

KRITERIA PRO STANOVENÍ SPOLEHLIVOSTI PROGRAMOVATELNÝCH SYSTÉMŮ A OVLÁDACÍCH PRVKŮ (PROJEKT Č. 54-07)

Anotace: Úkolem projektu výzkumu a vývoje P.č. 54-07 bylo „ Stanovení kritérií na spolehlivost programovatelných systémů měřicích, řídicích a bezpečnostních zařízení a na samočinnou kontrolu spolehlivosti ovládacích prvků“. Zadavatelem byl ČBÚ Praha, řešitelem VŠB-TU Ostrava a spoluřešitelem DIOS JEDLINK, s.r.o.

ABSTRACT: The aim of the project was a reliability criteria determination of programmable systems related to measurement, control and safety devices and determination of self-check of control components reliability. The assignment of the project originate from ČBÚ and is solved by VŠB-TU Ostrava in cooperation with DIOS company.

1. Úvod

Základními dokumenty zabývajícími se spolehlivostí technických zařízení, a to zejména z hlediska bezpečnosti, jsou technické normy. Při řešení funkční spolehlivosti programovatelných systémů pro měřicí, řídicí a bezpečnostní zařízení, což je úkolem tohoto projektu, nás zajímají zejména normy zabývající se spolehlivostí a bezpečností. Tyto normy tvoří skupinu tzv. bezpečnostních norem (safety standards), jejich obecná struktura je následující:

- a) Základní normy -normy typu A, (ČSN EN ISO 12100, ČSN EN ISO 14121) uvádějí základní pojmy, zásady pro konstrukci a všeobecná hlediska, která mohou být aplikována na všech strojních zařízeních.
- b) Skupinové bezpečnostní normy -normy typu B,(ČSN EN ISO 13849-1, ČSN EN 62061, ČSN EN 60204-1), se zabývají jedním nebo více bezpečnostními hledisky nebo jedním nebo více typy ochranných zařízení, která mohou být použita pro větší počet strojních zařízení:
 - normy typu B1 se týkají jednotlivých bezpečnostních hledisek (např. bezpečných vzdáleností, teploty, povrchu, hluku);
 - normy typu B2 se týkají příslušných bezpečnostních zařízení.
- c) Bezpečnostní normy pro stroje -normy typu C, určují detailní bezpečnostní požadavky pro jednotlivý stroj nebo skupinu strojů.

Pro stanovení funkční bezpečnosti elektrických, programovatelných elektronických systémů jsou nejdůležitější následující normy viz i obr. 1.

2. Určení rizik a jejich odstranění

Prvním krokem procesu vedoucím ke snižování rizik je jejich analýza. Je to proces definování hrozeb a nebezpečí, pravděpodobnosti jejich uskutečnění a dopadu na bezpečnost osob, technologického procesu i na zkoumané zařízení.

Zásadně musí být nebezpečí ohrožení zdraví vyloučeno nebo omezeno již při návrhu a konstrukci strojního zařízení. Dále musí následovat snížení rizika bezpečnostní ochranou i

doplňkovými ochrannými opatřeními a nakonec informacemi o zbytkovém riziku. Co se týče nebezpečí, která nelze vyloučit, musí být přijata nezbytná opatření a uživatel musí být informován o nebezpečích, která přes přijatá opatření přetrvávají. Při navrhování a výrobě strojního zařízení a při zpracování návodu k používání je důležité, aby konstruktér předvídal nejen běžné používání strojního zařízení, ale i další způsoby použití, které lze rozumně předpokládat. Strojní zařízení musí být navrženo tak, aby se předešlo jinému než běžnému použití, jestliže by takovým použitím mohlo vznikat riziko. Nelze-li jiné než běžné použití strojního zařízení vyloučit, musí návod k používání upozornit uživatele na způsoby, jak se má zařízení používat.

Pro identifikaci a stanovení rizikových situací vedoucích k ohrožení osob a majetku uvádí normy uvedené na obr.1 požadovaná bezpečnostní opatření pro konstrukci, provedení i provoz technických zařízení a strojů. Toto je dosaženo:

- identifikací rizika,
- stanovením rizikovosti,
- vyloučením a minimalizací rizikovosti vč. popisu řešení a stanovení zkušebních kritérií,
- informacemi pro používání.

Obdobný postup by měl být prováděn i u starších strojů při změnách.

Postup při posuzování rizika by měl být následující – obr. 2.

3. Určení schopnosti bezpečnostní části ovládacího systému k vykonávání bezpečnostní funkce podle ČSN EN ISO 13849-1.

Určení bezpečnostních funkcí je možno provést buď podle ČSN EN ISO13849-1 nebo ČSN EN 62061. Tyto normy používají různé klasifikační systémy a postup stanovení bezpečnosti je různý, ale výsledky jsou použitelné a srovnatelné.

Schopnost bezpečnostních částí ovládacího systému k vykonávání bezpečnostní funkce je podle ČSN EN ISO13849-1 rozdělena do pěti úrovní, které se nazývají úrovně vlastností (PL). Úrovně vlastností jsou definovány pravděpodobností nebezpečné poruchy za hodinu – tab. 1. Bezpečnostní části ovládacího systému (SRP/CS) vykonávají bezpečnostní funkce s úrovní vlastností (PL), kterou se dosáhne požadovaného snížení rizika. Úrovně vlastností se vztahují na ovládací části bezpečnostních systémů, jako: ochranná zařízení elektrická nebo citlivá na tlak, ovládací jednotky, prvky silového ovládnání apod.

PL	Průměrná pravděpodobnost Nebezpečné poruchy za hod. (1/h)
A	$\geq 10^{-5}$ až $< 10^{-4}$
B	$\geq 3 \times 10^{-6}$ až $< 10^{-5}$
C	$\geq 10^{-6}$ až $< 3 \times 10^{-6}$
D	$\geq 10^{-7}$ až $< 10^{-6}$
E	$\geq 10^{-8}$ až $< 10^{-7}$

Tab. 1

Úroveň vlastností (PL) bezpečnostní části ovládacího systému (Tab.1) musí být určena odhadem následujících parametrů:

- hodnoty střední doby do nebezpečné poruchy ($MTTF_d$) pro každou součást (dána výrobcem, stanovená výpočtem nebo se zvolí 10 roků),
- diagnostického pokrytí (DC),
- poruchy se společnou příčinou (CCF),
- struktury (architektury),
- chování bezpečnostní funkce v případě závady:
 - bezpečnostního software,

- systematické poruchy,
- schopnosti vykonávat bezpečnostní funkci v očekávaném prostředí.

Střední doba do nebezpečné poruchy ($MTTF_d$)

Doba	Rozsah doby
Krátká	$3 \leq MTTF_d < 10$ roků
Střední	$10 \leq MTTF_d < 30$ roků
Dlouhá	$30 \leq MTTF_d < 100$ roků

Tab. 2

Hodnota střední doby do nebezpečné poruchy ($MTTF_d$) je dána ve třech úrovních – Tab. 2. Maximální hodnota může být 100 let.

Diagnostické pokrytí (DC) je určeno pro čtyři úrovně:

Označení	Rozsah
Žádné	$DC < 60\%$,
Nízké	$60\% \leq DC < 90\%$
Střední	$90\% \leq DC < 99\%$
Vysoké	$99\% \leq DC$

Tab. 3

Kritéria pro posouzení schopnosti odolávat závadám:

- v důsledku závady neselžou další součásti,
 - dvě nebo více závad se společnou příčinou (CCF) musí být uvažovány jako jediná závada,
 - současný výskyt dvou nebo více závad, které mají samostatné příčiny, je považován za vysoce nepravděpodobný a proto výskyt takových závad neuvažujeme.
- Vyloučení závady je kompromisem mezi bezpečnostními požadavky a teoretickými možnostmi výskytu závady. Vyloučení závady musí být založeno na:
- technické nepravděpodobnosti výskytu,
 - obecně přijatelné zkušenosti,
 - požadavcích týkajících se použití a specifického nebezpečí.

Struktura (konstrukce či architektura) bezpečnostních částí

Znázornění kombinace bezpečnostních částí ovládacích systémů je na obr.3. Obvykle je to spojení vstupu -I, logické jednotky -L, výstupu -O a propojovacích prostředků i_x . Pod pojmem start v obr. 3 si můžeme představit např. stisk tlačítka nebo otevření krytu apod. Většina struktur bezpečnostních částí ovládacích systémů u strojního zařízení může být zařazena do typických bezpečnostních blokových schémat podle kategorií (B,1-4). Architektura na obr. 3 platí pro kategorii B a také pro kategorii 1 s tím, že na části systému musí být použity osvědčené součásti a zásady.

Dále jsou stanoveny architektury pro kategorie 2, 3 a 4.

Určení požadované úrovně vlastností (PL_r)

Úroveň vlastností (PL) může být dosaženo ohodnocením velikosti rizika a jeho snížením.

Při posouzení rizika je nutno brát v úvahu:

- Závažnost zranění (lehké S1, těžké nebo smrt S2).
- Četnost a dobu vystavení nebezpečí (čas od času F1, často nebo nepřetržitě F2 – někdy se uvádí častěji než 1x za hodinu).
- Možnost vyloučení nebezpečí (reálná možnost P1, žádná možnost vyloučení P2).

Podle této normy musí být pro každou bezpečnostní funkci provedeno grafické znázornění požadované úrovně vlastností (PL_r) vztahující se k bezpečnosti - obr. 4 (L je malé přispění a H je velké přispění ke snížení rizika). Na obr. 5 je červeně vyznačen příklad hodnocení úrovně vlastností tlumivky pro kompenzaci zemních zkratů.

Úroveň vlastností PL "c" $\geq 10^{-6}$ až $< 3 \cdot 10^{-6}$ – c je průměrná pravděpodobnost nebezpečné poruchy za hodinu.

Nyní by následovalo stanovení $MTTF_d$ z např. podle tab. C6 normy, doby činnosti, diagnostického pokrytí a srovnání úrovně vlastností PL s požadovanou úrovní PL_r . Pokud $PL \geq PL_r$ je snížení rizika dostatečné.

4. Určení požadavků na bezpečnou funkci elektrických řídicích systémů souvisejících s bezpečností strojů (SRECS) podle ČSN EN 62061.

Tato norma je určena pro konstruktéry strojního zařízení, výrobce řídicích systémů, montážní pracoviště a ostatní pracovníky, kteří se podílejí na specifikaci, návrhu a potvrzení platnosti SRECS (Elektrický řídicí systém související s bezpečností). Stanovuje postupy a požadavky pro dosažení požadované funkce. Norma poskytuje metodiku a požadavky pro:

- stanovení požadované integrity bezpečnosti pro každou řídicí funkci související s bezpečností, která má být v rámci SRECS realizována;
- umožnění návrhu SRECS odpovídajícího stanoveným řídicím bezpečnostním funkcím;
- začlenění podsestav vztahujících se k bezpečnosti podle ČSN ISO 13849;
- potvrzení platnosti (validace) SRECS.

Požadavky na úroveň integrity bezpečnosti (SIL) SRECS musí být odvozeny od vyhodnocení rizika a to tak, aby bylo zajištěno jeho nutné omezení. Potřebný stupeň SIL je určen na základě vzájemného vztahu mezi důsledky rizikového stavu (třeba zkratu) a pravděpodobnosti výskytu zkratu. Hodnocení může být částečně kvantitativní - přiřadí se stupeň ohrožení a intenzita výskytu ohrožení. Intenzita ohrožení se určí buď podle dosavadního provozu zařízení a to slovně (často, ...nepravděpodobně) a přiřadí se počet poruch za delší časové období (20roků) a dále se určí hodnoty FIT (failures in time unit): FIT je $10^{-9}/h$, obvykle podle údajů výrobců.

Kvantitativní hodnocení se provede výpočty zda splňuje požadovanou úroveň SIL. Požadavek na SIL je podle této normy pro každý elektrický řídicí systém vyjádřen cílovou mírou poruch.

Úroveň integrity bezpečnosti SIL	Pravděpodobnost nebezpečné poruchy za hodinu (PFH_D)
3	$\geq 10^{-8}$ až $< 10^{-7}$
2	$\geq 10^{-7}$ až $< 10^{-6}$
1	$\geq 10^{-6}$ až $< 10^{-5}$

Odhad rizika a přiřazení SIL se odvozuje od:

- závažnosti škody (Se) a
- pravděpodobnosti výskytu škody, která závisí na
 - .. četnosti a doby trvání ohrožení osob nebezpečím (Fr)
 - .. pravděpodobnosti výskytu nebezpečných událostí (Pr)
 - .. možnosti vyvarování se nebo omezení škody (Av).

Závažnost škody se odhaduje z míry zranění	Se
smrtelné zranění nebo trvalé následky	4
těžká zranění s trvalými následky	3

zranění s přechodnými následky	2
lehká zranění	1

Četnost a doba trvání ohrožení (Fr)

Četnost	Doba trvání >10min
≤ 1h	5
> 1 h až ≤ 1 den	5
> 1 den až ≤ 2 týdny	4
> 2 týdny až ≤ 1 rok	3
> 1rok	2

Pravděpodobnost výskytu nebezpečných událostí	Pr
velmi vysoká	5
pravděpodobná	4
možná	3
výjimečná	2
zanedbatelná	1

Pravděpodobnost vyvarování se nebo omezení škody (Av)	Av
nemožná	5
možná za určitých okolností	3
pravděpodobné	1

Pro každé nebezpečí a pokud přichází v úvahu pro každý stupeň závažnosti škody vypočteme třídu pravděpodobnosti škody CI

$$CI = Fr + Pr + Av$$

Pro určení SIL pak použijeme závažnost Se a CI

Závažnost Se	Třída CI				
3-4	5-7	8-10	11- 13	14-15	
SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	
	jiné	SIL 1	SIL 2	SIL 3	
		jiné	SIL 1	SIL 2	
			jiné	SIL 1	

Příklad odhadu rizika dopravního pásu

Číslo	Nebezpečí	Se	Fr	Pr	Av	CI
1	Zachycení	3	4	3	3	10
2	Pád na pás	4	2	2	1	5
3	Odření	2	5	2	3	10
Se		CI				
		3-4	5-7	8-10	11- 13	14-15
4		SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3			jiné	SIL 1	SIL 2	SIL 3
2				jiné	SIL 1	SIL 2
1					jiné	SIL 1

Určení SIL výpočtem

Na základě určení odolnosti proti vadám (schopnosti SRESC, subsystému nebo prvku subsystému, pokračovat v plnění požadované funkce i za přítomnosti vad nebo chyb), se stanoví architektura subsystému. Rozeznávají se čtyři architektury subsystému A,B,C,D. Určí se pravděpodobnost výskytu nebezpečné náhodné poruchy subsystémů z nichž je celý systém složen.

Pro subsystém A platí:

$$\lambda = \frac{0,1.C}{B_{10}}$$

Kde λ je celková intenzita poruch, C je počet provozních cyklů, B_{10} je počet cyklů do 10% nebezpečných selhání.

Intenzita nebezpečných poruch $\lambda_D = \lambda - \lambda_S$, kde λ_S je intenzita bezpečných poruch

Pro všechny prvky subsystému A

$$\lambda_{DA} = \lambda_{De1} + \dots + \lambda_{Den}$$

Střední pravděpodobnost nebezpečné poruchy za hodinu je pak

$$PFH_{DA} = \lambda_{DA} \times 1h$$

5. Výpočet spolehlivosti elektrických prvků a elektronických součástí podle MIL-HDBK-217-D /1/,/2/

Pokud chceme stanovit pravděpodobnost poruchy nějakého systému, musíme začít u jednotlivých jeho prvků, což v případě elektronických zařízení jsou polovodičové součástky, odpory, kondenzátory, konektory apod. I když tyto součástky jsou správně dimenzovány, dochází u nich k poruchám z vnějších i vnitřních příčin. Zkoumání takových dějů se může dít modelováním, ovšem nikdy nepostihneme působení všech degradačních dějů jak v časových souvislostech, tak i z hlediska velikosti namáhání. Proto se používá výpočet pravděpodobnosti poruchy, kdy intenzita poruch určená jako referenční se upravuje koeficienty respektující zatížení v provozu, okolní prostředí, mechanické namáhání apod.

Spolehlivost těchto prvků je vhodné vyjadřovat intenzitou poruch. Tato hodnota závisí na parametrech vnějšího i vnitřního prostředí, druhu a způsobu souhrnného namáhání, způsobu výroby a zvládnutí technologie.

Toto konstatování je možno vyjádřit vztahem

$$\lambda_p = \pi_Q \sum \lambda_{bi} \cdot \pi_{ij}$$

- kde λ_p je provozní intenzita poruch v hod^{-1}
- π_Q je součinitel kvality závislý na úrovni řízení jakosti při výrobě
- λ_{bi} je základní intenzita poruch způsobených i-tým mechanismem
- π_{ij} je součin činitelů, vyjadřujících vliv j-tého faktoru (prostředí, elektrické namáhání) na intenzitu poruch vyvolaným i-tým mechanismem vzniku poruch.

Vedle uvedených norem existuje ještě řada norem speciálních např.

ČSN EN 1088 +A2: Bezpečnost strojních zařízení - Blokovací zařízení spojená s ochrannými kryty - Zásady pro konstrukci a volbu.

ČSN EN ISO 13850: Bezpečnost strojních zařízení - Nouzové zastavení - Zásady pro konstrukci atd.

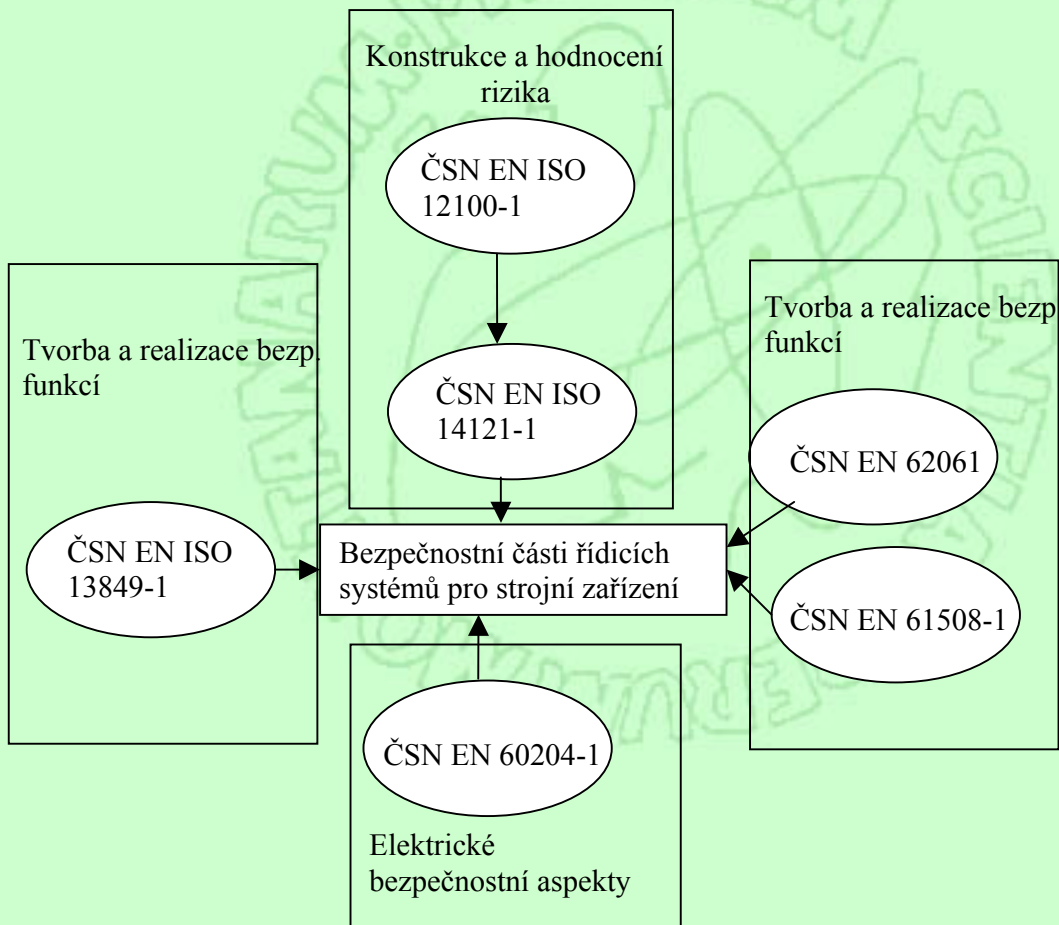
7. Závěr

Výsledkem řešení tohoto úkolu budou návrhy nových znění paragrafů a odstavců či návrhy doplnění nových paragrafů a odstavců vyhlášek v kompetenci orgánů státní báňské správy. Jedná se např. o vyhlášky: č. 22/1989 Sb., 26/1989 Sb., 51/1989 Sb.,

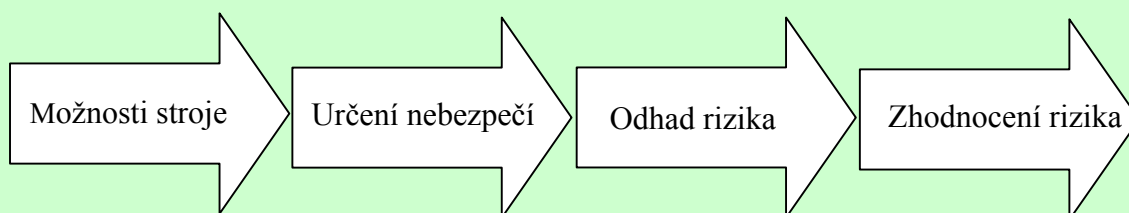
55/1996 Sb., atd. Půjde pouze o požadavky vázané na systémy související s bezpečností zařízení.

Literatura:

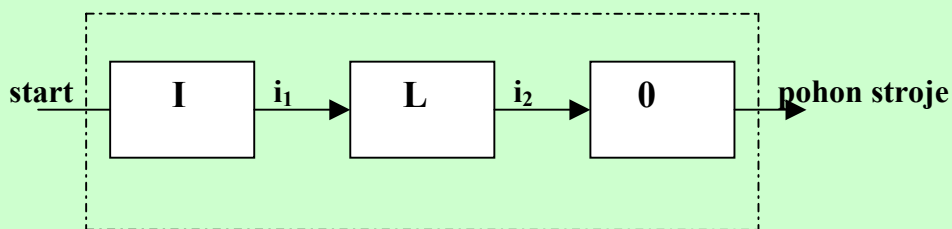
- [1] ČSN EN ISO 12100-1: Bezpečnost strojních zařízení - Základní pojmy, všeobecné zásady pro konstrukci
- [2] ČSN EN ISO 14121-1: Bezpečnost strojních zařízení- Posuzování rizika
- [3] ČSN EN ISO 13849-1: Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Všeobecné zásady pro konstrukci
- [4] ČSN EN 60204-1: Bezpečnost strojních zařízení – Elektrická zařízení strojů – Část 1: Všeobecné požadavky
- [5] ČSN EN 62061 Bezpečnost strojních zařízení: Funkční bezpečnost elektrických, a programovatelných elektronických řídicích systémů souvisejících s bezpečností
- [6] ČSN EN 61508-1: Funkční bezpečnost elektrických, elektronických programovatelných elektronických systémů souvisejících s bezpečností



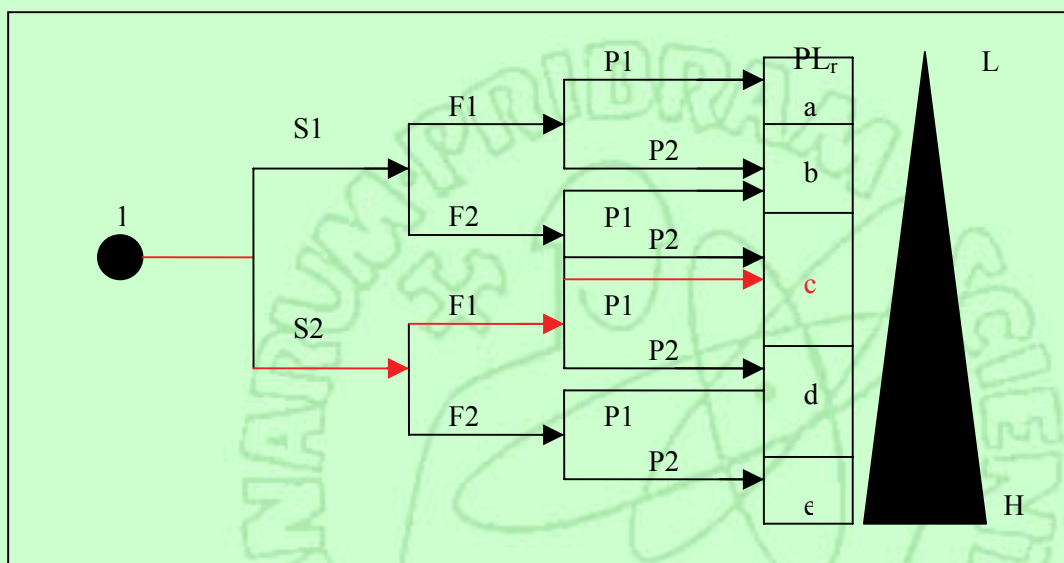
Obr. 1 Normy o bezpečnosti



Obr. 2 Posuzování rizika



Obr. 3 Bezpečnostní části ovládacího systému



Obr.4 Určení požadované úrovně vlastností.



Obr.5 Znáznornění subsystému A