ČESKÁ SPOLEČNOST PRO JAKOST

Novotného lávka 5, 116 68 Praha 1

Bezpečnost a spolehlivost nových technologií

Materiály z 53. setkání
odborné skupiny pro spolehlivost

Praha, prosinec 2013

Obsah

POROVNÁNÍ PŘÍSTUPŮ STANOVENÍ FUNKČNÍ BEZPEČNOSTI

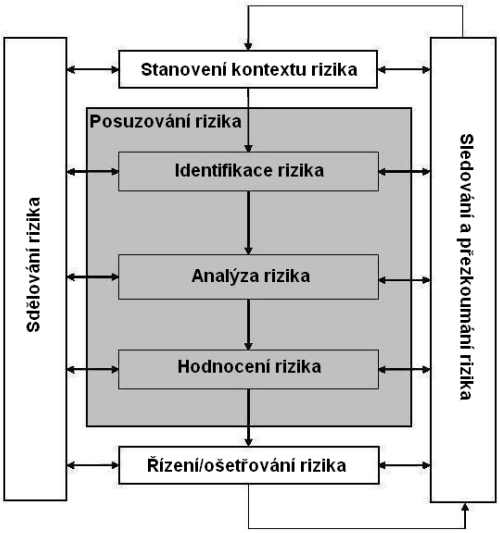
Ing. Jaroslav Zajíček, Ph.D.; Ing. Jan Kamenický, Ph.D.
VŠB-TUO, Výzkumné energetické centrum, 17. listopadu 15, Ostrava – Poruba 708 33
email: jaroslav.zajicek@vsb.cz; jan.kamenicky@vsb.cz
doc. Ing. Pavel Fuchs, CSc.
TUL, Fakulta mechatroniky, informatiky a mezioborových studií, Studentská 2, Liberec 461 17
email: pavel.fuchs@tul.cz

1. Úvod

Pro efektivní řízení rizika je třeba umět riziko správně posuzovat. V technické praxi se posuzování rizika stává jedním ze základních prostředků k prokázání, že zařízení je dostatečně bezpečné. To se promítá i do norem v různých průmyslových odvětvích. Tyto normy vyžadují provést posouzení rizika zařízení a prokázat, že riziko je přijatelné. Pro posuzování rizika pak nabízejí různé přístupy k hodnocení rizika – kvalitativní, semikvantitativní a kvantitativní. Tyto normy zpravidla nedávají konkrétní návod, jak postupovat při hodnocení rizika v jednotlivých případech. S ohledem na různorodost nebezpečných jevů a jejich následků jsou koncipovány jako obecná doporučení. Pokud normy tato obecná doporučení konkretizují formou příkladů, jsou tyto příklady řazeny do příloh, které jsou označovány jako informativní. Nejsou tedy závazné.
Za základní normy funkční bezpečnosti jsou považovány IEC 61508-5 [1] a IEC 61511-x [2]. Jejich principy pak přejímají další normy z různých průmyslových odvětví se vztahem k funkční bezpečnosti, např. IEC 62061 [3], ISO 13849 [4], IEC 61513 [5], EN 50129 [6] nebo i níže analyzovaná směrnice německého drážního úřadu. Uvedené dokumenty jsou výsledkem historického vývoje chápání úlohy bezpečnostních systémů při redukci rizika plynoucího z provozu technických zařízení. Jsou zaměřeny na to, aby návrh, výroba a provozování těchto bezpečnostních systémů zajistily jejich dostatečnou odolnost proti náhodným a systematickým poruchám. Jinými slovy řečeno, aby byla zajištěna vysoká funkceschopnost bezpečnostních systémů. Za tím účelem předepisují postupy a techniky, které je třeba aplikovat. Čím více je třeba snížit riziko, tím sofistikovanější a nákladnější jsou bezpečnostní systémy k tomu určené.
Při aplikaci požadavků norem pro konkrétní technické řešení je tedy třeba správně chápat podstatu rizika a způsobů jeho hodnocení. Nelze tedy neuváženě aplikovat příklady hodnocení rizika, které jsou uváděné v normách, především v informativních přílohách. To by mohlo vést k podhodnocení nebo nadhodnocení rizika a ve svých důsledcích k neefektivnímu řízení rizika.
Prvním krokem při snižování rizika pomocí bezpečnostních systémů je stanovení hodnoty rizika z provozovaného zařízení. Pokud není riziko v tomto kroku stanoveno korektně, nemůže být dosaženo optimálního řešení. Bezpečnostní systémy jsou pak navrhovány buď s nadměrnou, nebo nedostatečnou odolností proti systematickým a náhodným poruchám. Z toho pak vyplývají příslušné ekonomické a bezpečnostní důsledky.
V tomto příspěvku je prezentována analýza zjednodušených přístupů k určování integrity bezpečnosti ze tří mezinárodních standardů, a to IEC 61508-5, IEC 62061 a ISO 13849-1, a dále pak směrnice německého drážního úřadu SIRF - části SIRF 400. Účelem příspěvku je poukázat na některá společná východiska a na slabiny v hodnocení rizika a posuzování jeho přijatelnosti při použití těchto norem.

2. Účel a základní filosofie funkční bezpečnosti

Důvodem, proč byly normativně popsány procesy a postupy aplikace funkční bezpečnosti, bylo řízení rizika na úroveň, která je společností přijatelná. Důsledky poruch mohou být různého charakteru - čistě ekonomického, environmentálního nebo bezpečnostního (vliv na zdraví a životy osob). Vše níže uvedené, a tedy to, co řeší postupy funkční bezpečnosti, se týká posledního typu následku - bezpečnosti osob. Funkční bezpečnost je v souladu se schématem managementu rizika na následujícím obr. 1.



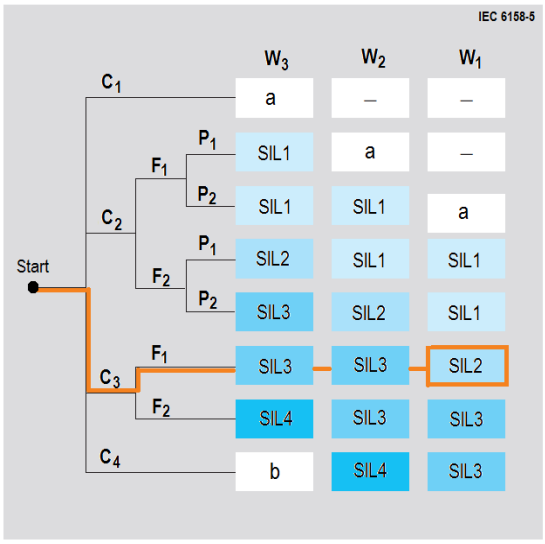
Obr. 1: Management rizika

Analýza rizika a hodnocení rizika probíhají v jednom kroku pomocí diagramů, matic nebo semikvantitativních výpočtů, uvedených přímo v normativních dokumentech (informativních přílohách). Zjednodušeně řečeno, na základě určení pravděpodobnosti a následku nežádoucí události je přiřazena úroveň bezpečnostního systému tak, aby po jeho realizaci byla míra rizika přijatelná.

3. Přístupy v posuzování rizika

Níže budou stručně charakterizovány 4 přístupy při posuzování rizika, a to dle:
- IEC 61508-5
- IEC 62061
- ISO 13849-1
- SIRF 400

Uvedené dokumenty se poměrně zásadně liší v procesu posuzování rizika. Liší se množství hodnocených faktorů, jejich kvantifikace i výsledné zpracování pro stanovení potřebné úrovně spolehlivosti bezpečnostního systému. To, v čem se postupy shodují, je základní filosofie rizika, tedy jeho chápání jako kombinace složky pravděpodobnosti a následků. Dva z postupů používají semikvantitativního přístupu v posuzování, zbylé dva pak kvalitativního přístupu s využitím rozhodovacího schématu a ordinálních stupnic (lze určit pořadí).



Následek (C)

C_1 menší zranění
C_2 zranění jedné nebo více osob s trvalými následky; smrt jedné osoby
C_3 smrt několika osob
C_4 smrt velkého počtu osob

Doba vystavení (F)

F_1 vzácné až častější
F_2 časté až trvalé

Možnost se nebezpečí vyhnout (P)

P_1 možné za určitých podmínek
P_2 téměř nemožné

Pravděpodobnost výskytu nežádoucí události (W)

W_1 velmi malá
W_2 malá
W_3 poměrně vysoká

– = Žádné bezpečnostní požadavky
a = Žádné speciální bezpečnostní požadavky
b = Jediný E/E/PE systém související s bezpečností není dostatečný

Obr. 2: Postup dle IEC 61508-5

IEC 62061

Určení SIL
(přiřazením SIL)

Četnost a doba trvání ohrožení Fr	
≤ 1 h	5
> 1 h až ≤ 1 den	5
> 1 den až ≤ 2 týdny	4
> 2 týdny až ≤ 1 rok	3
> 1 rok	2

Pravděpodobnost výskytu nebezpečné události Pr	
velmi vysoká	5
pravděpodobná	4
možná	3
výjimečná	2
zanedbatelná	1

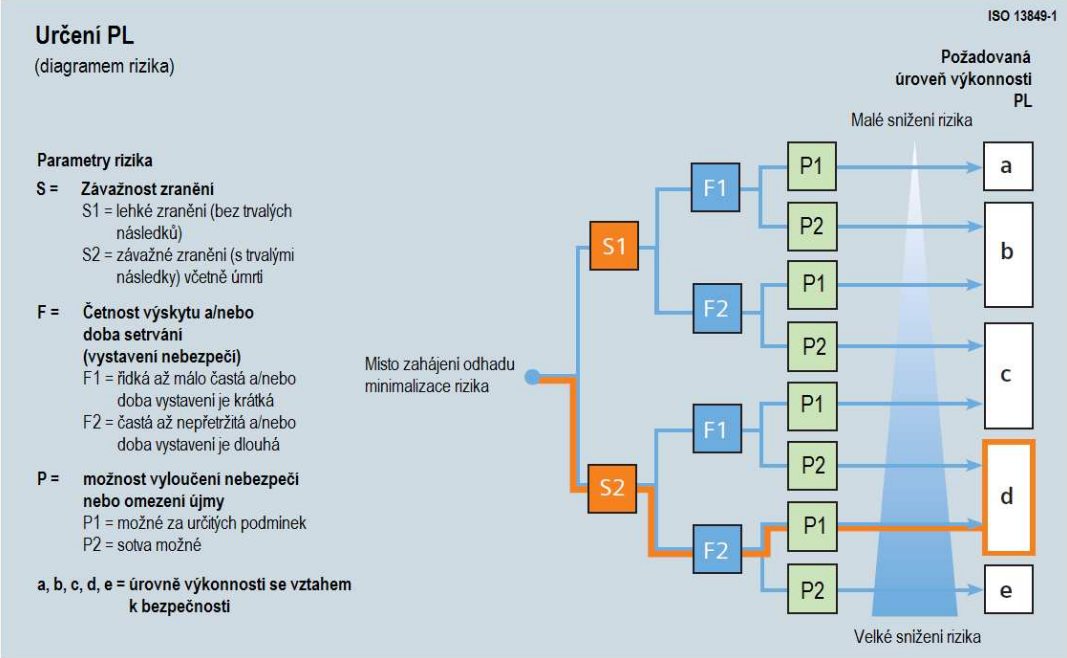
Možnosti prevence Av	
nemožné	5
možné	3
pravděpodobné	1

Následky	Závažnost Se	Třída Cl = Fr + Pr + Av				
		3–4	5–7	8–10	11–13	14–15
Smrt, ztráta oka nebo paže	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Trvalé, ztráta prstů	3	Jiná opatření		SIL 1	SIL 2	SIL 3
Přechodné, lékařské ošetření	2				SIL 1	SIL 2
Přechodné, ošetření (první pomoc)	1					SIL 1

Postup

1. Určení třídy závažnosti poškození (následku) Se
2. Určení bodů pro četnost (frekvenci) Fr, pravděpodobnost výskytu Pr a prevenci Av
3. Součet bodů Fr + Pr + Av = třída Cl
4. Průnik řádku závažnosti následku Se a sloupce třídy pravděpodobnosti následku Cl = požadovaná SIL

Obr. 3: Postup dle IEC 62061



Obr. 3: Postup dle ISO 13849-1

Parametr škody (S)			
Počet S_a		Stupeň zranění S_v	
jeden	3	lehké poranění (LV)	2
více	5	těžké poranění (SV)	4
mnoho	8	smrt	9
Parametr pravděpodobnost výskytu (W)			
nízká		1	
střední		1,7	
vysoká		3	
Parametr čas výskytu (E)			
krátká		1	
dlouhá		1,3	
Parametr zamezení (V)			
není možné		1	
možné		1,7	

$$I = \frac{S_a \cdot S_v \cdot W \cdot E}{V}$$

klasifikační indikátor I	stupeň požadavku na bezpečnosti (SIL, něm. SAS)
0 - 21	= SAS 0
22 - 35	= SAS 1
36 - 72	= SAS 2
73 - 122	= SAS 3

Obr. 4: Postup dle SIRF 400

4. Kvalitativní porovnání přístupů

Pro porovnání uvedených postupů byly vytvořeny tabulky 1 až 3. První tabulka dělí postupy podle typu hodnotících stupnic, způsobu stanovení SIL, toho, jakým způsobem jsou úrovně požadované funkční bezpečnosti vůbec značeny, počtu hodnocených kritérií a počtu úrovní hodnotících stupnic.

Tab. 1: Způsoby dosažení požadované funkční bezpečnosti

	Typ stupnic	**Způsob stanovení SIL**	**Označení požadavku**	**Počet hodnocených kritérií**	**Počet úrovní hodnotících stupnic**
IEC 61508-5	Kvalitativní ordinální	Rozhodovací diagram	- a SIL1 SIL2 SIL3 SIL4 b	4	2 až 4
IEC 62061	Semikvantitativní	Kombinace semikvantitativního výpočtu a matice	SIL1 SIL2 SIL3	4	3 až 5
ISO 13849-1	Kvalitativní ordinální	Rozhodovací diagram	a b c d e	3	2
SIRF 400	Semikvantitativní	Semikvantitativní výpočet	SAS0 SAS1 SAS2 SAS3	5	2 až 3

Tab. 2: Porovnání značení úrovní funkční bezpečnosti a jejich kvantitativní význam

		IEC 61508-5	**IEC 62061**	**ISO 13849-1**	**SIRF 400**
Požadavek na průměrnou frekvenci nebezpečné poruchy bezpečnostní funkce [h^{-1}]	**žádné bezpečnostní požadavky**	-			SAS 0
	žádné speciální bezpečnostní požadavky	a			
	>1E-5 to <1E-4			a	
	>3E-6 to <1E-5	SIL 1	SIL 1	b	SAS 1
	>1E-6 to <3E-6			c	
	>1E-7 to <1E-6	SIL 2	SIL 2	d	SAS 2
	>1E-8 to <1E-7	SIL 3	SIL 3	e	SAS 3
	>1E-9 to <1E-8	SIL 4			SAS 4
	jediný bezpečnostní systém není dostatečný	b			

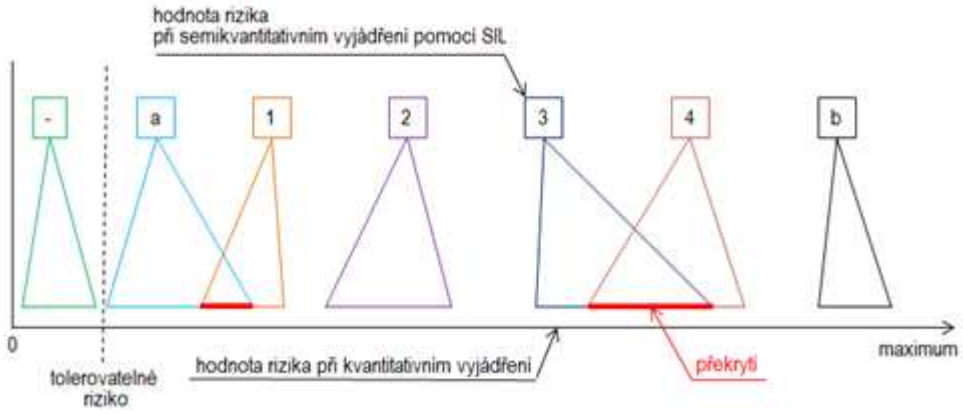
Tab. 3: Značení jednotlivých faktorů rizika

	Parametry pravděpodobnosti			Parametr následků	
	Výskyt	**Vystavení**	**Vyhnutí**	**Počet osob**	**Stupeň zranění**
IEC 61508-5	W	F	P	C	
IEC 62061	Pr	Fr	Av		Se
ISO 13849-1		F	P		S
SIRF 400	W	E	V	Sa	Sv

Na základě takovéhoto stručného porovnání přístupů je evidentní, že uvedené metody se snaží dosáhnout stejného cíle různým způsobem. Ani jeden z postupů není plně kvantitativního charakteru, aby ho bylo možné snadno podrobit ověření - validaci. I bez dalšího podrobnějšího zkoumání je téměř jisté, že různé metody budou při posuzování stejné události dosahovat různých výsledků a tedy se budou lišit i v požadavku na úroveň funkční bezpečnosti.

5. Porovnání přístupů s plně kvantitativním přístupem

Testování, zda doporučený model koresponduje s plně kvantitativním přístupem kvantifikace rizika, je založeno na přiřazení kvantitativních hodnot jednotlivým stupňům hodnotících stupnic. V tomto testování se omezujeme na přiřazení geometrických posloupností, tedy se předpokládá, že sousední úrovně stupnice se liší právě x-krát. Hodnota X je testována na intervalu <2; 20> a omezuje se na celočíselné hodnoty. Důležité je zmínit, že jednotlivé faktory (výskyt, vystavení, vyhnutí, počet osob a stupeň zranění) mohou mít tyto hodnoty (kvocienty geometrické posloupnosti) různé. Např. pro postup v normě IEC 61508-5, do kterého vstupují 4 hodnocené faktory, bylo testováno $19^4 = 130\ 321$ variant.
Následně je porovnáváno, zda pro nízké riziko není požadováno přísnějšího SILu než pro událost s vyšším rizikem. Kritériem tedy je, zda se kategorie rizika překrývají dle následujícího schématu. Překrytí přitom nemusí nastat pouze mezi přímo sousedícími kategoriemi, ale i přes několik kategorií.



Obr. 4: Pokrytí rizika prostřednictvím SIL

5.1 IEC 61508-5

Počet vstupních faktorů: 4
Množství testovaných variant: $19^4 = 130\ 321$
Tab. 4: Překrývání intervalů rizika pro IEC 61508-5

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**						
	0	**1**	**2**	**3**	**4**	**5**	**6**
Jedna (sousední) kategorie SIL	0	0	0	14	82	2 114	128 111
Dvě kategorie SIL	2	169	16 107	26 263	27 773	60 007	-
Tři kategorie SIL	2 995	4 695	50 819	57 508	14 304	-	-
Čtyři kategorie SIL	58 236	14 490	41 143	16 452	-	-	-
Pět kategorií SIL	108 870	0	21 451	-	-	-	-
Šest kategorií SIL	124 922	5 399	-	-	-	-	-

Význam zvýrazněné buňky: U 4 695 variací kvocientů se 1 dvojice intervalů rizika překrývá, dvojice je od sebe vzdálena 3 kategorie SIL. Příklad může být například situace, kdy minimum intervalu rizika úrovně SIL 4 může být nižší než maximum intervalu rizika úrovně SIL 1.

Informačně nejdůležitější buňka je v levém horním rohu tabulky, která vypovídá o počtu variant, kdy se intervaly rizika vůbec nepřekrývají. Za předpokladu geometrických stupnic a platnosti vzorce pro výpočet rizika, který je daný součinem pravděpodobnosti a následků, lze tedy konstatovat, že výsledky při aplikaci doporučeného schématu pro stanovení SIL nejsou v souladu s kvantitativním posuzováním a řízením rizika.

5.2 IEC 62061

Metoda stanovení úrovně integrity bezpečnosti je v této normě odlišná od metody uvedené v IEC 61508-5. Je založena na semikvantitativním hodnocení rizika. Používá 4 parametry (*Se*, *Fr*, *Pr*, *Av*), které jsou hodnoceny body a promítnuty do matice rizika, ve které se uskutečňuje stanovení SIL. Vzhledem k tomu, že se bodová ohodnocení pravděpodobnostních parametrů *Fr*, *Pr* a *Av* sčítají do jediného výsledného parametru *Cl*, je zde pravděpodobné použití geometrických stupnic se stejným kvocientem *Q*. Součet tedy vyplývá ze vztahu:

$$Q^{Fr} \cdot Q^{Pr} \cdot Q^{Av} = Q^{Fr + Pr + Av}$$

Počet vstupních faktorů: 4
Množství testovaných variant: $19^2 = 361$
Tab. 5: Překrývání intervalů rizika pro IEC 62061

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**			
	0	**1**	**2**	**3**
Jedna (sousední) kategorie SIL	0	11	15	335
Dvě kategorie SIL	4	79	278	-
Tři kategorie SIL	298	63	-	-

Výše uvedená tabulka je menšího rozměru z důvodu, že norma IEC 62061 stanovuje pouze 3 kategorie SIL. Komentář je v souladu s hodnocením IEC 61508-5, opět neexistuje varianta, kdy by navržený model byl v souladu s plně kvantitativním hodnocením rizika.

5.3 ISO 13849-1

Počet vstupních faktorů: 3
Množství testovaných variant: $19^3 = 6\,859$
Tab. 6: Překrývání intervalů rizika pro ISO 13849-1

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**				
	0	**1**	**2**	**3**	**4**
Jedna (sousední) kategorie SIL	2 109	0	4 750	0	0
Dvě kategorie SIL	6 459	400	0	0	-
Tři kategorie SIL	6 859	0	0	-	-
Čtyři kategorie SIL	6 859	0	-	-	-

Z tabulky 6 je zřejmé, že zjednodušený přístup podle ISO 13849-1 je v porovnání s přístupy podle IEC 61508-5 a IEC 62061 mnohem robustnější ve smyslu jeho odolnosti proti nevhodnému způsobu sestavení stupnic parametrů rizika. To je zřejmé i z koncentrace hodnot ve sloupci "0". Ani tento způsob však není imunní proti jeho nesprávnému použití a nelze jej tedy považovat za zcela korektní - viz body zmíněné v závěru.

5.4 SIRF 400

Tento přístup využívá 5 hodnotících faktorů rizika. Z důvodu vysokých časových nároků na provedení simulací byly kvocienty generovány pouze na intervalu <2; 15>, a to opět celočíselné. Tato varianta je časově 5x méně náročná oproti původnímu intervalu <2; 20>.
Počet vstupních faktorů: 5
Množství testovaných variant: $14^5 = 537\,824$
Tab. 7: Překrývání intervalů rizika pro SIRF 400

Rozsah překrytí	**Počet překrývajících se dvojic kategorií SIL**				
	0	**1**	**2**	**3**	**4**
Jedna (sousední) kategorie SIL	12	32	636	18 020	519 124
Dvě kategorie SIL	80 110	68 610	47 973	341 131	-
Tři kategorie SIL	387 187	73 301	77 336	-	-
Čtyři kategorie SIL	519 147	18 677	-	-	-

Stejně jako u předchozího postupu v normě ISO 13849-1 existují jisté variace kvocientů, které požadovaných kritériím odpovídají. Důvody, proč ani tento postup nelze přímo označit jako korektní, jsou uvedeny v závěru.

6. Závěr

Cílem článku bylo představit postupy stanovení funkční bezpečnosti, udělat jejich vzájemné porovnání a dále testovat, zda za jistých předpokladů jsou metody konzistentní s plně kvantitativním posuzováním a řízením rizika.
Po provedení simulací je evidentní, že nejvíce robustní je stanovení potřebné úrovně SIL dle ISO 13849-1. To je způsobeno především tím, že do modelu vstupují pouze 3 faktory a intervaly rizika pro jednotlivé kategorie SIL jsou tedy užší.

Zkoumání a porovnání přístupů následně generuje další náměty a otázky k řešení:

- Jaký je důvod existence různých metod? Všechny postupy v závěru doporučují kategorie SIL, které mají konkrétní kvantitativní parametry. To by znamenalo, že různé standardy předpokládají různou míru přijatelného rizika.
- Jaká je tedy hodnota přijatelného rizika? Ani jeden z dokumentů se nezmiňuje o konkrétní hodnotě. Vzhledem k tomu, že se přístupy nejeví v souladu s plně kvantitativním hodnocením rizika, není možné je zpětně z postupů určit.
- Předpoklad použitý v tomto článku - geometrické stupnice - může být samozřejmě mylný. Stupnice stejně tak mohou být aritmetické nebo zcela obecné. Jakým způsobem byly normativní postupy vytvořeny? Chybí jakékoliv zdůvodnění navržených rozhodovacích diagramů, bodových hodnocení semikvantitativních stupnic atd. Stejný přístup, uplatňovaný různými analytiky, se pak může ve výsledcích diametrálně lišit. Například "vysoká" pravděpodobnost výskytu bude vnímána odlišně analytikem pracujícím standardně s mechanickými komponentami vykazující opotřebení a analytikem, který se standardně věnuje spolehlivé elektronice - a to v rozdílech až několika řádů.
- Rozdíl mezi kvantitativní hodnotou kategorie SIL je 1 řád. Toto kritérium nebylo zohledněno při překrývání intervalů. Varianty, které po simulaci vyšly bez překryvu intervalů, by tedy bylo vhodné dále podrobit testu, zda tyto intervaly, respektive středy těchto intervalů, jsou od sebe vzdáleny přibližně o jeden řád.

Autoři příspěvku se domnívají, že využití plně kvantitativních přístupů posuzování a řízení rizika je mnohem efektivnější a prokazatelnější oproti zkoumaným metodám, a to i za předpokladu, že pro kvantitativní analýzu nejsou k dispozici přesná vstupní data a je třeba pracovat s expertními odhady.

Použitá literatura:

[1] ČSN EN 61508-5:2011, *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Příklady metod určování úrovní integrity bezpečnosti.*
[2] ČSN EN 61511-x:2005, *Funkční bezpečnost. Bezpečnostní přístrojové systémy pro sektor průmyslových procesů.*
[3] ČSN EN 62061:2005, *Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností.*
[4] ČSN EN ISO 13849-1:2006, *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci*.
[5] ČSN IEC 61513:2003, *Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Všeobecné požadavky na systémy*.
[6] ČSN EN 50129:2003, *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy*.
[7] SIRF 400 - směrnice německého drážního úřadu

Poděkování:

Tato práce byla vypracována v rámci projektu Příležitost pro mladé výzkumníky, reg. č. CZ.1.07/2.3.00/30.0016, podpořeného Operačním programem Vzdělávání pro konkurenceschopnost a spolufinancovaného Evropským sociálním fondem a státním rozpočtem České republiky.

Tato práce vznikla za podpory Technologické Agentury České republiky, projekt TA01030833 - Integrovaný informační systém pro silniční přepravu nebezpečných chemických látek

SPOLEHLIVOST LIDSKÉHO VÝKONU PŘI INTERAKCI S MODERNÍ TECHNOLOGIÍ

Ing. Radim Doležal, *CPS servis, s.r.o., Technická univerzita v Liberci*
e-mail: dolezal@zkusebny.cz, radim.dolezal@tul.cz

Abstrakt
Lidská interakce s technologií je silně ovlivněna její spolehlivostí. Nová technologie sebou často přináší úplně nové fenomény v lidském chování a paradoxně snižující schopnost člověka vyrovnat se s mimořádnými událostmi. Článek ukazuje některé nové fenomény v lidském chování, jak je předpovídáme a snažíme se s nimi vypořádat.

Klíčová slova
lidské faktory, analýza spolehlivosti člověka, ergonomie

1. Úvod
Lidská interakce s technologií je silně ovlivněna její spolehlivostí. Snahy v oboru technické spolehlivosti vedou ke správné trendu zvyšující se spolehlivosti technologií a celkové bezpečnosti. Na druhou stranu však přináší úplně nové fenomény v lidském chování a paradoxně snižující schopnost člověka vyrovnat se s mimořádnými událostmi. Můžeme pozorovat, že spolehlivost člověka se v těchto situacích snižuje a je tak potřeba hledat nové nástroje, jak jí předpovídat a řídit.

1.1 Spolehlivost člověka

Definice spolehlivosti člověka se v zásadě nemusí lišit od té z technické spolehlivosti, respektive pohotovosti:
Spolehlivost člověka (human reliability) - schopnost člověka splnit úkol jak je to požadováno, a tehdy, když je to požadováno (v definovaném časovém období a v přípustných mezích).
Metoda jakou tuto schopnost hodnotíme se nazývá analýza spolehlivosti člověka (human reliability analysis - HRA). Jeji definice je:
Systematický proces s cílem ohodnotit spolehlivost člověka.
HRA se snaží najít vyjádření lidského chování uvnitř systému. Jde o predikci, která se snaží najít příspěvek lidských chyb za účelem předpovědi podstatných selhání systému. Obvykle nás zajímá pravděpodobnostní hodnocení některých aspektů interakce člověka s technologií. Může jít o naprosto intuitivní odhad (např. jediným expertním odhadem) nebo sofistikované metody využívající mnoho složitých teoretických konceptů. Paleta nástrojů HRA je tak velmi široká.

Se spolehlivostí člověka jsou nedílně spojeny tzv. **faktory ovlivňující (lidský) výkon**. Označujeme je zkratkou PSF (*performance shaping factors*), zřídka PIF (*performance influencing factors*) a jsou charakteristiky vnějšího prostředí, úkolu a lidí, které utvářejí individuální výkonnost (ČSN EN 62508). Obvykle jsou děleny na vnější (prostředí) a vnitřní (individuální). Vnější vlivy a individuální schopnosti jedince můžeme podle různých hledisek

zařazovat do různých tříd tak, aby posuzování spolehlivosti člověka zahrnovalo spektrum nejdůležitějších vlivů. Vnější faktory také můžeme rozdělit na ty, kterou souvisí se samotným úkolem a ty, které jsou ovlivněny organizací (tzv. organizační faktory).
Nutno podotknout, že univerzální seznam PSF neexistuje a každá metoda a každý autor k nim přistupuje s vlastním pojetím. Chápání jejich vlastností se tak často pohybuje v paletě od naprosto kvalitativního, přes semikvantitativní až k plně kvantitativnímu ocenění (např. při stanovení pravděpodobnosti lidské chyby).

Obrázek 1 - Vliv a interakce faktorů ovlivňujících výkon.
Komplexní interakce PSF vyvolaných moderní technologií se zabývají především nové metody HRA - tzv. druhé generace. Právě ty se snaží o zachycení nových fenoménů v lidském chování, které vedou na nové druhy lidských chyb s následky, které dříve nebyly uvažovány.

1.2 Moderní technologie

Již dnes se setkáváme s tím, že si lidé techniku tzv. polidšťují. Uvažují a vnímají ji podobným způsobem jako živý organismus, který není možné naprosto predikovat a vyjádřit. Přesto vnímají některé její prvky jako naprosto spolehlivé a nejsou schopni o nich kriticky uvažovat. Dochází ke ztrátě vědomí o skutečné struktuře a principech na jakých technologie funguje.
Díky zvýšené spolehlivosti se například výrazně snížila údržba některých systémů a tím pádem i počet pracovníků, které jsou k ní potřeba. Ti pak mají na starost větší počet zařízení a těžko si udržují správné povědomí pro potřebu rychlé reakce. Pokud dané zařízení vidíme pouze jednou za rok nebi vzácněji, musíme se s ním nejprve podrobně seznámit. Jak rychlost, tak i celková spolehlivost údržby však klesá.
Moderní technologie také již často obsahují vlastní autodetekci poruch. S úrovní sofistikovanosti autodetekce klesá schopnost člověka rozlišit chybu, kterou autodetekce nepokryla a zároveň schopnost rozpoznání falešného zásahu autodetekce.

1.3 Přehnaná důvěra ve spolehlivé technologie

Pokud konkrétní stroj chybuje s velmi malou frekvencí, může se stát, že přestaneme být ostražitý vůči jeho možných chybám (těm, které nejsou zjevné, nebo ho samotná autodetekce stroje není schopná zachytit). Konzervativním předpokladem z pohledu analýz lidských faktorů je, že existuje jak obecná (pro velkou část populace), tak individuální hranice spolehlivosti, při které nejsou lidé schopni kriticky hodnotit získané informace od tohoto stroje.
Příkladem ze života mohou být dopravní GPS navigace. Stalo se Vám také, že jste byli někdy navedeni doprostřed pole? Nebo jste díky radám navigace sjeli z hlavní, přehledné a nejrychlejší silnice do nějaké „nesmyslné zkratky“ i přesto, že Vám to bylo divné, kam Vás to vlastně navigace žene? Autorovi tohoto článku se to už několikrát stalo.
Zde jsou navíc podmínky, za kterých musíme techniku kriticky posuzovat ztíženy tím, že jsme omezeni časem na rozhodnutí (zdali navigaci poslechnete či nikoli) - obvykle máme na odbočení (nebo neodbočení) pouze sekundy, ve který musíme vyhodnotit pravděpodobnost, že v danou chvíli navigace nevybrala optimální trasu.
K daným faktorům se může přidat i spěch, únava po dlouhé cestě apod. V těchto chvílích má člověk zaděláno na problémy. Tak jako si před několika desetiletími málokdo uměl představit fungování dopravní GPS navigace - i dnes si my nemůžeme plně představit, jaké technologie nás budou brzy obklopovat. Jistě budou mít dobrou až výbornou úroveň spolehlivosti. Můžeme jen doufat, že jejich selhání bude mít tak „relativně bezpečné“ následky jako je zabloudění při cestování.

2. Kognitivní faktory a vliv záměru na spolehlivost lidského výkonu

Lidský mozek neustále sbírá informace a porovnává je s vnitřní reprezentací světa (Sträter, 2000). Toto se děje občas vědomě, ale většinu času jako naprosto nevědomý proces. Tento proces je mnohdy nazýván jako tzv. kognitivní mlýn (*cognitive mill*). Teorie tohoto procesu dokáže vysvětlit, jakým způsobem zpracováváme informace z vnějšího světa, porovnáváme s vnitřním obrazem světa, vlastními cíli našeho snažení a na základě toho jednáme.
Tento psychologický model dokáže dobře reprezentovat lidské chování při výskytu vzácných chyb a predikovat jeho spolehlivost.
V okamžiku, kdy jsme konfrontování s potřebou předpovědi charakteristik lidského výkonu při situacích, které se stávají velmi zřídka, nebo se ještě vůbec nikdy nestaly - nemáme k dispozici jiný nástroj než „nové“ metody druhé generace. Jde především o metody CAHR a CREAM (Hollnagel, 1998). Problematika a bližší vysvětlení těchto metod přesahuje rámec této publikace. Některé podstatné vlastnosti již byly zveřejněny v předchozích příspěvcích, nebo budou prezentovány na samotné přednášce.

2.1 Příklad výpočtu metodou CAHR- testování lidské spolehlivosti

Tento příklad velmi dobře ukazuje, jakým způsobem lidé chybují v interakci s moderní technologií, která je z inženýrského pohledu velmi dobře navržená (např. z pohledu ergonomie, ale i jiných technických hledisek) a měla by v celkové součinnosti s člověkem vykazovat vysokou úroveň spolehlivosti (Sträter, 2005):

Velká automobilová společnost chtěla v rámci vývoje elektrického vozu zjistit možnost využívání tzv. řízení po drátě. Tedy, že by všechny ovládací prvky včetně volantu nebyly mechanicky propojeny se samotnými koly. Řízení by probíhalo předáváním digitálních informací. Aby bylo dosaženo požadované úrovně spolehlivosti a bezpečnosti, bylo zvoleno trojnásobné zálohování digitálního řídicího systému včetně neustálého testování, zdali se všechny systému chovají standardně (stejně). V případě, že by jeden z nich vykazoval abnormalitu, systém jako celek by měl být co nejdříve odstaven a opraven. Jde o podobnou praxi, kterou můžeme vidět ve velmi náročných a nebezpečných provozech.
Protože však automobil nemůžeme v mnoha případech odstavit automaticky (v okamžiku, kdy se porucha vyskytne) - musíme tuto funkci přenechat řidiči. Např. nemůžeme vypnout řízení automobilu ve vysoké rychlosti na dálnici, uprostřed křižovatky nebo na jiném nebezpečném místě. Po řidiči je tak požadováno, aby automobil odstavil na první „bezpečném“ místě a přivolal si opravu/odtah.
Klasickými metodami HRA první generace, využívající logické inženýrské přístupy byla pravděpodobnost lidské chyby při úkolu *bezpečně odstavit vozidlo* predikována v řádech setin. Toto zjištění vyhovovalo celkovému požadavku na spolehlivost a bezpečnost systému. Pro jistotu byla tato úloha předána ke zkoumání odborníkům na druhou generaci metod HRA. Ti přišli s řádově jiným výsledkem, přesahujícím 20%. V okamžiku, kdy byly provedeny dvě analýzy s takto rozdílným výsledkem se automobilka rozhodla uspořádat simulační studii konkrétního příkladu. Výsledkem byla naměřená chybovost přibližně 22% a celkové potvrzení závěrů metod druhé generace.
V tomto konkrétním příkladu tedy započtení vlivu záměru na lidskou spolehlivost. Pro většinu chybujících řidičů bylo včasné dokončení jízdy do cíle cesty mnohem důležitější, než potřeba reagovat ne výstrahy řídicího systému. Ať už si uvědomovali závažnost nebo důsledky dané situace, nebo ne. Lidská mysl tzv. „táhnutá“ těmito zájmy tak v různých případech vědomě i nevědomě ignorovala potřeby systému, které byly v konfliktu s jejími vlastními.
S trochou zjednodušení můžeme tuto ignorací informací přirovnat i k tomu, jak lidé už dnes reagují na současné výstražné kontrolky v automobilech (o potřebě servisu, nefunkčnosti nějakého podsystému apod.). Operátor jaderné elektrárny by jistě díky svému tréninku na tyto informace reagoval adekvátně. Nejde ale o vzorek běžné populace. V té je nezanedbatelné procento lidí, kteří jsou schopni s podobným varováním tzv. „počkat do plánovaného servisu“, nebo prostě čekat „ještě den, ještě týden atd.“ Více podrobností k danému příkladu je k nalezení v odborné literatuře (Sträter, 2005).

2.2 Potřeba tréninku a udržování znalostí, které možná již nikdy nevyužijeme

Při konfrontaci s těmito zjištěními se jistě nabízí otázka řešení těchto problémů. Prvotním a jednoznačně nejlepším nástrojem je prevence.
Pouze pravidelné školení, trénink a simulace dokáže v lidech udržet potřebnou znalost a schopnost vypořádat se s málo frekventovanými a mimořádnými událostmi. S rozšiřováním spolehlivých systémů do stále širších oblastí průmyslu a lidské společnosti se bude zvyšovat potřeba implementovat znalosti teorie prevence z oblastí jako je např. jaderný průmysl, letectví apod.
Stále více lidí napříč společností si tak bude muset udržovat povědomí a znalosti v problematice, kterou možná nikdy skutečně nevyužijí. I přesto bude kriticky důležité, aby si tyto znalosti podniky (ale i společnost jako celek) udržely a tím i základní úroveň kritického povědomí o technologii jako nedílnou součást systému spolehlivosti.

Teprve druhotným nástrojem je předvídání lidských chyb při konfrontaci s takto řídkými jevy. Zde budou vhodně využity znalosti metod HRA druhé generace k tomu, aby byly předpovězeny různé módy lidských chyb a zavedeny opatření ke zmírnění jejich následků.

3. Závěr

Ukazuje se, že klasické inženýrské přístupy k lidskému výkonu při obsluze moderních a spolehlivých technologií přestávají fungovat. Stejně tak staré metody analýzy spolehlivosti člověka již nedokáží přinést kvalitní výsledky předpovědi lidského výkonu.
Předpověď lidské spolehlivosti se ztěžuje příchodem jiného druhu pracovníků (nebo úplně jiného vzorku lidí) a nových spolehlivých technologií. Tyty postupné procesy přinášejí nové fenomény v lidském chování, pro které je již potřeba využívat psychologické poznatky a kombinovat je s technickým uvažováním o fungování a možných stavech systému.
Stále větší důraz bude také kladen na školení a tréninky a potřebná míra jejich využívání poroste. Více informací a příkladů přinese samotná přednáška na toto téma.

Literatura

ČSN EN 62508. *Návod pro lidská hlediska spolehlivosti.* Česká technická norma. Platnost od 1.6.2011. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Model* (CREAM). 1. vyd. Elsevier. ISBN 978-0-08-042848-2.

Sträter, O. 2000. *Evaluation of Human Reliability on the Basis of Operational Experience. GRS-170.* 1. vyd. GRS. ISBN 3-931995-37-2.

Sträter, O. 2005. *Cognition and Safety.* 1. vyd. Ashgate. ISBN 0-7546-4325-5.

PROBLEMATIKA BEZPEČNOSTI TERMOCHEMICKÉ KONVERZE PALIV
ISSUE OF FUEL THERMOCHEMICAL CONVERSION SAFETY

Jan Najser, Václav Peer

Klíčová slova : termochemická konverze, bezpečnost, syntéza Fischer-Tropsch

Anotace :
Příspěvek se zabývá základním popisem technologie termochemické konverze pevných paliv pro kogenerovanou výrobu elektrické energie a tepla a syntézu kapalných paliv. Ve fázi přípravy výrobní dokumentace byla charakterizována klíčová místa a standardní postupy nezbytná pro bezpečný provoz celého zařízení.

Abstract :
This article deals with a basic description of the technology of solid fuels thermochemical conversion for cogeneration of electricity and heat and synthesis of liquid fuels. In the stage of preparation of production documentation was characterized key points and standard procedures necessary for the safe operation of the technology.

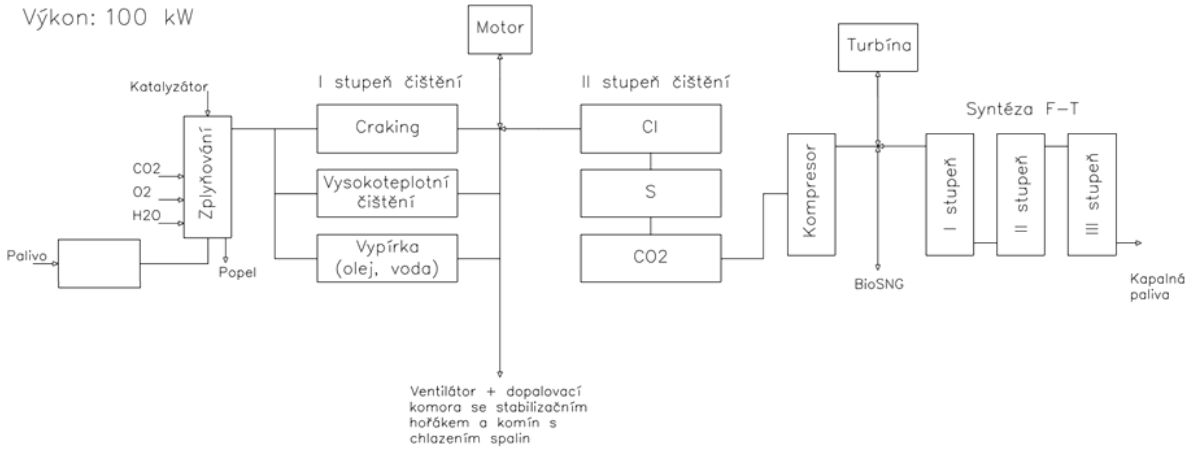
1. Úvod

V současnosti je zplyňování pevných paliv (uhlí, biomasa) velmi perspektivním způsobem výroby elektrické energie a tepla. Představuje alternativu k běžně využívaným postupům využívajícím parní oběhy. Díky jinému způsobu transformace vstupního paliva (nejprve na plynnou fázi následně využívanou pro pohon plynových spalovacích motorů či turbín) představuje zejména pro nižší rozsah výkonů (do 1 MW) velmi účinný způsob kogenerované výroby elektřiny a tepla.

Pevné palivo se v generátoru převádí za vysokých teplot na hořlavý plyn, který se před dalšími procesy nejprve upravuje – odstraňují se z něho dehtovité látky a prach. Tím vzniká plyn použitelný pro pohon motoru kogenerační jednotky. Pro využití vyrobeného plynu k syntéze kapalných paliv je nutno jej nejprve transformovat na tzv. syntézní plyn, což je směs vodíku a oxidu uhelnatého. To je dosaženo odstraněním vodní pár a sloučenin síry a halogenů. Následně se syntézní plyn ohřívá a stlačuje a prochází reaktorem syntézy, kde probíhají heterogenně katalyzované reakce a vzniká směs plynných, kapalných a pevných uhlovodíků a vody. Následně se tato směs dělí a čistí a výsledná kapalná frakce (surová ropa) se odesílá do rafinerie k dalšímu zpracování na dopravní paliva (benzíny, naftu, letecká paliva).

2. Popis zařízení

Celé zařízení bylo rozděleno na dva provozní soubory. Vzhledem k tomu, že je umístěno uvnitř budovy, bylo z hlediska požární bezpečnosti rozhodnuto o použití vestavby s vlastním odvětráním.



Obr.1 Schéma technologie zplyňování a syntézy kapalných paliv

V prvním provozním souboru je začleněna výroba plynu a první sekce čištění a chlazení plynu. Takto upravený plyn je připraven pro využití jako palivo v kogenerační jednotce s pístovým motorem nebo jako surovina pro druhý provozní soubor. Přebytek plynu se likviduje v dopalovací komoře.
Ve druhém provozním souboru je možno využívat plyn vyrobený v prvním provozním souboru nebo plyn připravený smícháním plynů z tlakových lahví. Surový plyn prochází druhou sekcí čištění a chlazení, následně je kompresorem stlačen na 2 MPa a ohřát na 250 - 300°C a vstupuje do reaktoru syntézy. Plynné, kapalné i tuhé produkty budou následně děleny na jednotlivé frakce. Kapalná a tuhá organická část budou dále zkoumány a testovány jako surovina pro dopravní paliva.

3. Provozní soubor I – zplyňování

Nejdůležitější součástí provozního souboru I bude generátor plynu. Jedná se o zařízení, v němž při mírném podtlaku (desítky Pa) a vysokých teplotách (750 – 1100 °C) vzniká z pevného paliva v přítomnosti zplyňovacího média (vzduch, vodní pára, kyslíko – parní směs, kyslík, vodík, oxid uhličitý) surový plyn. Vzhledem k nízkým rychlostem proudění zplyňovacího média i vyráběného plynu se jedná o reaktor s pevným ložem tzv. fix-bed. Reaktor má tepelný výkon 100 kW. Palivem budou dřevěné pelety průměru 6 – 12 mm, avšak předpokládá se, že budou testovány také pelety z agromateriálů (sláma, seno, rýže, obilí) či jiná pevná paliva (směsi biomasy s uhlím či odpady).
Vznikající plyn má různé složení dle typu zplyňování, zplyňovacího média, použitého paliva a teploty zplyňování. Reaktor je schopen pracovat ve dvou režimech – autotermním a alotermním. Při autotermním je teplo nutné pro průběh zplyňování získáváno spalováním části paliva v generátoru, zatímco při alotermním se teplo získává z vnějšího zdroje (elektrické topení, předehřáté zplyňovací médium). Hlavními složkami vznikajícího plynu jsou oxid uhelnatý a vodík, v menší míře jsou zastoupeny dusík, oxid uhličitý, vodní pára, methan a vyšší uhlovodíky. Nežádoucími složkami jsou dehtovité látky (směs vyšších organických sloučenin), prach (úlet z reaktoru, nezreagované palivo, popeloviny), sloučeniny síry a halogenů.
Vzniklý plyn je z reaktoru veden do čistící sekce přes cyklonový odlučovač hrubých částic. Dalším čistícím zařízením je dolomitový filtr. Jedná se o vyhřívanou nádobu naplněnou jemně mletým dolomitem, kterou prochází surový plyn. Na částicích dolomitu se při teplotách okolo 550 °C katalyticky rozkládají dehtovité látky a zachycuje se část prachu. V dalším zařízení tzv. horkém filtru se odlučuje prach. Znečištěný plyn prochází při teplotách vyšších než 450

°C přes filtrační elementy z keramických vláken. Na nich se usazují tuhé částice, které jsou následně protitlakem čistícího média (dusík, zemní plyn, vyčištěný plyn) odstraňovány kontinuálně z filtru tak, aby nedocházelo k nadměrnému zvyšování tlakové ztráty. V poslední části jsou vodní chladiče, které dochlazují plyn na přibližně 25.
Množství vznikajícího plynu bude přibližně 50 m^3_n za hodinu, přičemž připojená kogenerační jednotka bude mít nejvyšší výkon 28 kW_e. Celková účinnost zařízení se předpokládá vyšší než 85%.

Složení plynu [obj. %]	Zplyňovací medium				
	Vzduch	Kyslík	Směs O_2 + H_2O	Vodní pára	Vodík
Vodík	8 - 16	10 - 25	28 - 40	35 - 40	34,8
Oxid uhelnatý	10 - 18	40 - 60	15 - 25	25 - 30	4,3
Oxid uhličitý	12 - 16	15 - 30	20 - 40	20 - 25	10,1
Methan	2 - 6	< 3	5 - 8	9 - 11	50,2
Dusík	45 - 60	< 1	< 1	< 1	< 1
Uhlovodíky C_2 a vyšší	0,5 - 2	< 0,5	< 2	< 5	-
Obsah dehtu [g / m^3]	1 - 100	< 20	< 0,5	< 20	-
Výhřevnost [MJ / m^3]	4 - 7	9 - 12	10 - 14	10 - 16	> 22

Tab.1 Složení plynu a výhřevnost při různých druzích zplyňovacího média

Palivo se ze z hermeticky uzavřeného zásobníku dopravuje do reaktoru systémem šnekových dopravníků.
Vzhledem ke zkušenostem s předchozím provozem podobného zařízení předpokládáme, že při zplyňování dřevní biomasy nebude docházet k problémům se spékáním paliva. Bohužel agromateriály obsahují vyšší množství popelovin (až 20%) s nižšími teplotami tavitelnosti, což způsobuje problémy s řízením reaktoru, které může vést až k jeho zablokování struskou.

Obr.2 Pelety z pšeničné slámy a struska vzniklá při po zplyňování

4. Provozní soubor II – syntéza Fischer-Tropsch

Druhá část technologie je projektována na zpracovávání 10 m^3_n plynu za hodinu. Nejdříve plyn prochází sekcí vysoce účinného čistění (alkalickou pračkou), kde jsou odstraňovány sloučeniny síry a halogenů a také oxid uhličitý a zbývající vodní pára. Tím vzniká tzv.

syntézní plyn (syngas) tj. směs oxidu uhelnatého a vodíku. Následně je plyn veden do zásobníku, odkud je odebírán kompresorem. Po stlačení na 2 MPa a ohřátí na 250 - 300°C vstupuje do reaktoru syntézy. Jedná se o trubkové reaktory s intenzivním vodním chlazením a sypanou vrstvou katalyzátoru na bázi kobaltu a ruthenia. Při heterogenně katalyzovaných reakcích vznikají plynné, kapalné a pevné uhlovodíky a voda. Tato směs se bude následně rozdělovat a sledovat její množství a složení.

5. Bezpečnost zařízení

Vzhledem k přítomnosti výbušných a jedovatých látek, vysokých teplot a množství elektrických a mechanických zařízení se jedná o komplexní bezpečnostní problematiku.
Před uvedením zařízení do provozu se budou provádět jak individuální tak komplexní zkoušky, včetně zkoušek těsností a tlakových, RTG kontrol potrubí a aparátů a revizí. Součástí dodávky bude také kompletní dokumentace včetně návodů k obsluze a standardních postupů při obsluze zařízení. Nedílnou součástí provozu budou také pravidelné kontroly a preventivní údržba namáhaných součástí. Z tohoto pohledu se zvláštní pozornost bude věnovat zejména zplyňovacímu generátoru, dolomitovému a horkému filtru, dopalovací komoře, kompresoru a reaktoru syntézy.
Pro bezpečné najíždění a odstavování reaktoru z provozu budou vypracovány přesné postupy, které bude provádět pouze příslušně proškolený personál. Systém řízení bude sledovat všechny důležité parametry a v případě překročení nastavených limitů bude schopen provádět automaticky korekce.
Vzhledem k tomu, že bude celé zařízení osazeno množstvím měřící techniky (teploty, tlaky, průtoky) a také dálkově ovládaných armatur a aparátů, bude zařízení také vybaveno náhradním zdrojem elektrické energie pro případ výpadku distribuční sítě.
Kvůli přítomnosti jedovatých látek (zejména oxidu uhelnatého) budou v obou částech zařízení instalovány detektory. Ty budou prostřednictvím systému spojeny se systémem havarijního větrání, který bude v případě poruchy schopen spustit a řídit odvětrávání zasaženého prostoru.
Pro inertizaci potrubních tras a aparátů bude využíván dusík z tlakových lahví případně generátoru dusíku.
Celé zařízení bude pro snížení tepelných ztrát vybaveno izolací tak, aby povrchové teploty aparátů a potrubí nepřesáhly teplotu 60°C.

Závěr:

Řešení komplexní problematiky bezpečnosti provozu malých energetických zařízení představuje v současné době perspektivní odvětví, protože se v blízké budoucnosti předpokládá výrazné navýšení počtu zařízení tohoto typu nejen v naší republice, ale také v zahraničí. Proto je nutné sledovat a implementovat nejnovější poznatky z oblasti bezpečnosti do stávajících zařízení k zajištění jejich bezporuchového a efektivního provozování.

Poděkování:

Příspěvek vznikl za podpory Ministerstva školství, mládeže a tělovýchovy prostřednictvím projektu č. CZ.1.05/2.1.00/01.0036 "Inovace pro efektivitu a životní prostředí (INEF)".

ISBN 978-80-02-02505-4

BEZPEČNOST A SPOLEHLIVOST NOVÝCH TECHNOLOGIÍ
Sborník přednášek,
Kolektiv autorů
1. vydání, rok vydání 2013
vazba brožovaná, počet stran 20