Ročník 2009 electroscope Číslo II

Zajištění bezpečného chodu strojů a zařízení

Chmelík K., Koziorek J.
FEI VŠB-TU Ostrava

Anotace
There always exists certain risk in operation of any equipment that will not work reliable or with failures presence. For overall risk minimization of an item we have to use protective devices with safety function performed. Diagnostic coverage is a measure of diagnostics efficiency in principle, and can be included in protective devices.

ÚVOD

Provozované stroje a zařízení mohou při poruše představovat jistá rizika pro zdraví či životy lidí, ale i pro okolní prostředí. Poruchy mohou být zapříčiněny buď vadami strojů, chybami v projekci či obsluze strojů nebo působením vnějšího prostředí. Poruchám je tedy nutno předcházet a to nejlépe již při návrhu bezpečné činnosti, návrhem ochranného systému, diagnostikou a vytvořením bezpečnostní strategie.

ZAJIŠTĚNÍ BEZPEČNÉHO PROVOZU ZAŘÍZENÍ

Nebezpečí lze definovat jako nenadálé ohrožení života nebo majetku či nepřípustnou kombinaci nebezpečnosti a rizika, která vznikla porušením bezpečnostech opatření. Existují dvě formy nebezpečí :
- nepřijatelná forma,
- přijatelná forma.

První forma vzniká při závažném porušení bezpečnostech opatření, nedbalosti, nedostatečné ochraně a vede k vážným úrazům nebo i smrti. Druhá forma je ospravedlnitelná při mimořádných událostech např. záchranných akcí. Pro celkové snížení rizika objektu musíme použít ochranných zařízení, která budou plnit bezpečnostní funkci. Mluvíme pak o bezpečnostní části systému, která bude reagovat na bezpečnostní vstupní signály a vytvářet bezpečnostní výstupní signály /2/. K bezpečnostní části systému mohou patřit ochranná zařízení, ovládací jednotky i prvky silového ovládání. Jedná se tedy o relé, snímače polohy, čidla tlaku, teploty, programovatelné elektronické ochrany apod. K ochranným zařízením můžeme počítat rovněž diagnostické pokrytí, což je vlastně mírou účinnosti diagnostiky.
Bezpečnost složitých systémů je zajišťována prostřednictvím několika ochranných systémů založených na různých technických principech např. mechanických, elektrických, programovatelných elektronických apod. Tedy mnohé elektrické a elektronické součásti a přístroje mohou vedle svých běžných funkcí plnit i bezpečnostní funkce ve složitých systémech. Je však nutno mít jistá pravidla, podle nichž je možné posoudit zda požadované bezpečnosti sytému bude dosaženo. K tomuto účelu je možno použít řadu technických norem, které řeší bezpečnost zařízení pro jeho celý životní cyklus.
Riziko chápeme jako četnost výskytu nebezpečné události a jejího následku. Je tedy nutné posoudit velikost rizika, navrhnout prostředky pro jeho snížení a určit také velikost zbytkového rizika. Existuje tedy riziko procesu, přijatelné riziko a zbytkové riziko. Ke snížení velikosti rizika nám mohou sloužit běžná bezpečnostní opatření (zábrany, kryty, poučení osob), anebo jsou realizovány přístrojové bezpečnostní systémy k dosažení nebo udržení bezpečného procesu a snížení rizika.
Všeobecné zásady pro posouzení rizika jsou uvedeny v /1/. Struktura bezpečnostních norem je uvedena ve /2/. Strategie pro snížení rizika je zde řešena určením pěti úrovní vlastností (PL), definovaných pravděpodobností nebezpečné poruchy za hodinu, střední dobou do nebezpečné poruchy a diagnostickým pokrytím. Norma popisuje požadavky na návrh a integraci řídicího systému souvisejícího s bezpečností, včetně určitých softwarových aspektů. Může být aplikován u systémů realizovaných pomocí různých technologií, včetně elektrické, hydraulické, pneumatické a mechanické.
Při posuzování velikosti rizika musíme provést analýzu při níž definujeme nebezpečí a nebezpečné situace s ohledem na dané zařízení, jeho okolí a ohrožení osob. Dále musíme odhadnout velikost rizika ze závažnosti možné škody, pravděpodobnosti výskytu škody, která je závislá na době trvání a četnosti výskytu ohrožení osob nebezpečím.
Při posouzení rizika je nutno brát v úvahu:
- závažnost zranění (lehké S1, těžké nebo smrt S2)
- četnost a doba vystavení nebezpečí (čas od času F1, často nebo nepřetržitě F2)
- možnost vyloučení nebezpečí (reálná možnost P1, žádná možnost vyloučení P2)

Úroveň vlastností: a,b,c,d,e určuje schopnost bezpečnostních částí ovládacího systému k vykonávání bezpečnostní funkce. Je vyjádřena pravděpodobností nebezpečné poruchy za hodinu (např. a- ≥10-5 až < 10-4, e- ≥10-8 až < 10-7).
Další metoda návrhu bezpečnostního systému je popsána ve /4/. Jde o aplikací pro oblast strojních zařízení. Je vhodná zejména pro případy, kdy je vyžadován komplexní systém pro zajištění funkční bezpečnosti, realizovaný zejména programovatelným prostředkem, ale lze využít i pro jednoduché systémy. Tato norma je omezena na elektrické, elektronické a programovatelné elektronické systémy. Zde jsou stanoveny 3 úrovně integrity bezpečnosti (SIL) a dále naznačeny metody pro určení požadované úrovně. Zavedený pojem integrity bezpečnosti je mírou pravděpodobnosti, že bezpečnostní přístrojové funkce a jiné ochranné prostředky dosáhnou stanovených bezpečnostních funkcí.
Funkce související s bezpečností musí být zdokumentovány a jejich popis musí obsahovat:
Specifikaci funkčních požadavků každé funkce – četnost, požadovanou časovou odezvu, popis funkce, počet provozních cyklů, podmínky stroje, kdy bude bezpečnostní funkce vyřazena apod.
Specifikaci požadavků integrity bezpečnosti každé funkce – požadavky na integritu bezpečnosti musí být předepsány pomocí úrovní SIL tj. pravděpodobností nebezpečné poruchy za hodinu.

Požadavky na úroveň integrity bezpečnosti (SIL) musí být odvozeny od vyhodnocení rizika a to tak, aby bylo zajištěno jeho nutné omezení. V této normě je požadavek na SIL pro každý elektrický řídící systém vyjádřen cílovou mírou poruch.

Úroveň integrity bezpečnosti SIL
Pravděpodobnost nebezpečné poruchy za hodinu (PFHD)
3- 10-8 až < 10-7
2- ≥10-7 až < 10-6
1- ≥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)
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
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

Vedle norem / 2/ a /4/ existuje další skupina norem zabývajících se funkční bezpečností přístrojových systémů pro sektor průmyslových procesů /5/ a také funkční bezpečností elektrických, elektronických programovatelných systémů souvisejících s bezpečností /6/. V /5/ jsou stanoveny 4 úrovně integrity bezpečnosti a dále naznačeny metody pro

určení požadované úrovně. Normy /5/ uvádějí možné postupy výpočtu pravděpodobnosti výskytu poruch, číselné hodnoty průměrné pravděpodobnosti poruch na vyžádání a četnost nebezpečných poruch.
Bezpečnostní přístrojový systém (SIS) se používá k realizaci jedné nebo více bezpečnostních přístrojových funkcí. Skládá se z různých senzorů (neprogramovatelných nebo programovatelných), logických automatů (neprogramovatelných nebo programovatelných) a koncových členů (neprogramovatelných nebo programovatelných). Bezpečnostní přístrojová funkce pro režim vyžádání je potřebná činnost (např. vypnutí stykače) související s reakcí na události v procesu. Zde je pak nutné určit pravděpodobnost poruchy přístroje, která způsobí, že již ona vyžádaná potřebná činnost nebude vykonána.
Norma /5/ mj. zavádí číselné hodnoty cílové průměrné pravděpodobnosti poruchy na vyžádání - PFD (vyžádání je jev, který způsobí, že diagnostická funkce řídicího systému vykoná svoji řídicí funkci související s bezpečností). Dále stanovuje četnost nebezpečných poruch za hodinu pro úrovně bezpečné integrity (SIL) a také stanovuje nejvyšší úroveň funkčnosti SIL 4.

ZÁVĚR

Účelem příspěvku bylo ukázat jaká pozornost je věnována zajištění bezpečného provozu strojů a zařízení. V současné době již řada výrobců elektrických i elektronických přístrojů a prvků i programovatelných zařízení uvádí potřebné hodnoty pro výpočet bezpečnostních funkcí. Jsou to např. střední doba do poruchy, intenzita nebezpečných poruch, pravděpodobnost poruchy na vyžádání, průměrná pravděpodobnost poruchy, hodnoty SIL apod. Všechny tyto údaje pak mohou posloužit projektantovi zařízení pro zajištění bezpečné funkce a omezení rizika při činnosti zařízení.

Tvorba příspěvku byla podpořena projektem ČBÚ č. 54-07.

LITERATURA

- ČSN EN ISO 14121-1 Bezpečnost strojních zařízení – Zásady pro posouzení rizika
- ČSN ISO 13849-1 Bezpečnost strojních zařízení – Bezpečnost ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci.
- ČSN EN ISO 12100-1 Bezpečnost strojních zařízení- Základní pojmy, všeobecné zásady pro konstrukci-Část 1: Základní terminologie, metodologie
- ČSN EN 62061 Bezpečnost strojních zařízení - Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností.
- ČSN EN 61511-1 až 3 Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů
- ČSN EN 615508-1 až 6 Funkční bezpečnost elektrických /elektronických/ programovatelných elektronických systémů souvisejících s bezpečností

Autoři
doc.Ing. Karel Chmelík, Katedra elektrických strojů a přístrojů, e-mail: *karel.chmelik@vsb.cz*
doc. Ing. Jiří Koziorek, PhD., Katedra měřicí a řídicí techniky, e-mail: jiri.koziorek@vsb.cz Fakulta elektrotechniky a informatiky, VŠB-TU Ostrava, 17. listopadu 15, 708 33 Ostrava – Poruba