K úrovni integrity bezpečnosti

František Babinec

V článku je přehledně shrnut současný přístup k zajišťování funkční bezpečnosti průmyslových technologických zařízení a procesů a je ukázáno jeho použití na konkrétním případu tlakové skladovací nádoby.

1. Úvod

Je známou skutečností, že velké bezpečnosti složitých procesů se ve většině případů efektivně dosahuje přihlédnutím k požadavkům na bezpečnost již ve fázi návrhu bezpečného procesu. Dodatečně zajišťovat bezpečnost procesu, zejména po mimořádné události, je vždy velmi nákladné. Pro zajištění vysoké úrovně bezpečnosti složitých zařízení se již mnoho let používají systémy regulace a bezpečnostní přístrojové systémy. K efektivnímu využití bezpečnostních přístrojových systémů je však nutný vysoký stupeň jejich pohotovosti.

kých, elektronických, programových elektronických).

Pro zjednodušení postupu návrhu a zavedení bezpečnostního systému se používá ČSN EN 61511-1, 2 a 3. Postup podle uvedené normy:

- vyžaduje k zjištění požadované celkové bezpečnosti posouzení nebezpečí a rizika,
- vyžaduje, aby k bezpečným přístrojovým systémům byly přiřazeny požadavky na bezpečnost,
- využívá k dosažení funkční bezpečnosti v rámci možností všechny přístrojové metody.

2. Použitelnost normy

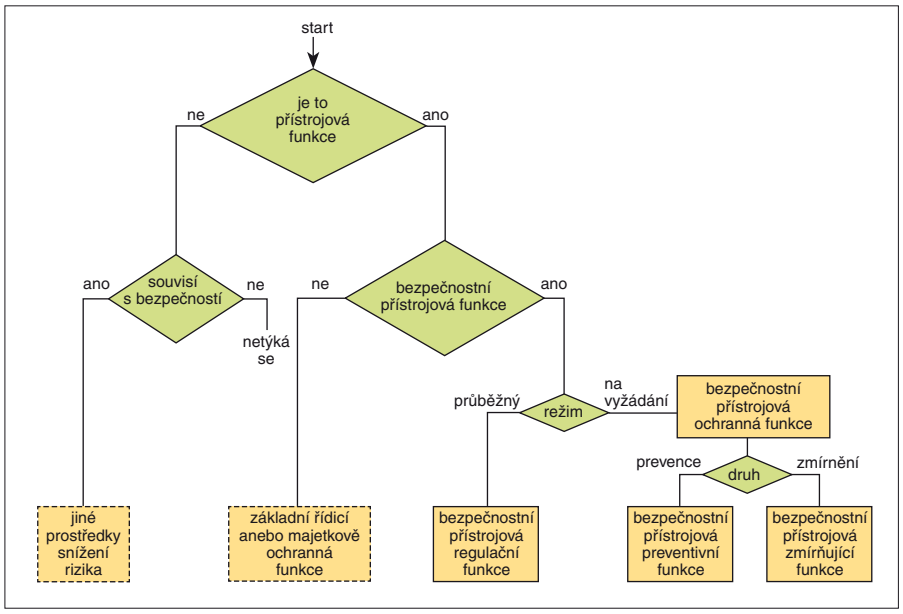
Norma ČSN EN 61511-1, 2 a 3, o bezpečnostních přístrojových systémech pro průmyslová technologická zařízení se spojitými procesy:

- platí pro všechny fáze životního cyklu bezpečnosti od počáteční koncepce, přes projekt, zavádění, provoz a údržbu až po vyřazení z provozu,
- umožňuje, aby s ní byly harmonizovány existující i nové národní normy pro určité průmyslové procesy.

Pro normu ČSN EN 61511 je mj. charakteristické následující:

a) stanovuje požadavky na funkční bezpečnost, nestanovuje však, kdo za uplatnění těchto požadavků odpovídá (např. vývojáři, dodavatelé, majitelé provozované společnosti, smluvní strana); tato odpovědnost tedy může být přidělena různým stranám podle bezpečnostního plánování a národních ustanovení,

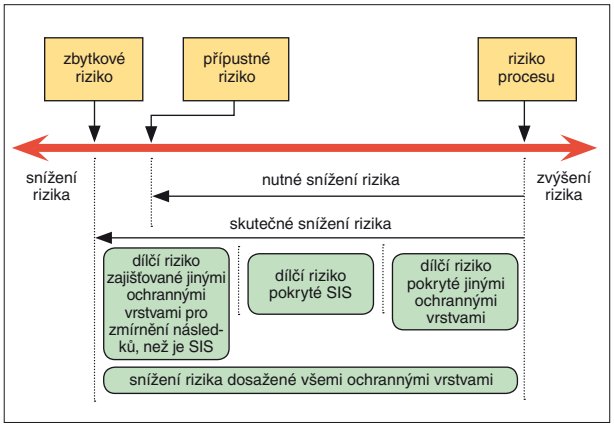
b) používá se pro široké spektrum průmyslových spojitých technologických procesů v ropných rafineriích, při výrobě benzinu, olejů, tuků, maziv a plynů, drtí, buničiny a papíru, v nejaderných elektrárnách a teplárnách apod.



Obr. 1. Vztah mezi bezpečnostní přístrojovou funkcí a jinými funkcemi

Jestliže je to z hlediska hodnocení rizik nezbytné, může být stávající přístrojový systém doplněn ochranným systémem nebo bezpečnostními přístrojovými systémy určenými k minimalizaci možných zbytkových rizik.

Ochranné systémy mohou být založeny na různých technických principech (chemických, mechanických, hydraulických, pneumatických, elektric-



Obr. 2. Obecná koncepce snižování rizik

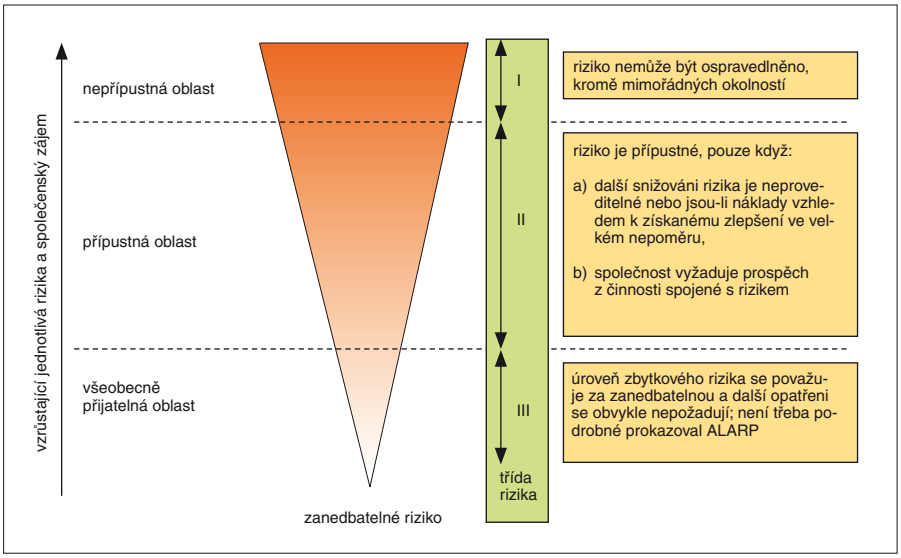
3. Základní pojmy v oblasti integrity bezpečnosti

V oblasti integrity bezpečnosti se používají tyto základní pojmy:

- *specifikace požadavků na bezpečnost* (*Safety Requirement Specification* – SRS),
- *bezpečnostní přístrojová funkce* (*Safety Instrumented Function* – SIF): bezpečnostní funkce se stanovenou úrovní integrity bezpečnosti nezbytnou k dosažení funkční bezpečnosti; může jí být buď bezpečnostní přístrojová ochranná funkce nebo bezpečnostní přístrojová regulační funkce (vztah mezi bezpečnostní přístrojovou funkcí a ostatními funkcemi ukazuje *obr. 1*),
- *bezpečnostní přístrojový systém* (*Safety Instrumented System* – SIS): přístrojový systém používaný k realizaci jedné nebo několika bezpečnostních přístrojových funkcí,
- *integrita bezpečnosti* (*Safety Integrity*): střední pravděpodobnost, že bezpečný přístrojový systém uspokojivě provádí požadované bezpečnostní přístrojové funkce za všech stanovených podmínek ve stanovené době,
- *úroveň integrity bezpečnosti* (*Safety Integrity Level* – SIL): diskrétní úroveň (jedna ze čtyř) pro stanovení požadavků na integritu bezpečnosti bezpečnostních přístrojových funkcí, které mají být přiděleny do bezpečnostních přístrojových systémů; nejvyšší úrovní integrity bezpečnosti je 4, nejnižší 1.

Tab. 1. Úrovně integrity bezpečnosti: pravděpodobnost poruchy SIF při vyžádání (režim provozu „na vyžádání“)

Úroveň integrity bezpečnosti (SIL)	Cílová střední pravděpodobnost poruchy při vyžádání	Cílové snížení rizika
4	$(1 \cdot 10^{-5}; 1 \cdot 10^{-4})$	(10 000; 100 000)
3	$(1 \cdot 10^{-4}; 1 \cdot 10^{-3})$	(1 000; 10 000)
2	$(1 \cdot 10^{-3}; 1 \cdot 10^{-2})$	(100; 1000)
1	$(1 \cdot 10^{-2}; 1 \cdot 10^{-1})$	(10; 100)



Obr. 3. Přijatelné riziko a princip ALARP

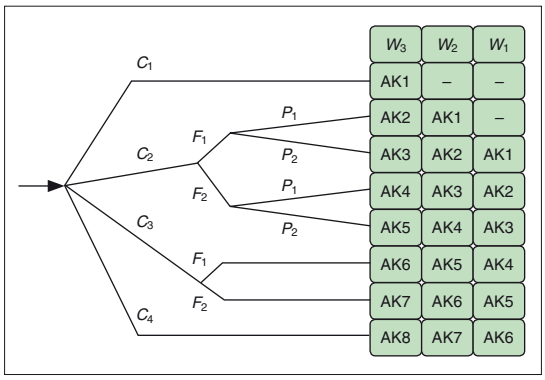
K definici bezpečnostního přístrojového systému (SIS) je třeba poznamenat, že:
- SIS může obsahovat buď bezpečnostní přístrojové regulační funkce, nebo bezpečnostní přístrojové ochranné funkce, nebo obojí současně,
- SIS může, ale nemusí obsahovat software,
- je-li částí SIS činnost člověka, musí být ve specifikaci požadavků na bezpečnost (SRS) stanovena pohotovost a bezporuchovost činnosti operátora a zahrnuta do výpočtů pohotovosti SIS.

Úroveň integrity bezpečnosti v závislosti na pravděpodobnostních charakteristikách pro pracovní režim „na vyžádání“ a „průběžný“ uvádějí *tab. 1* a *tab. 2*.

4. Koncepce snižování rizika

Riziko nehody je neoddělitelnou vlastností mnoha technologických procesů. Riziko je však možné obecně snižovat, např. lze snižovat riziko způsobené vlastnostmi řídicího systému procesu. Ve snaze zabránit neracionálním požadavkům na integritu bezpečnosti základního systému řízení zavádí norma omezení na požadavky, které jsou realizovatelné. Nutné snížení rizika je minimální úroveň snížení rizika, kterého se musí dosáhnout, aby bylo dodrženo přípustné (přijatelné) riziko. Lze ho dosáhnout použitím jedné nebo kombinace několika technik zajišťujících snížení rizika.

Princip snížení rizika nutného k dosažení stanoveného přijatelného rizika z výchozí úrovně rizika vlastního procesu je znázorněn na *obr. 2*.



Obr. 4. Diagram rizika podle DIN V 19250 – ochrana pracovníků

Tab. 2. Úrovně integrity bezpečnosti: četnost nebezpečných poruch SIF (průběžný provoz)

Úroveň integrity bezpečnosti (SIL)	Cílová četnost nebezpečných poruch výkonu bezpečnostní přístrojové funkce (h^{-1})
4	$(1 \cdot 10^{-9}; 1 \cdot 10^{-8})$
3	$(1 \cdot 10^{-8}; 1 \cdot 10^{-7})$
2	$(1 \cdot 10^{-7}; 1 \cdot 10^{-6})$
1	$(1 \cdot 10^{-6}; 1 \cdot 10^{-5})$

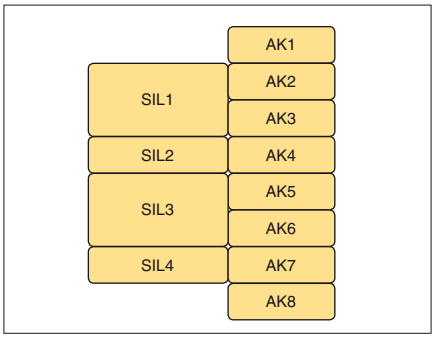
5. Výběr metod k určení požadované SIL

Existuje několik způsobů, jak stanovit požadovanou SIL pro určitou úlohu. Která metoda je pro daný případ vhodná, závisí na mnoha faktorech, jako jsou např.:
- složitost úlohy,
- metodické pokyny od dozorčího orgánu,
- povaha rizika a požadované snížení rizika,
- zkušenost a odbornost osob, které jsou k dispozici,
- dostupnost informací o parametrech týkajících se rizika.

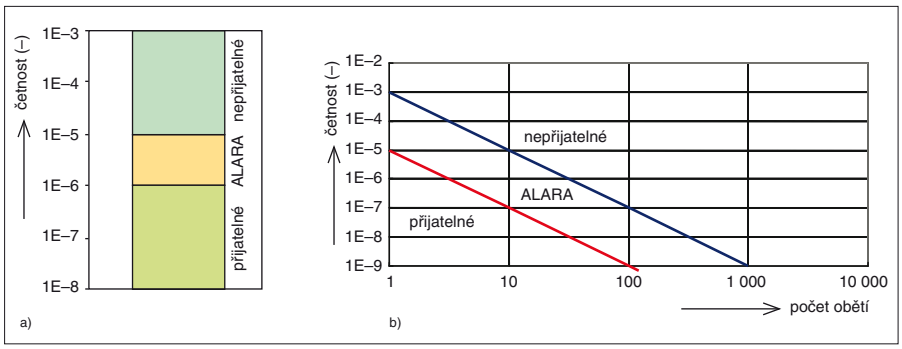
V některých případech lze zvolit i více než jednu metodu. Při prvním pokusu o stanovení požadované SIL lze použít kvalitativní metodu. Jestliže byla kvalitativní metodou přiřazena SIL 3 nebo SIL 4, kvalitativní posouzení nestačí a je požadován následný podrobnější rozbor při použití semikvantitativní metody.

6. Model ALARP

K hlavním kritériím, která se používají při správě rizik v průmyslu, patří tyto údaje:



Obr. 5. Souvislost mezi hodnotami SIL a AK



Obr. 6. Kritéria přijatelnosti rizika: a) individuálního, b) společenského (ALARA – As Low As Reasonably Achievable)

Tab. 3. Parametry pro kvalitativní hodnocení podle normy DIN V 19250 (viz obr. 4)

Parametr rizika		Klasifikace	Poznámky
následek (*C*)	C_1	lehké zranění osob	1: systém klasifikace vytvořen pro posuzování zranění a smrti osob; pro škody na životním prostředí nebo majetku je třeba vytvořit jiná klasifikační schémata.
	C_2	vážné trvalé zranění jedné nebo více osob; smrt jedné osoby	
	C_3	smrt několika osob	
	C_4	katastrofický účinek, velmi mnoho lidí zabito	
frekvence přítomnosti v nebezpečné zóně násobená dobou vystavení (*F*)	F_1	vzácné až častější vystavení v nebezpečné zóně	2: viz poznámka 1 shora
	F_2	časté až trvalé vystavení v nebezpečné zóně	
možnost vyhnout se následkům nebezpečné události (*P*)	P_1	možné za určitých podmínek	3: parametr *P* bere v úvahu: – provozování procesu (s dozorem, tj. provozované kvalifikovanými nebo nekvalifikovanými osobami, nebo bez dozoru), – rychlost vzniku nebezpečné události (např. neočekávané, rychle nebo pomalu), – snadnost rozpoznání nebezpečí (např. okamžitě spatřené, zjištěné technickými prostředky, zjištěné bez technických prostředků), – vyhnutí se nebezpečné události (např. únikové cesty jsou možné, nejsou možné, jsou možné za určitých okolností), – skutečná bezpečnostní zkušenost (může existovat s identickým procesem nebo podobným procesem, popř. nemusí existovat)
	P_2	téměř nemožné	
pravděpodobnost nežádoucího výskytu (*W*)	W_1	velmi malá pravděpodobnost nežádoucích výskytů, pravděpodobných je pouze několik nežádoucích výskytů	4: účelem činitele *W* je odhadnout frekvenci nežádoucího výskytu bez přidání jakýchkoliv přístrojových systémů bezpečnosti (elektrických, elektronických anebo elektronických programovatelných – E/E/PE – nebo založených na jiných technických principech), ale včetně všech vnějších prostředků pro snížení rizika
	W_2	malá pravděpodobnost nežádoucích výskytů, pravděpodobný je malý počet nežádoucích výskytů	

a) je dané riziko tak velké, že se musí zcela odmítnout,
b) je riziko tak malé nebo bylo natolik minimalizováno, že je bezvýznamné,
c) je riziko někde mezi stavy uvedenými ad a) a b) a již bylo sníženo na nejnižší možnou úroveň, a to s přihlédnutím k přínosům plynoucím z jeho přijetí a se zvážením nákladů na jakékoliv jeho další snížení.

Zkratka ALARP označuje princip, který lze použít při určování SIL. Nejde o metodu k určování SIL. Princip ALARP doporučuje, aby se riziko snížilo, „až když je to rozumně možné“ čili na úroveň, která je „nejnižší rozumně možná“ (*As Low As Reasonably Practicable*). Podle tohoto principu se předpokládá, že riziko spadá do jedné ze tří oblastí klasifikovaných jako „nepřijatelné“, „přijatelné“ nebo „všeobecně přijatelné“ (třídy I, II a III na *obr. 3*).

7. Příklad kvalitativního posouzení (DIN V 19250)

Vhodnou kvalitativní metodou ke stanovení SIL je metoda definovaná v normě DIN V 19250, která při definovaní osmi tříd bezpečnostních systémů vychází z analýzy rizika způsobem uvedeným na *obr. 4* a v *tab 3*. Třídy se označují alfanumerickým znakem AK1 až AK8. Mezi AK a SIL neexistuje přímý převod, ale jen přibližné porovnání (*obr. 5*).

8. Kritéria přijatelnosti rizika

Při kvantifikaci rizik hrají významnou roli frekvence události a následky či ztráty spojené s výskytem události.

Vztah mezi četností výskytu *F* neočekávané události a jejími následky *N*, vyjádřenými počtem fatálních zranění, bývá vyjadřován ve tvaru

$$FN^2 = k \qquad (1)$$

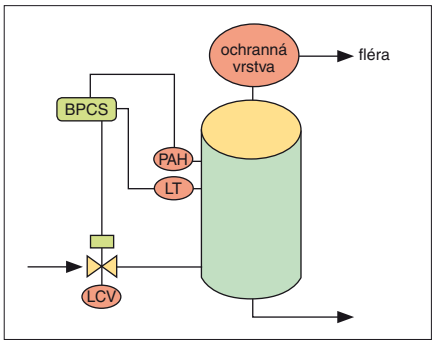
kde *k* je parametr (obvykle konstantní pro dané spektrum událostí a lokalitu).

Na základě výsledků studií a analýz společenského rizika realizovaných v Nizozemí v roce 1980 byla za kritérium (mez) nepřijatelnosti rizika stanovena hodnota $k = 1 \cdot 10^{-3}$ (*obr. 6*).

9. Semikvantitativní metoda

Postup posouzení rizik s použitím semikvantitativní metody lze rozdělit do těchto hlavních kroků (z nichž první čtyři lze provést během studie HAZOP):

1. Odhalení/identifikace nebezpečí procesu.
2. Identifikace bezpečnostních vrstev (bezpečnostní vrstvy zahrnují všechny bezpečnostní systémy, které jsou k dispozici k zabezpečení procesu, tj. SIS, bezpečnostní systémy založené na jiných technických principech, vnější zařízení pro snížení rizik a reakci obsluhy).
3. Určení iniciačních událostí.
4. Vytvoření scénáře nebezpečných událostí pro každou iniciační událost.
5. Odhad četnosti výskytu iniciačních událostí a spolehlivosti existujících bezpečnostních systémů na základě historických dat nebo technikou modelování.
6. Kvantifikování četnosti výskytu podstatných nebezpečných událostí.
7. Vyhodnocení následků všech podstatných nebezpečných událostí.



Obr. 7. Schéma aparátu a systému měření a regulace (PAH – spínač tlaku, LT – snímač polohy hladiny, LCV – regulační ventil)

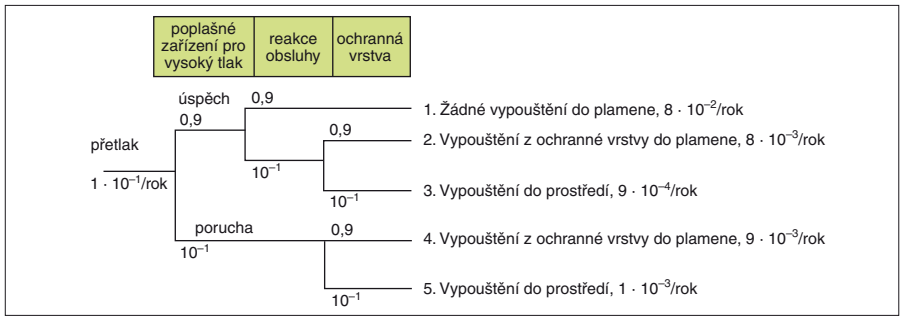
10. Případová studie

Jako příklad je uvažována tlaková skladovací nádoba s těkavou hořlavou kapalinou. Aparát je vybaven základním řídicím systémem (*Basic Process Control System* – BPCS) umožňujícím sledovat polohu hladiny a podle ní regulovat přítok do nádoby.

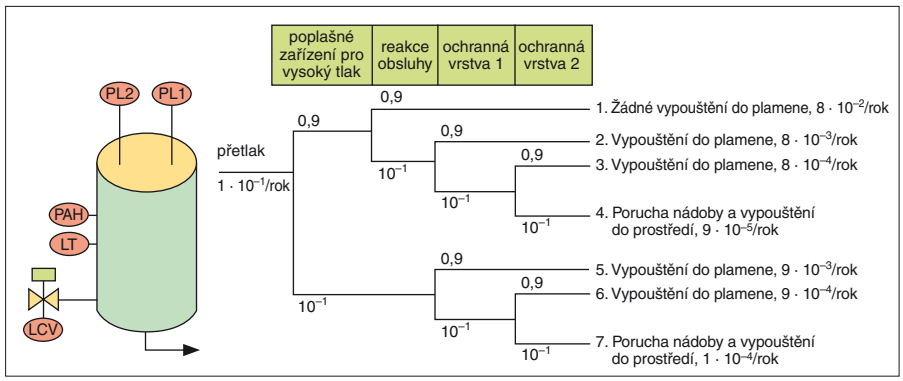
Dostupné technické systémy jsou tyto:

a) nezávislý snímač tlaku, který má aktivovat okruh výstražného hlášení o vysokém tlaku v nádobě a upozorňovat obsluhu, že má zastavit přítok látky,
b) nepřístrojová ochranná vrstva, která je zaměřena na nebezpečí spojená s vysokým tlakem v nádobě v případě, že obsluha nereaguje (pojistná armatura).

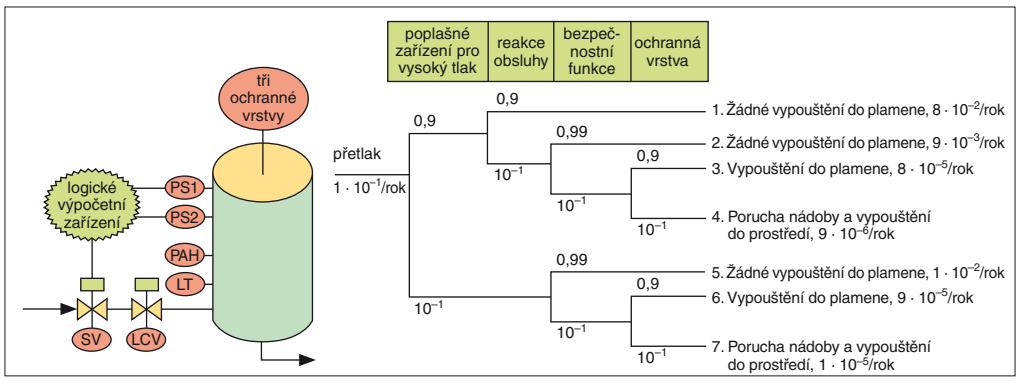
Úniky z ochranné vrstvy jsou přivedeny potrubím do odlučovací nádrže, která uvolňuje plyny do spalovacího systému fléry pro jejich vyhoření. V tomto příkladu se předpokládá, že fléra je řádně navržena, instalována a provozována; potenciální poruchy fléry nejsou v tomto příkladu uvažovány.



Obr. 8. Rozvoj stromem událostí – přetlak v nádobě



Obr. 9. Použití zdvojené ochranné vrstvy PL1 a PL2



Obr. 10. Použití bezpečnostního přístrojového systému se SIL 2 (SV – bezpečnostní uzavírací ventil; PS1, PS2 – tlakový spínač)

Základní schéma aparátu a systému regulace je na *obr. 7*.

Scénář nebezpečné události – uvolnění přetlaku z tlakové nádoby – byl rozvinut s použitím stromu událostí zobrazeného na *obr. 8*. Je zřejmé, že scénáře 3 a 5 mají frekvence výskytu $9 \cdot 10^{-4}$/rok a $1 \cdot 10^{-3}$/rok, přičemž dochází k úniku nebezpečné látky do životného prostředí.

Podnikové metodické pokyny stanovují cílovou četnost úniku do životního prostředí menší než $1 \cdot 10^{-4}$ /rok. Současné řešení bezpečnosti tedy nesplňuje stanovenou podmínku a je požadováno zmenšit četnost výskytu pod cílovou úroveň danou předpisem.

Nově navrhované řešení a kvantitativní ocenění stromem událostí jsou na *obr. 9*. Navrhované řešení nesplňuje stanovené kritérium: četnost úniku do životního prostředí je stále větší než $1 \cdot 10^{-4}$ /rok. Celková četnost úniku do prostředí je $1{,}9 \cdot 10^{-4}$/rok.

Ke zmenšení celkové četnosti vypouštění škodlivé látky do atmosféry při dodržení cílové úrovně bezpečnosti je nutné instalovat novou bezpečnostní přístrojovou funkci. Výsledný nový bezpečnostní přístrojový systém je znázorněn na *obr. 10*.

11. Závěr

Cílové úrovně bezpečnosti v mnoha případech nelze dosáhnout použitím ochranných vrstev založených na jiné technice nebo vnějších prostředků pro snížení rizika. V posuzovaném případě je celková četnost úniku do životního prostředí 1,9 až 10^{-3}/rok. Ke snížení celkové četnosti úniku do životního prostředí se požaduje pro dodržení cílové úrovně bezpečnosti nová bezpečnostní přístrojová funkce(SIF) zavedená do SIS.

Nová SIF je zobrazena na *obr. 10*. Ke stanovení hodnoty SIL není nutný podrobný návrh přístrojové bezpečnostní funkce. Například nová SIF může používat dvojité tlakové spínače určené pro bezpečnostní účely. Výstup logického automatu řídí jeden nový, dodatečný uzavírací ventil.

Pro stanovení SIL při plynulé funkci je nutné vyjít ze současného stavu. Četnost úniku látky do životního prostředí je $1{,}9 \cdot 10^{-3}$/rok, požadovaná četnost je menší než $1 \cdot 10^{-4}$/rok. V praxi to znamená, že od nového bezpečnostního přístroje se požaduje frekvence poruch 10^{-2}/rok nebo menší. Při plynulé funkci, tj. asi 10 000 provozních hodin za rok, odpovídá četnost 10^{-2}/rok četnosti 10^{-6}/h. Této hodnotě četnosti podle *tab. 2* pro plynulou bezpečnostní přístrojovou funkci odpovídá hodnota SIL 2.

Použít ČSN EN 61511 ke stanovení úrovně integrity bezpečnosti se doporučuje zvláště v těchto případech:

a) funkční bezpečnosti se dosahuje s použitím jedné nebo několika bezpečnostních přístrojových funkcí pro ochranu buď zaměstnanců, veřejnosti nebo prostředí,
b) úlohy netýkající se bezpečnosti ve vztahu k majetku,
c) typické metody posouzení nebezpečí a rizik, které se mohou provádět pro definování funkčních požadavků na bezpečnost a úroveň integrity bezpečnosti pro každou bezpečnostní přístrojovou funkci,
d) opatření pro určení požadovaných úrovní integrity bezpečnosti,
e) stanovení úrovní integrity bezpečnosti, ale bez specifikování úrovně integrity bezpečnosti pro konkrétní úlohy.

Při řešení konkrétních požadavků z praxe zůstává zásadní otázkou stanovení úrovně rizika, kterého se má dosáhnout. Tuto úlohu norma neřeší. Předpokládá se, že hodnota bude stanovena racionálním postupem.

Literatura:

[1] *Land Use Planning Guidelines in the Context of Article 12 of the SEVESO II DIRECTIVE 96/82/EC as Amended by DIRECTIVE 105/2003/EC*. Joint Research Centre, September 2006.

[2] *ČSN EN 61511-1 Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů – Část 1: Požadavky na systémy hardwaru a softwaru, struktura, definice*. ČNI, Praha, říjen 2005.

[3] *ČSN EN 61511-2 Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů – Část 2: Metodický pokyn pro používání IEC 61511-1*. ČNI, Praha, 2005.

[4] *ČSN EN 61511-3 Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů – část 3: Pokyn pro stanovení požadované úrovně integrity bezpečnosti*, ČNI, Praha, 2005.

prof. Ing. František Babinec, CSc.,
Fakulta strojního inženýrství, VUT v Brně
(babinec@fme.vutbr.cz)