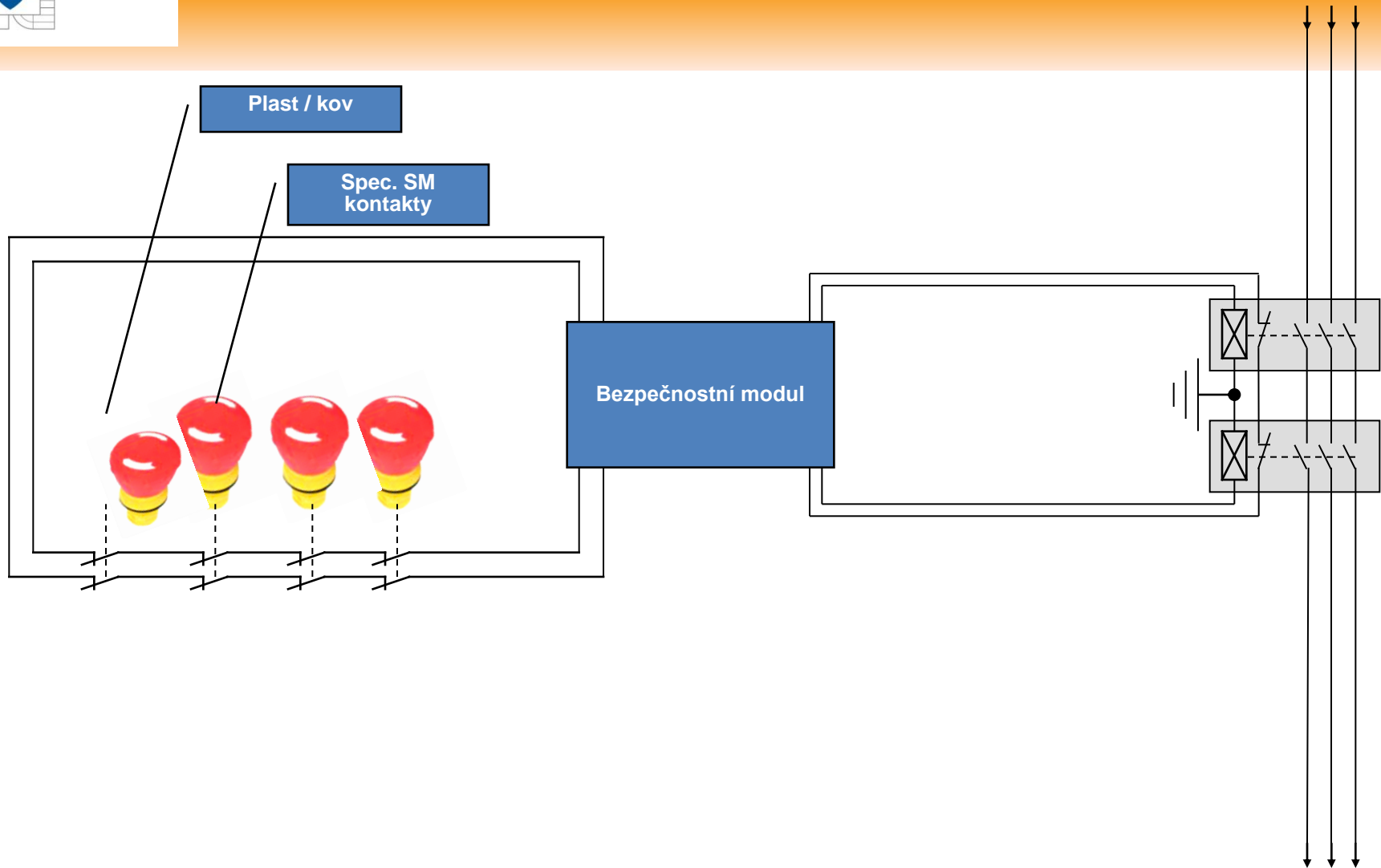
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





# Nouzové zastavení



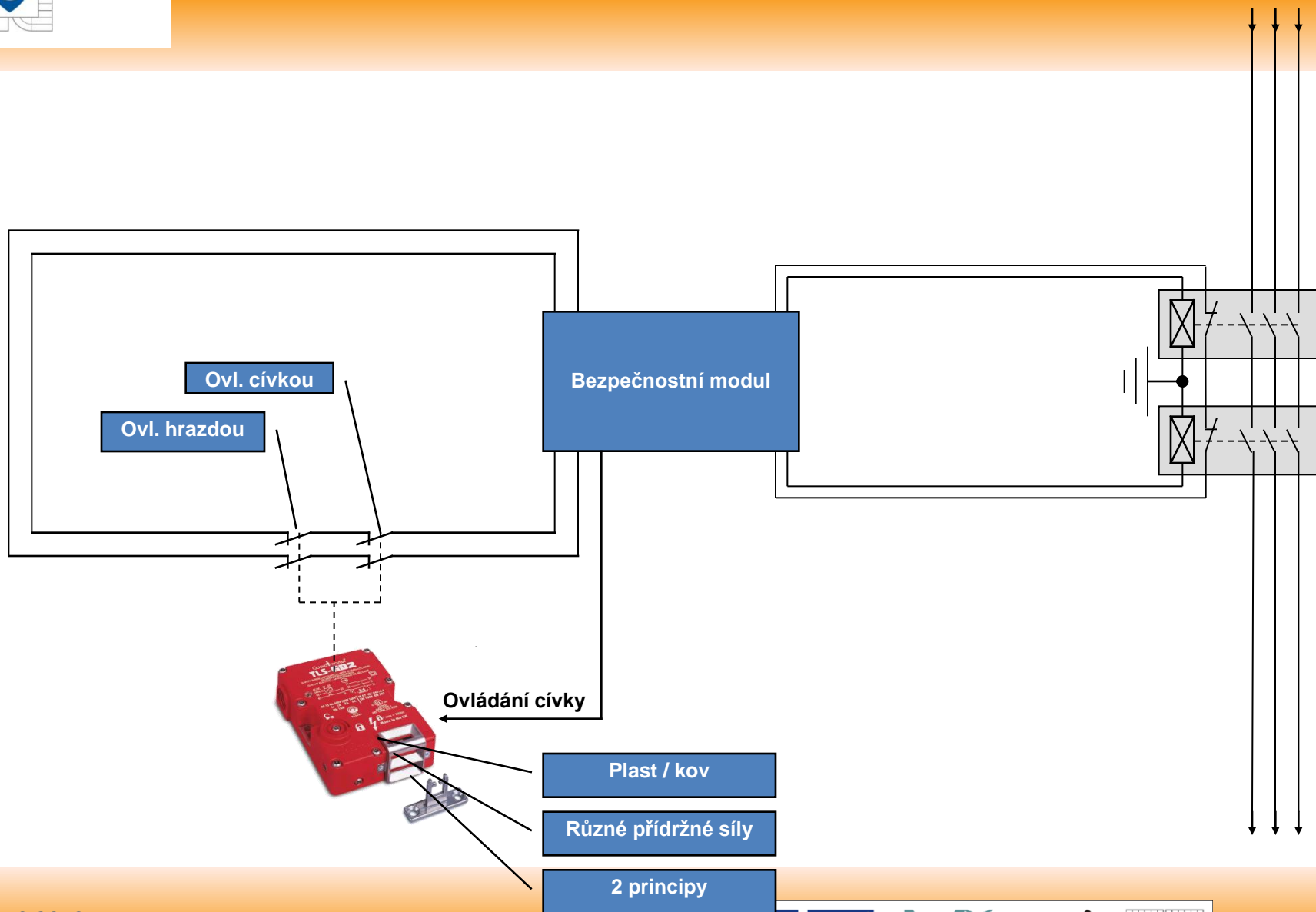
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





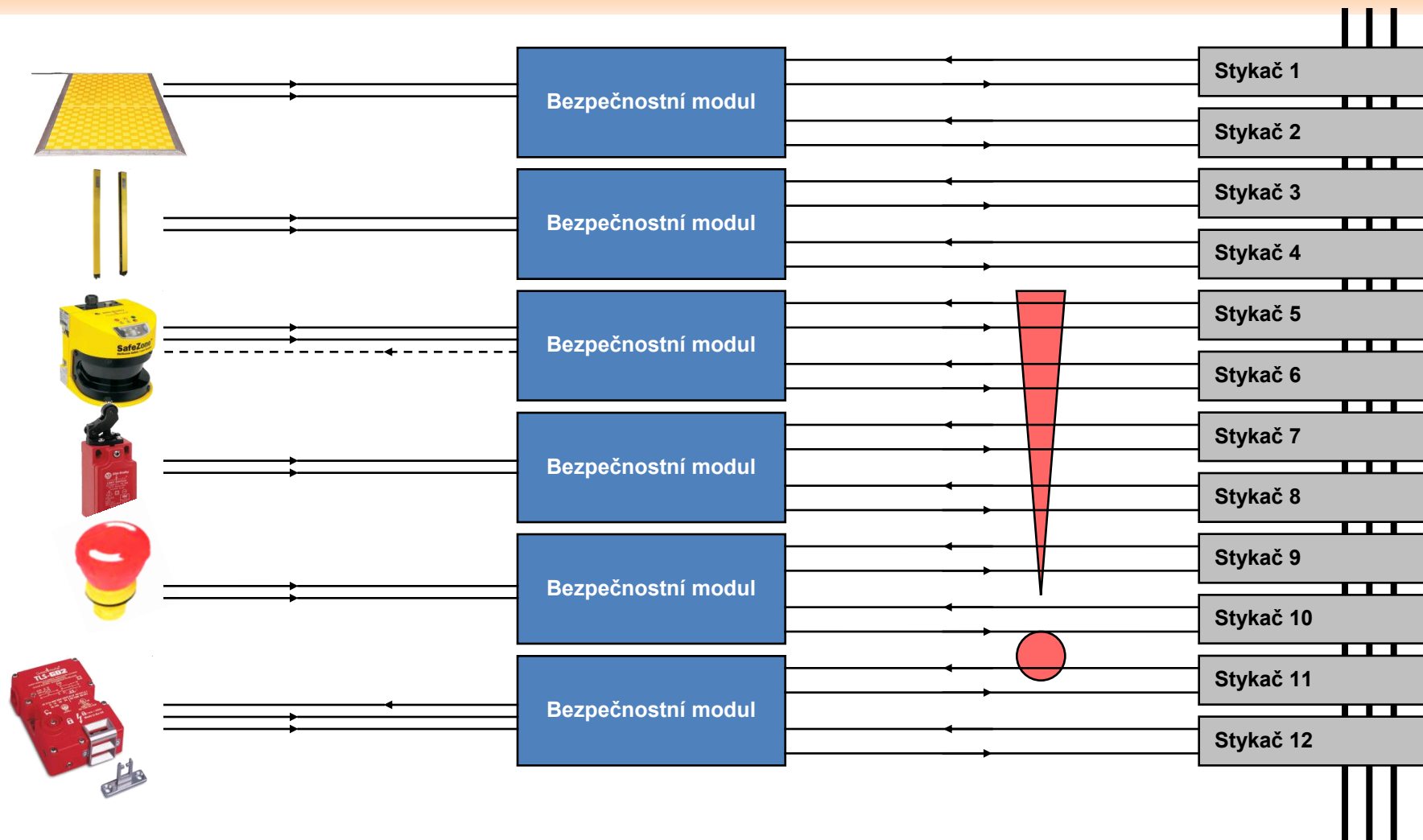
# Vstup obsluhy



15.10.2010



# Logické obvody – diskrétní řešení



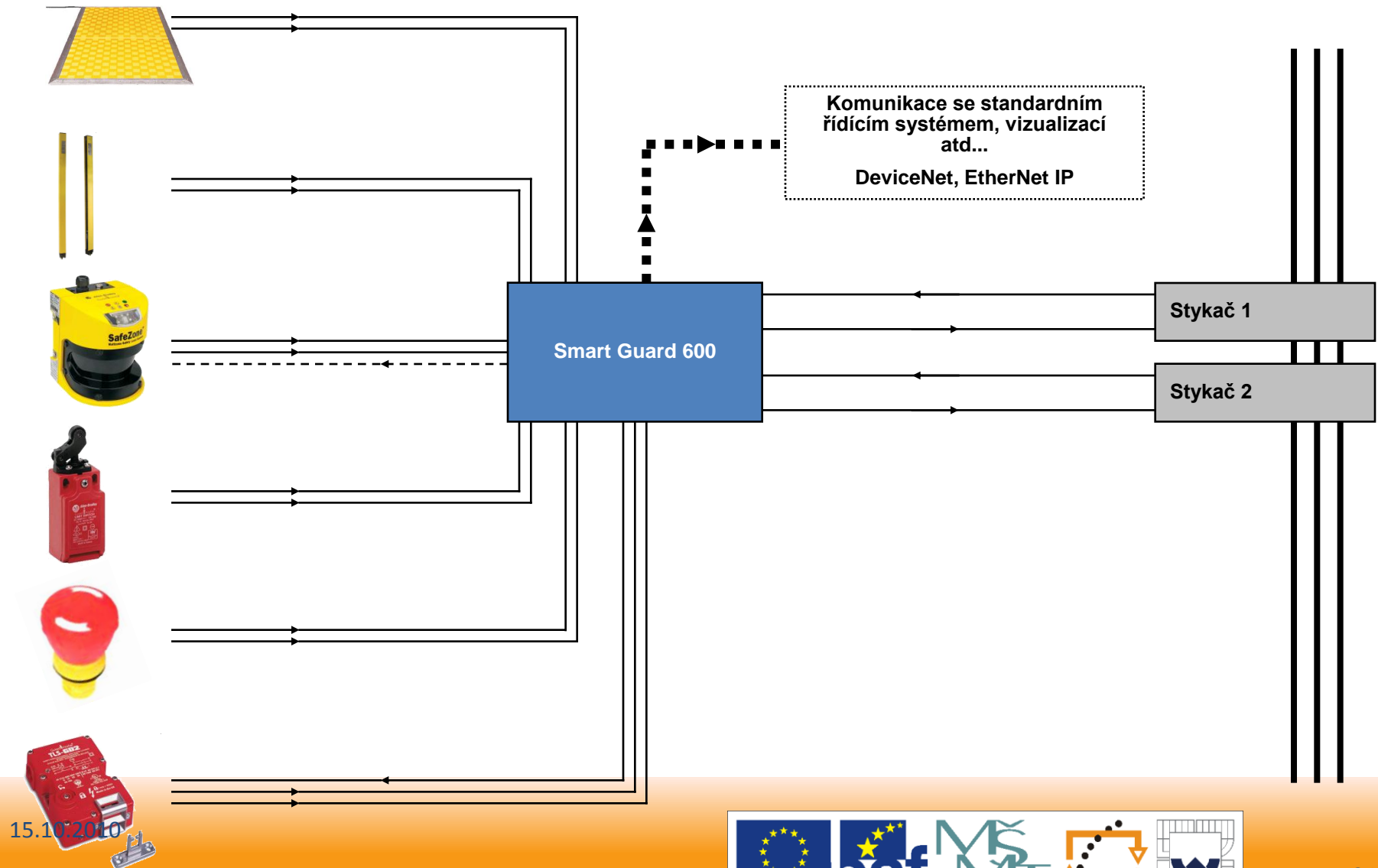
15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ





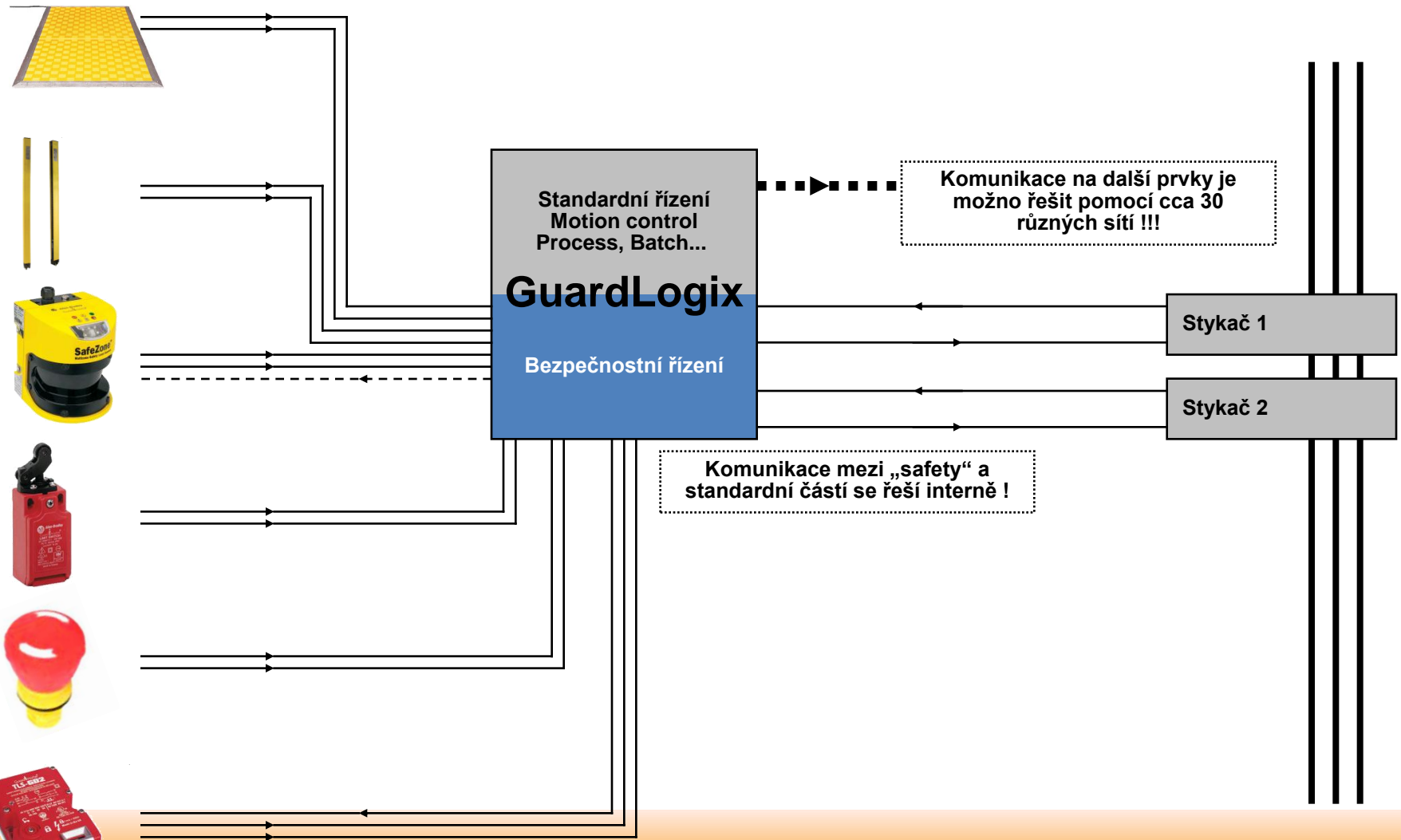
# Logické obvody – malé bezpečnostní PLC



15.10.2010



# Logické obvody – integrované bezpečnostní PLC



15.10.2010





Děkuji za pozornost...  
DOTAZY ?

15.10.2010

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

