

5 TECHNOLOGICKÁ RIZIKA A PRŮMYSLOVÁ BEZPEČNOST

*Petr Skřehot, Vilém Sluka, Jan Bumba,
Miloš Paleček, Šárka Vlková*

5.1 Průmyslová bezpečnost

5.1.1 Úvod do prevence závažných havárií

Prevencí závažných havárií rozumíme systém zaměřený na snižování pravděpodobnosti vzniku průmyslových havárií, způsobených vybranými nebezpečnými chemickými látkami a chemickými přípravky, a závažnosti jejich dopadů na životy a zdraví lidí (uvnitř podniku i z řad obyvatelstva), na hospodářská zvířata, na složky životního prostředí a na majetek. Systém prevence závažných havárií je na celostátní úrovni zabezpečován Ministerstvem životního prostředí jako součást civilního nouzového plánování státu.

Základní terminologie

Systém prevence závažných průmyslových havárií na základě Směrnice Rady 96/82/ES (SEVESO II) zavedl novou terminologii. Tato terminologie je převzata do české verze zákona č. 59/2006 Sb., o prevenci závažných havárií. Některé pojmy ovšem představují přesné definice pro účely pouze tohoto zákona (např. s ohledem na zařazování do skupin rizikových podniků atd.). Je třeba vyvarovat se jejich zaměňování s podobnými pojmy z jiných systémů, které mohou mít jiný význam a byly určeny k jiným účelům. Proto je dále uveden výčet základních pojmů zákona č. 59/2006 Sb. Jedná se o následující pojmy:

- **Objekt** – celý prostor, popřípadě soubor prostorů, v němž je umístěna jedna nebo více nebezpečných látek v jednom nebo více zařízeních, včetně společných nebo souvisejících infrastruktur a činností, v užívání právnických osob a podnikajících fyzických osob.
- **Zařízení** – technická nebo technologická jednotka, ve které je nebezpečná látka vyráběna, zpracovávána, používána, přepravována nebo skladována, a která zahrnuje také všechny části nezbytné pro provoz, například stavební objekty, potrubí, skladovací tankoviště, stroje, průmyslové dráhy a nákladové prostory.
- **Provozovatel** – právnická osoba nebo podnikající fyzická osoba, která užívá nebo bude užívat objekt nebo zařízení, v němž je nebo bude vyráběna, zpracovávána, používána, přepravována nebo skladována nebezpečná látka

v množství stejném nebo větším, než je množství uvedené v příloze č. 1 k tomuto zákonu v části 1 sloupci 1 tabulky I nebo tabulky II, nebo který byl zařazen do skupiny A nebo skupiny B rozhodnutím krajského úřadu.

- **Nebezpečná látka** – vybraná nebezpečná chemická látka nebo chemický přípravek, uvedené v příloze č. 1 k tomuto zákonu v části 1 tabulce I nebo splňující kritéria stanovená v příloze č. 1 k tomuto zákonu v části 1 tabulce II a přítomné v objektu nebo zařízení jako surovina, výrobek, vedlejší produkt, zbytek nebo meziprodukt, včetně těch látek, u kterých se dá důvodně předpokládat, že mohou vzniknout v případě havárie.
- **Závažná havárie** – mimořádná, částečně nebo zcela neovladatelná, časově a prostorově ohraničená událost, například závažný únik, požár nebo výbuch, která vznikla nebo jejíž vznik bezprostředně hrozí v souvislosti s užíváním objektu nebo zařízení, v němž je nebezpečná látka vyráběna, zpracovávána, používána, přepravována nebo skladována, a vedoucí k vážnému ohrožení nebo k vážnému dopadu na životy a zdraví lidí, hospodářských zvířat a životní prostředí nebo k újmě na majetku.
- **Zdroj rizika** (nebezpečí) – vlastnost nebezpečné látky nebo fyzická či fyzikální situace vyvolávající možnost vzniku závažné havárie.
- **Riziko** – pravděpodobnost vzniku nežádoucího specifického účinku, ke kterému dojde během určité doby nebo za určitých okolností.
- **Skladování** – umístění určitého množství nebezpečných látek pro účely uskladnění, uložení do bezpečného opatrování nebo udržování v zásobě.
- **Domino efekt** – možnost zvýšení pravděpodobnosti vzniku nebo velikosti dopadů závažné havárie v důsledku vzájemné blízkosti objektů, nebo zařízení nebo skupiny objektů nebo zařízení a umístění nebezpečných látek.
- **Umístění nebezpečné látky** – projektované množství nebezpečné látky, která je nebo bude vyráběna, zpracovávána, používána, přepravována nebo skladována v objektu nebo zařízení, nebo která se může nahromadit v objektu nebo zařízení při ztrátě kontroly průběhu průmyslového chemického procesu nebo při vzniku závažné havárie.
- **Zóna havarijního plánování** – území v okolí objektu nebo zařízení, v němž krajský úřad, v jehož působnosti se nachází objekt nebo zařízení, uplatňuje požadavky havarijního plánování formou vnějšího havarijního plánu.
- **Scénář** – variantní popis rozvoje závažné havárie, popis rozvoje příčinných a následných na sebe navazujících a vedle sebe i posloupně probíhajících událostí, a to buď spontánně probíhajících, a nebo probíhajících jako činnosti lidí, které mají za účel zvládnout průběh závažné havárie.

5.1.2 Legislativní rámec

Právní úprava Evropské unie

Právní úprava problematiky prevence závažných havárií má v Evropské unii pětadvacetiletou historii. Její počátky je však nutno hledat již v 70. letech 20. století. Když se v roce 1976 stala nehoda v italském chemickém závodě ICMESO v Sevesu, při které uniklo do ovzduší asi 20 kilogramů silně toxických dioxinů, nikdo již nepochyboval o tom, že na rozvoj chemického průmyslu musí reagovat i právní úprava, která by podobným událostem dokázala účinně předcházet. Státy tehdejšího Evropského společenství (ES) proto přijaly jednotnou filozofii pro prosazování aktivní prevence průmyslových havárií, jež vyústily v přijetí směrnice 82/501/EEC, která je často označovaná jako směrnice SEVESO I. Základní teze této směrnice lze shrnout následovně (Česká společnost chemického inženýrství, on line):

- Nejlepší politikou je prevence možných nehod přímo u zdroje (technický pokrok je potřeba řídit s ohledem na nutnou ochranu životního prostředí).
- Požadavky na bezpečnost je třeba integrovat ve všech stádiích vzniku a technického života zařízení (vývoji, projekci, konstrukci, provozu, intenzifikaci i po ukončení životnosti, tj. při likvidaci).
- U nebezpečných průmyslových činností je potřeba věnovat pozornost ochraně veřejnosti a životního prostředí.
- Provozovatel je povinen učinit veškerá opatření pro předcházení nehodám.
- Provozovatel je povinen poskytnout kompetentním orgánům podrobné informace o látkách, procesu a zařízeních a o krocích směřujících ke snížení rizika a následků.
- Všechny osoby mimo objekt musí být vhodným způsobem informovány o bezpečnostních opatřeních v případě závažné havárie.
- Členské státy musejí předávat komisi ES informace o závažných nehodách.
- Neomezuje se právo členských států přijímat opatření zajišťující vyšší stupeň ochrany člověka a životního prostředí.
- Komise poskytne členským státům souhrnné informace o závažných nehodách.
- Členské státy musí sdělit ustanovení přijatá v rámci národní legislativy pro tuto oblast.

Jak se však postupem času ukázalo, řada bodů nebyla dostatečně řešena a situace si vyžádala přijetí nové, opravené směrnice. Tato potřeba vyplynula zejména ze zkušeností získaných implementací direktivy SEVESO I a dále z havárií, které se staly v období po jejím přijetí. Byla proto přijata nová směrnice 96/82/EC, která bývá

označována jako direktiva SEVESO II (Zákon č. 59/2006 Sb., v platném znění). Směrnice SEVESO II přinesla tyto hlavní změny (Česká společnost chemického inženýrství, online):

- Rozsah působnosti byl rozšířen a zjednodušen – je odkazováno na přítomnost nebezpečných látek v podniku – množství překračující určité limitní hodnoty (SEVESO I poukazovala pouze buď na látky ve spojení s určitými průmyslovými činnostmi, nebo na oddělené skladování látek).
- Opakovaně stanovuje opatření, která musí přijmout provozovatelé podniků, aby předešli závažným haváriím a omezili jejich následky, a nově bylo zahrnuto ustanovení o „přístupu k prevenci závažných havárií“. (Záměrem je zdůraznit závazek provozovatelů podniků ve smyslu zavedení systémů řízení bezpečnosti jako nejdůležitějšího prvku k dosažení vysoké úrovně ochrany z hlediska prevence závažných havárií.)
- Zvýšený důraz na opatření pro minimalizaci dopadů závažných havárií na životní prostředí včetně havarijního plánování a územního plánování, identifikaci možných domino efektů, informování veřejnosti tam, kde je to přiměřené, včetně sousedních států (viz „UN ECE’s Convention on the Transboundary Effects of Industrial Accidents“ = Úmluva o účincích průmyslových havárií překračujících hranice států, také zvaná Helsinská úmluva, podepsána 17. 3. 1992).
- Podrobné stanovení povinností pověřených úřadů ve vztahu k hodnocení bezpečnostních zpráv (čl. 9.4) a zvláště ve vztahu k ustavení systému inspekce nebo jiných kontrolních opatření, která jsou definovaná podrobně v článku 18 směrnice.
- Právní základ směrnice SEVESO I byl v člancích 100 a 235 Římské smlouvy, protože účelem této směrnice je prevence závažných havárií a harmonizace úsilí v tomto oboru v rámci Společenství, aby byly eliminovány výrazné rozdíly v opatřeních pro prevenci závažných havárií, které by mohly záporně ovlivnit fungování společného trhu.
- Právní základ směrnice SEVESO II je v článku 130 o ochraně životního prostředí, který bere v úvahu novou legislativu Evropské unie o ochraně zdraví pracovníků a bezpečnosti práce, která vešla v platnost od přijetí směrnice SEVESO I, zvláště pak směrnici 89/391/EHS.

Další právní úpravou, kterou si vyžádaly okolnosti, byla směrnice 2003/105/ES. Ta upravila směrnici SEVESO II tak, že zahrnula do oblasti řešené direktivou SEVESO II také těžební činnosti, skladování odpadů, a také rozšířila tuto směrnici o nové poznatky z toxikologie karcinogenních látek. Potřeba zakomponovat tyto úpravy do společné evropské legislativy vyplynula zejména ze zkušeností, které odhalily havárie v Aznalcollár (Španělsko, 1998), v Baia Mare (Rumunsko, 1999), v Enschede (Holandsko, 2000), či v Toulouse (Francie, 2001) (Bartlová, 2002).

Právní úprava v České republice

Před vstupem České republiky do EU u nás existoval v podstatě jediný předpis, který danou problematiku řešil. Tímto předpisem byla instrukce Ministerstva obrany ČSSR č. CO-51-5 z roku 1981, která jako jediná stanovovala povinnosti na úseku havarijní připravenosti. Ačkoli se jednalo o instrukci určenou pro složky civilní ochrany, aplikována byla i na průmyslové podniky. Obsahovala celkem dvanáct hlavních průmyslových toxických látek uvedených v tomto pořadí: chlór, amoniak, kyanovodík, formaldehyd, fosgen, sirovodík, sirouhlík, oxid siřičitý, fluorovodík, chlorovodík, chlorid fosforitý, nitrózní plyny (z hlediska toxicity nebo početnosti výskytu na teritoriu státu). Pomůcka obsahovala mimo jiné požadavky na havarijní plán objektu, kde byla specifikována obecná a grafická část plánu, poplachové směrnice, plán vyrozumění a spojení a plán havarijních prací.

V polovině 90. let 20. století, tedy dlouho před vstupem ČR do EU, však byl zahájen proces přibližování národní legislativy s právem Evropského společenství, který pro oblast prevence závažných havárií vyvrcholil dne 30. 12. 1999, kdy byl přijat zákon č. 353/1999 Sb., o prevenci závažných havárií. Jeho účinnost byla stanovena od 29. ledna 2000. Důležitou skutečností v tomto ohledu je, že tento zákon do českého právního řádu implementoval obě směrnice direktivy SEVESO. Tento krok představoval tedy zásadní milník v této oblasti u nás.

Účelem zákona bylo deklarovat požadavky pro předcházení závažným haváriím, což představovalo stanovení povinností příslušným podnikům, jež splňovaly podmínku pro tzv. zařazení (tj. na které se dle příslušných kritérií tento zákon vztahoval), vytvořit systém prevence vzniku závažných havárií, včetně požadavků pro nakládání s vybranými nebezpečnými chemickými látkami. Konkrétně zákon upravoval:

- Povinnosti právnických nebo fyzických osob oprávněných k podnikání při prevenci vzniku závažných havárií.
- Způsob zařazení podniku do příslušných skupin (podle množství a druhu nebezpečné látky).
- Zvláštní požadavky pro stanovení občanskoprávní zodpovědnosti za škody vzniklé v důsledku závažné havárie.
- Poskytování informací veřejnosti.
- Výkon státní správy na úseku prevence.

K zákonu č. 353/1999 Sb. byly vydány také příslušné prováděcí předpisy:

- Nařízení vlády č. 6/2000 Sb., kterým se stanoví způsob hodnocení bezpečnostního programu prevence závažné havárie a bezpečnostní zprávy, obsah ročního plánu kontrol, postup při provádění kontroly, obsah informace a obsah výsledné zprávy o kontrole.

- Vyhláška č. 7/2000 Sb., kterou se stanoví rozsah a způsob zpracování hlášení o závažné havárii a konečné zprávy o vzniku a následcích závažné havárie.
- Vyhláška č. 8/2000 Sb., kterou se stanoví zásady hodnocení rizik závažné havárie, rozsah a způsob zpracování bezpečnostního programu prevence závažné havárie a bezpečnostní zprávy, zpracování vnitřního havarijního plánu, zpracování podkladů pro stanovení zóny havarijního plánování a pro vypracování vnějšího havarijního plánu a rozsah a způsob informací určených veřejnosti a postup při zabezpečování informování veřejnosti v zóně havarijního plánování.

Vstupem České republiky do Evropské unie však proces úpravy legislativy zdaleka neskončil. V roce 2004 byl přijat zákon č. 349/2004 Sb. K tomuto zákonu byly také přijaty zcela nové prováděcí předpisy, kterými byly:

- Vyhláška č. 366/2004 Sb., o některých podrobnostech systému prevence závažných havárií.
- Vyhláška č. 367/2004 Sb., kterou se mění vyhláška č. 7/2000 Sb., kterou se stanoví rozsah a způsob zpracování hlášení o závažné havárii a konečné zprávy o vzniku a následcích závažné havárie.
- Vyhláška č. 373/2004 Sb., kterou se stanoví podrobnosti o rozsahu bezpečnostních opatření fyzické ochrany objektu nebo zařízení zařazených do skupiny A nebo do skupiny B.
- Nařízení vlády č. 452/2004 Sb., kterým se stanoví způsob hodnocení bezpečnostních programů prevence závažné havárie a bezpečnostní zprávy, obsah ročního plánu kontrol, postup při provádění kontroly, obsah informace a obsah výsledné zprávy o kontrole.

V roce 2003 přijala EU směrnici 2003/105/ES, která byla věnována problematice nakládání s chemickými látkami, a která upravovala také směrnici SEVESO II. V reakci na to bylo nutné opětovně provést změny v české legislativě, což představovalo přijetí nového zákona č. 59/2006 Sb., o prevenci závažných havárií. K tomuto zákonu byly opět přijaty zcela nové prováděcí předpisy, které jsou uvedeny níže, a jsou v současnosti platné. Jedná se o:

- Vyhlášku č. 103/2006 Sb., o stanovení zásad pro vymezení zóny havarijního plánování a o rozsahu a způsobu vypracování vnějšího havarijního plánu.
- Vyhlášku č. 250/2006 Sb., kterou se stanoví rozsah a obsah bezpečnostních opatření fyzické ochrany objektu nebo zařízení zařazených do skupiny A nebo do skupiny B.
- Vyhlášku č. 256/2006 Sb., o podrobnostech systému prevence závažných havárií.

- Vyhlášku č. 255/2006 Sb., o rozsahu a způsobu zpracování hlášení o závažné havárii a konečné zprávy o vzniku a dopadech závažné havárie.

Důležitou skutečností je, že zákon č. 59/2006 Sb. se nevztahuje na:

- Vojenské objekty a vojenská zařízení.
- Nebezpečí spojená s ionizujícím zářením.
- Silniční, drážní, leteckou a vodní přepravu vybraných NCHL mimo objekty a zařízení, včetně dočasného skladování, nakládky a vykládky během přepravy.
- Přepravu vybraných NCHL v potrubích, včetně souvisejících přečerpávacích, kompresních a předávacích stanic postavených mimo objekt a zařízení v trase potrubí.
- Dobývání ložisek nerostů v dolech, lomech nebo prostřednictvím vrtů, s výjimkou povrchových objektů, a zařízení chemické a termické úpravy a zušlechťování nerostů, skladování a ukládání materiálů na odkaliště.
- Průzkum a dobývání nerostů na moři.
- Skládky odpadu.

5.1.3 Základní povinnosti provozovatelů

K základním povinnostem provozovatelů podle zákona patří:

- Zařazení subjektu do působnosti zákona.
- Oznámení o návrhu zařazení objektu nebo zařízení do příslušné skupiny A nebo B.
- Analýza a hodnocení rizik závažné havárie.
- Zpracování bezpečnostního programu prevence závažné havárie nebo zpracování bezpečnostní zprávy.
- Zpracování plánu fyzické ochrany objektu nebo zařízení.
- Zpracování vnitřního havarijního plánu.
- Zpracování podkladů pro stanovení zóny havarijního plánování a pro vypracování vnějšího havarijního plánu.
- Sjednání pojištění odpovědnosti za škody vzniklé v důsledku závažné havárie.
- Poskytování informací o vzniku a dopadech závažné havárie.

Základní postup plnění povinností provozovatelů a příslušných orgánů státní správy, které jsou uvedeny v příslušných paragrafech zákona, je obsahem příloh zákona a prováděcích předpisů k zákonu. Jedná se o:

- Přílohu č. 1 k zákonu č. 59/2006 Sb. – Minimální množství nebezpečných látek, která jsou určující pro zařazení objektu nebo zařízení do skupiny A nebo skupiny B a pro sčítání poměrného množství nebezpečných látek.
- Přílohu č. 2 k zákonu č. 59/2006 Sb. – Vzor návrhu na zařazení objektu nebo zařízení do skupiny A nebo skupiny B.
- Přílohu č. 3 k zákonu č. 59/2006 Sb. – Kritéria vymezující závažnou havárii podle jejích následků pro zpracování informace o vzniku a následcích závažné havárie.
- Vyhlášku č. 103/2006 Sb., o stanovení zásad pro vymezení zóny havarijního plánování a o rozsahu a způsobu vypracování vnějšího havarijního plánu.
- Vyhlášku č. 250/2006 Sb., kterou se stanoví rozsah a obsah bezpečnostních opatření fyzické ochrany objektu nebo zařízení zařazených do skupiny A nebo do skupiny B.
- Nařízení vlády č. 254/2006 Sb., o kontrole nebezpečných látek.
- Vyhlášku č. 255/2006 Sb., o rozsahu a způsobu zpracování hlášení o závažné havárii a konečné zprávy o vzniku a dopadech závažné havárie.
- Vyhlášku č. 256/2006 Sb., o podrobnostech systému prevence závažných havárií.
- Zákon č. 267/2006 Sb., o změně zákonů souvisejících s přijetím zákona o úrazovém pojištění zaměstnanců – (část patnáctá).

5.1.4 Zařazení subjektu do působnosti zákona

Právníká osoba nebo podnikající fyzická osoba, která užívá objekt nebo zařízení, je povinna zařadit objekt nebo zařízení do příslušné skupiny v případě, kdy množství nebezpečné látky umístěné v objektu nebo zařízení je stejné nebo větší, než je množství uvedené v příslušných tabulkách přílohy č. 1 k zákonu.

Je-li v objektu nebo zařízení umístěno více nebezpečných látek v množství menším, než je uvedeno v příslušných tabulkách přílohy č. 1 k zákonu, musí každá právnická osoba nebo podnikající fyzická osoba, která užívá takový objekt nebo zařízení, provést součet poměrných množství umístěných nebezpečných látek podle níže uvedeného vzorce.

$$N = \sum_{i=1}^n \frac{q_i}{Q_i}, \quad (5-1)$$

kde q_i je množství nebezpečné látky i umístěné v objektu nebo zařízení (t), Q_i je příslušné množství nebezpečné látky i (t) uváděné v části 1 přílohy 1 zákona č. 59/2006 Sb., resp. jako limitní množství nebezpečné látky.

Pravidla pro zařazení objektu do skupiny A resp. B

Zařazení objektu nebo zařízení do skupiny A se provede tehdy pokud:

- množství nebezpečné látky umístěné v objektu nebo zařízení je stejné nebo větší, než je množství uvedené v příloze č. 1 k zákonu 59/2006 Sb. v části 1 sloupci 1 tabulky I nebo tabulky II a současně je menší než je množství uvedené v příloze č. 1 v části 1 sloupci 2 tabulky I nebo tabulky II, nebo
- v případě, že není dosaženo množství nebezpečné látky podle zákona, součet poměrných množství nebezpečných látek zjištěný podle přílohy č. 1 k zákonu 59/2006 Sb. v části 1 tabulce I a tabulce II podle vzorce a za podmínek uvedených v příloze č. 1 k zákonu v části 2 je roven nebo je větší než 1.

Zařazení objektu nebo zařízení do skupiny B se provede tehdy pokud:

- množství nebezpečné látky umístěné v objektu nebo zařízení je stejné nebo větší, než je množství uvedené v příloze č. 1 k zákonu č. 59/2006 Sb. v části 1 sloupci 2 tabulky I nebo tabulky II, nebo
- v případě, že není dosaženo množství nebezpečné látky podle zákona, součet poměrných množství nebezpečné látky zjištěný podle přílohy č. 1 k tomuto zákonu v části 1 tabulce I a tabulce II podle vzorce a za podmínek uvedených v příloze č. 1 k tomuto zákonu v části 2 je roven nebo je větší než 1.

Pravidlo pro výpočet poměru N dle rovnice 5-1 se postupně použije pro vyhodnocení zdroje rizika souvisejícího s toxicitou, hořlavostí a ekologickou toxicitou:

- Pro sčítání látek a přípravků jmenovitě uvedených v tabulce I a klasifikovaných jako T nebo T+ spolu s látkami a přípravky klasifikovanými jako T nebo T+⁴⁴.
- Pro sčítání látek a přípravků jmenovitě uvedených v Tabulce I a klasifikovaných jako O, E, F, nebo F+, spolu s látkami a přípravky klasifikovanými jako O, E, F, nebo F+⁴⁴.
- Pro sčítání látek a přípravků uvedených v tabulce I a klasifikovaných jako N (R50, R50/53 nebo R51/53), spolu s látkami a přípravky uvedenými a klasifikovanými jako N⁴⁴.

⁴⁴ T – toxický, T+ – silně toxický, O – oxidující, E – výbušný, F – hořlavý, F+ – vysoce hořlavý, N – nebezpečný pro životní prostředí.

Dále platí, že nebezpečná látka umístěná v objektu nebo zařízení pouze v množství stejném nebo menším než 2 % množství nebezpečné látky uvedené v tabulce I nebo tabulce II nebude pro účely výpočtu celkového množství nebezpečné látky uvažována, pokud její umístění v objektu nebo zařízení je takové, že nemůže působit jako iniciátor závažné havárie nikde na jiném místě objektu nebo zařízení. Pokud nebezpečné látky uvedené v tabulce I náleží také do některé skupiny s vybranou nebezpečnou vlastností uvedenou v tabulce II, použije se pro jejich zařazení do skupiny A nebo skupiny B množství uvedené v tabulce I. Jde-li o nebezpečnou látku, která má více nebezpečných vlastností uvedených v tabulce II, použije se pro její zařazení do skupiny A nebo B nejnižší množství z množství uvedených u jejích nebezpečných vlastností v tabulce II.

Oznámení návrhu zařazení objektu nebo zařízení do příslušné skupiny

V případě, že právnická osoba nebo podnikající fyzická osoba, která splnila povinnosti podle odstavců 1 a 2, zjistí, že se na ni nevztahují povinnosti podle tohoto zákona, je povinna tuto skutečnost protokolárně zaznamenat, kopii zaslat krajskému úřadu a předložit kontrolním orgánům podle § 22, včetně identifikace a množství umístěných nebezpečných látek.

Návrh na zařazení objektu nebo zařízení do příslušné skupiny je dokument, jímž provozovatel oznámí krajskému úřadu základní identifikační údaje o objektu nebo zařízení, uvede v něm seznam umístěných nebezpečných látek podle jejich druhu a množství, návrh zařazení objektu nebo zařízení do skupiny A nebo B.

Návrh zařazení je provozovatel povinen zpracovat podle vzoru uvedeného v příloze č. 2 zákona a předložit krajskému úřadu v jednom písemném výtisku a v elektronické podobě. Návrh na zařazení je provozovatel nového objektu nebo zařízení povinen doručit krajskému úřadu současně s podáním na stavební úřad návrhu na zahájení územního řízení o jeho umístění, popřípadě žádosti o stavební povolení stavby nebo její změny nebo žádosti o dodatečné povolení stavby v případě, kdy se územní rozhodnutí nevydává.

Krajský úřad návrh zařazení objektu nebo zařízení do skupiny A nebo B posoudí a vyhodnotí možnosti vzniku domino efektu vyplývajícího z polohy okolních objektů nebo zařízení a z druhu a množství v nich umístěné nebezpečné látky. Na základě návrhu zařazení a vyhodnocení možnosti vzniku domino efektu vydá krajský úřad právnické osobě nebo podnikající fyzické osobě, která užívá určený objekt nebo zařízení, rozhodnutí o zařazení tohoto objektu do skupiny A nebo do skupiny B; přitom není vázán tím, zda právnické osoby nebo podnikající fyzické osoby navrhly zařadit alespoň jeden z posuzovaných objektů nebo zařízení do skupiny A nebo do skupiny B.

5.1.5 Bezpečnostní dokumentace

Systém prevence závažných havárií vyžaduje, aby provozovatel zpracoval soubor dokumentace, která bývá často hovorově nazývána „bezpečnostní dokumentace“. Konkrétně se jedná o:

- Bezpečnostní program nebo bezpečnostní zprávu.
- Vnitřní havarijní plán.
- Podklady pro stanovení zóny havarijního plánování.
- Informace pro veřejnost žijící v zóně havarijního plánování.

Provozovatel prostřednictvím bezpečnostní dokumentace seznamuje a přesvědčuje státní správu a občany v okolí objektu nebo zařízení, včetně svých zaměstnanců:

- ... že ví co, kde a kolik „toho nebezpečného“ má,
- ... že zná kvalifikovaný odhad, co „to nebezpečné“ může za určitých okolností udělat,
- ... že provedl kvalifikovaný odhad, jak asi často se „to“ může stát,
- ... že je na „to“ připraven,
- ... že dělá opatření, aby „to“ bylo menší, a aby byla co nejmenší pravděpodobnost, že se „to“ stane, pokud se tomu nedá vyhnout,
- ... že veškerá činnost v objektu nebo zařízení se provádí v duchu bezpečného počínání.

V praktické rovině se jedná o to, aby provozovatel doložil, že provedl:

- Identifikaci nebezpečí (zdrojů rizik), analýzu, ocenění a hodnocení rizik, stanovení opatření k omezení rizik a příslušnou havarijní přípravu.
- Zavedení systému řízení bezpečnosti, vycházející z celkových cílů a zásad prevence závažné havárie.
- Zpracování příslušné bezpečnostní dokumentace (za použití již platných dokumentů provozovatele, rozšířených nebo dopracovaných podle této legislativy).

Zpracování analýzy a hodnocení rizik závažné havárie

Provozovatel je povinen provést analýzu a hodnocení rizik závažné havárie. Analýza a hodnocení rizik závažné havárie musí zahrnovat zejména:

- Identifikaci zdrojů rizik (nebezpečí).
- Určení možných scénářů událostí a jejich příčin, které mohou vyústit v závažnou havárii.

- Odhad dopadů možných scénářů závažných havárií na zdraví a životy lidí, hospodářská zvířata, životní prostředí a majetek.
- Odhad pravděpodobností scénářů závažných havárií.
- Stanovení míry rizik.
- Hodnocení přijatelnosti rizik vzniku závažných havárií.

Zpracování bezpečnostního programu prevence závažné havárie

Bezpečnostní program prevence závažné havárie představuje dokument zpracovaný provozovatelem, který stanoví systém řízení bezpečnosti v objektu nebo zařízení. Provozovatel objektu nebo zařízení zařazeného ve skupině A je povinen zpracovat bezpečnostní program a podle něj postupovat. V programu je provozovatel povinen uvést:

- Zásady prevence závažné havárie.
- Strukturu a systém řízení bezpečnosti zajišťující ochranu zdraví a životů lidí, hospodářských zvířat, životního prostředí a majetku.

Provozovatel je povinen na základě sdělení krajského úřadu do programu zahrnout preventivní bezpečnostní opatření vztahující se k možnému vzniku domino efektu. Provozovatel stávajícího objektu nebo zařízení je povinen předložit program ke schválení krajskému úřadu. Provozovatel, který bude zřizovat nový objekt nebo nové zařízení výstavbou nebo změnou užívání, je povinen předložit program ke schválení krajskému úřadu spolu s prohlášením o předložení návrhu na vydání územního rozhodnutí o umístění objektu nebo zařízení, popřípadě o předložení žádosti o stavební povolení nebo žádosti o dodatečné povolení stavby v případě, kdy územní rozhodnutí nebylo vydáno.

Provozovatel je dále povinen prokazatelně seznámit zaměstnance v potřebném rozsahu se schváleným programem a ostatní fyzické osoby zdržující se v objektu nebo u zařízení prokazatelně v potřebném rozsahu informovat o rizicích závažné havárie, o preventivních bezpečnostních opatřeních a o jejich žádoucím chování v případě vzniku závažné havárie.

Provozovatel je povinen bezodkladně zajistit aktualizaci programu po každé změně druhu nebo množství umístěné nebezpečné látky přesahujícím 10 % dosavadního množství anebo po každé změně technologie, ve které je nebezpečná látka použita, nebo po organizačních změnách, pokud tato změna vede ke změně bezpečnosti užívání objektu nebo zařízení. Aktualizaci je provozovatel povinen do jednoho měsíce ode dne nastalé změny předložit krajskému úřadu ke schválení. Užívání nového objektu nebo zařízení nesmí být zahájeno, dokud rozhodnutí o schválení programu krajským úřadem nenabude právní moci. Provozovatel nového objektu nebo zařízení je povinen vypracovat a předložit návrh bezpečnostního programu ke schválení kraj-

skému úřadu nejpozději 3 měsíce před uvedením nového objektu nebo zařízení do zkušebního provozu; v případě, kdy se zkušební provoz neprovádí, ve stejné lhůtě před uvedením do užívání.

Zpracování bezpečnostní zprávy

Provozovatel objektu nebo zařízení je povinen zpracovat bezpečnostní zprávu a podle ní postupovat v případě zařazení objektu nebo zařízení do skupiny B. Bezpečnostní zpráva je provozovatelem zpracovaný dokument, ve kterém provozovatel v jednotlivých kapitolách uvede:

- Informace o systému řízení u provozovatele s ohledem na prevenci závažné havárie.
- Informace o složkách životního prostředí v lokalitě objektu nebo zařízení.
- Technický popis objektu nebo zařízení.
- Postup a výsledky identifikace zdrojů rizika (nebezpečí), analýz a hodnocení rizik a metody prevence.
- Opatření pro ochranu a zásah k omezení dopadů závažné havárie.
- Aktualizovaný seznam nebezpečných chemických látek v podniku.
- Jmenovitě uvedené právnické osoby a fyzické osoby, podílející se na vypracování bezpečnostní zprávy.

Provozovatel stávajícího objektu nebo zařízení je povinen předložit bezpečnostní zprávu krajskému úřadu ke schválení. Provozovatel, který bude zřizovat nový objekt nebo nové zařízení výstavbou nebo změnou užívání, je povinen předložit bezpečnostní zprávu ke schválení spolu s prohlášením o předložení návrhu na vydání územního rozhodnutí o umístění objektu nebo zařízení, popřípadě o předložení žádosti o stavební povolení nebo o dodatečné povolení stavby v případě, kdy územní rozhodnutí nebylo vydáno.

Užívání nového objektu nebo zařízení nesmí být zahájeno, dokud rozhodnutí o schválení bezpečnostní zprávy krajským úřadem nenabude právní moci. Provozovatel nového objektu nebo zařízení, které je stavbou, je povinen předložit ke kolaudačnímu řízení pravomocné rozhodnutí krajského úřadu o schválení bezpečnostní zprávy. Toto rozhodnutí je provozovatel povinen předložit též k žádosti o povolení změny v užívání stavby, pokud by nový účel užívání stavby souvisel s umístěním nebezpečné látky uvedené v příloze č. 1 k zákonu.

Provozovatel je povinen bezodkladně zajistit aktualizaci bezpečnostní zprávy po každé změně druhu nebo množství umístěné nebezpečné látky přesahujícím 10 % dosavadního množství anebo po každé změně technologie, ve které je nebezpečná látka použita, nebo po organizačních změnách, pokud tyto změny vedou ke změně

bezpečnosti užívání objektu nebo zařízení. Aktualizaci je provozovatel povinen do jednoho měsíce ode dne nastalé změny předložit krajskému úřadu ke schválení.

Provozovatel je povinen zajistit posouzení bezpečnostní zprávy nejpozději do 5 let ode dne jejího schválení, aktualizace nebo předchozího posouzení a předložit v této lhůtě krajskému úřadu zprávu o výsledku tohoto posouzení k evidenci a archivaci.

Provozovatel je povinen na základě sdělení krajského úřadu zahrnout do bezpečnostní zprávy preventivní bezpečnostní opatření vztahující se k možnému vzniku domino efektu v důsledku polohy objektu nebo zařízení, ve vztahu k jinému objektu nebo zařízení, v němž je umístěna nebezpečná látka v množství stejném nebo nižším, než je množství uvedené v příloze č. 1 k zákonu, nebo vzájemným působením těchto objektů nebo zařízení.

Provozovatel nového objektu nebo zařízení je povinen vypracovat a předložit návrh bezpečnostní zprávy ke schválení krajskému úřadu nejpozději 3 měsíce před uvedením nového objektu nebo zařízení do zkušebního provozu; v případě, kdy se zkušební provoz neprovádí, ve stejné lhůtě před uvedením do užívání.

Provozovatel může z výtisků návrhu bezpečnostního programu, bezpečnostní zprávy a vnějšího havarijního plánu nebo z jejich aktualizace, do nichž bude umožněno veřejné nahlížení, vypustit po projednání s krajským úřadem údaje, jejichž zveřejnění by mohlo vést k vyzrazení obchodního tajemství, utajovaných skutečností anebo zvláštních skutečností, z důvodů veřejné bezpečnosti nebo důvodů obrany státu. Tyto údaje musí být uvedeny ve výtiscích opatřených na titulní straně datem a podpisem statutárního orgánu, které provozovatel zasílá krajskému úřadu pro potřeby vydání souhlasu.

Zpracování plánu fyzické ochrany

Provozovatel objektu nebo zařízení, jež je zařazeno do skupiny A nebo B, je povinen zpracovat plán fyzické ochrany objektu nebo zařízení (dále jen „plán fyzické ochrany“). V plánu fyzické ochrany uvede bezpečnostní opatření, kterými jsou:

- Analýza možností neoprávněných činností a provedení případného útoku na objekty nebo zařízení.
- Režimová opatření.
- Fyzická ostraha.
- Technické prostředky.

Plán fyzické ochrany a jeho změny zasílá provozovatel objektu nebo zařízení krajskému úřadu a Policii České republiky na vědomí. Provozovatel je povinen přijmout

a zajistit bezpečnostní opatření pro fyzickou ochranu objektů nebo zařízení uvedená v plánu fyzické ochrany, k zabránění vzniku závažných havárií a omezení jejich důsledků na zdraví a životy lidí, hospodářská zvířata, životní prostředí a majetek.

Funkčnost bezpečnostních opatření, včetně funkčních zkoušek poplachového systému, je provozovatel povinen prověřit nejméně jedenkrát ročně. O provedených funkčních zkouškách provede zápis, který uchovává po dobu 3 let.

O bezpečnostních opatřeních obsažených v plánu fyzické ochrany jsou povinni zaměstnanci provozovatele, zaměstnanci orgánů veřejné správy a jiné osoby, které se s nimi seznámili v souvislosti s plněním pracovních povinností, zachovávat mlčenlivost a neposkytovat o nich informace podle zvláštního zákona. Povinnost mlčenlivosti trvá i po skončení pracovního poměru nebo příslušných prací.

Náležitosti bezpečnostních opatření stanoví provozovatel vnitřním předpisem v rozsahu stanoveném prováděcím právním předpisem.

Zpracování vnitřního havarijního plánu

Provozovatel, který zpracovává bezpečnostní zprávu, je povinen zpracovat vnitřní havarijní plán. Vnitřní havarijní plán stanoví opatření uvnitř objektu nebo zařízení při vzniku závažné havárie vedoucí ke zmírnění jejích dopadů. Ve vnitřním havarijním plánu musí provozovatel uvést:

- Jména, příjmení a funkční zařazení fyzických osob, které mají pověření provozovatele realizovat preventivní bezpečnostní opatření.
- Scénáře možných havárií, scénáře odezvy na možné havárie, scénáře řízení odezvy na možné havárie a matice odpovědnosti za jednotlivé fáze odezvy na možné havárie.
- Popis možných dopadů závažné havárie.
- Popis činností nutných ke zmírnění dopadů závažné havárie.
- Přehled ochranných zásahových prostředků, se kterými disponuje provozovatel.
- Způsob vyrozumění dotčených orgánů veřejné správy a varování osob.
- Opatření pro výcvik a plán havarijních cvičení.
- Opatření k podpoře zmírnění dopadů závažné havárie mimo objekt a spolupráci se složkami integrovaného záchranného systému.

Ostatní plány pro řešení mimořádných událostí zpracované provozovatelem a schválené podle zvláštních předpisů jsou součástí vnitřního havarijního plánu a tvoří samostatné přílohy. Provozovatel stávajícího objektu nebo zařízení je povinen předložit

vnitřní havarijní plán k evidenci a archivaci a popřípadě k dalšímu využití pro účely sestavení vnějšího havarijního plánu krajskému úřadu. Provozovatel je povinen:

- Zajistit aktualizaci vnitřního havarijního plánu do 1 měsíce po každé změně druhu nebo množství umístěné nebezpečné látky přesahujícím 10 % dosavadního množství nebo po každé změně technologie, ve které je nebezpečná látka použita, pokud tyto změny vedou ke změně bezpečnosti užívání objektu nebo zařízení, a při organizačních změnách ovlivňujících systém zajištění bezpečnosti.
- Předložit krajskému úřadu neprodleně aktualizaci vnitřního havarijního plánu k evidenci a archivaci a popřípadě k dalšímu využití pro účely sestavení vnějšího havarijního plánu.
- Zahrnout na základě rozhodnutí krajského úřadu do vnitřního havarijního plánu preventivní bezpečnostní opatření vztahující se k možnosti vzniku domino efektu.
- Zvažovat ve vnitřním havarijním plánu také opatření na zmírnění dopadů závažné havárie a souvislosti umístění objektu nebo zařízení vzhledem k dopravní nebo technické infrastruktuře, sídelním útvarům nebo významným krajinným prvkům, zvláště chráněným územím a územím soustavy NATURA 2000.
- Zajistit prověření vnitřního havarijního plánu z hlediska jeho aktuálnosti nejméně jednou za 3 roky ode dne, kdy se stal vnitřní havarijní plán platným dokumentem. Tento den musí být v dokumentu vyznačen včetně podpisu oprávněné fyzické osoby.
- Prokazatelně seznámit zaměstnance a ostatní fyzické osoby zdržující se v objektu nebo u zařízení o rizicích závažné havárie, o preventivních bezpečnostních opatřeních a o žádoucím chování v případě vzniku závažné havárie.
- Uložit vnitřní havarijní plán tak, aby byl dostupný osobám, které mají pověření realizovat opatření vnitřního havarijního plánu a provádět kontroly.
- Postupovat podle vnitřního havarijního plánu v případě, kdy závažnou havárii nelze odvrátit nebo k závažné havárii již došlo.

Provozovatel nového objektu nebo zařízení zařazeného do skupiny B je povinen vypracovat a předložit krajskému úřadu vnitřní havarijní plán k evidenci a uložení a písemné podklady pro stanovení zóny havarijního plánování a vypracování vnějšího havarijního plánu nejpozději 3 měsíce před uvedením nového objektu nebo zařízení do zkušebního provozu; v případě, kdy se zkušební provoz neprovádí, ve stejné lhůtě před uvedením do užívání.

Zpracování podkladů pro stanovení zóny havarijního plánování a pro vypracování vnějšího havarijního plánu

Provozovatel, který zpracovává bezpečnostní zprávu, je povinen:

- Vypracovat a předložit krajskému úřadu písemné podklady pro stanovení zóny havarijního plánování a pro vypracování vnějšího havarijního plánu současně s předložením bezpečnostní zprávy.
- Spolupracovat s krajským úřadem a jím pověřenými organizacemi a institucemi na zajištění havarijní připravenosti v oblasti vymezené vnějším havarijním plánem.

Písemné podklady pro stanovení zóny havarijního plánování a pro vypracování vnějšího havarijního plánu musí obsahovat zejména:

- Identifikační údaje provozovatele.
- Jméno a příjmení fyzické osoby odpovědné za zpracování podkladů.
- Popis závažné havárie, která může vzniknout v objektu nebo zařízení a jejíž dopady se mohou projevit mimo objekt nebo zařízení.
- Přehled možných dopadů závažné havárie na život a zdraví lidí, hospodářská zvířata, životní prostředí a majetek, včetně způsobů účinné ochrany před těmito dopady.
- Přehled preventivních bezpečnostních opatření ke zmírnění dopadů závažné havárie.
- Seznam a popis technických prostředků využitelných při odstraňování následků závažné havárie, které jsou umístěny mimo objekt nebo zařízení provozovatele.
- Další nezbytné údaje vyžádané krajským úřadem (například podrobnější specifikaci technických prostředků na odstraňování dopadů závažné havárie, podrobnější plán únikových cest a evakuačních prostorů), a dále údaje vyžádané podle zvláštního právního předpisu.

Provozovatel je povinen předložit krajskému úřadu podklady pro stanovení zóny havarijního plánování a pro vypracování vnějšího havarijního plánu nejpozději 3 měsíce před uvedením nového objektu nebo zařízení do zkušebního provozu a v případě, kdy se zkušební provoz neprovádí, ve stejné lhůtě před uvedením do užívání. Krajský úřad stanoví zónu havarijního plánování a vypracuje pro ni vnější havarijní plán. Při vypracování vnějšího havarijního plánu musí vyhodnotit možnost vzniku domino efektu a přihlížet k oprávněným připomínkám veřejnosti a obcí v zóně havarijního plánování, jakož i k vyjádřením dotčených orgánů veřejné správy. Podle vnějšího havarijního plánu krajský úřad postupuje v případě, kdy závažnou havárii nelze od-

vrátit nebo k závažné havárii již došlo. Krajský úřad zašle vnější havarijní plán po jeho schválení územně příslušným základním složkám integrovaného záchraného systému.

Sjednání pojištění odpovědnosti za škody vzniklé v důsledku závažné havárie

Provozovatel je povinen sjednat pojištění odpovědnosti za škody vzniklé v důsledku závažné havárie do 100 dnů od nabytí právní moci rozhodnutí krajského úřadu o schválení bezpečnostního programu nebo bezpečnostní zprávy; výše limitu pojistného plnění sjednaného provozovatelem musí odpovídat rozsahu možných dopadů závažné havárie, které jsou uvedeny ve schváleném bezpečnostním programu nebo ve schválené bezpečnostní zprávě. Provozovatel má povinnost být pojištěn podle předchozího odstavce po celou dobu užívání objektu nebo zařízení, po kterou splňuje podmínky pro zařazení objektu nebo zařízení do skupiny A nebo B, a po celou dobu zkušebního provozu podle následujícího třetího odstavce.

Provozovatel je povinen sjednat pojištění před uvedením nového objektu nebo zařízení do zkušebního provozu; není-li zkušební provoz prováděn, postupuje provozovatel podle prvního odstavce. Výše limitu pojistného plnění sjednaného provozovatelem pro etapu zkušebního provozu musí odpovídat rozsahu možných dopadů závažné havárie stanovených na základě výsledku analýzy a hodnocení rizik, předložené krajskému úřadu pro účely územního řízení nebo vydání stavebního povolení (§ 21 odst. 1).

Výše pojistné částky navržená provozovatelem musí odpovídat rozsahu možných dopadů závažné havárie, které jsou vyjádřeny ve schváleném programu nebo ve schválené bezpečnostní zprávě. Provozovatel je povinen předat krajskému úřadu ověřenou kopii smlouvy o pojištění podle prvního odstavce, a jejích změn nejpozději do 30 dnů ode dne jejího uzavření. Provozovatel je povinen předat krajskému úřadu ověřenou kopii smlouvy o pojištění sjednané podle třetího odstavce před zahájením zkušebního provozu objektu nebo zařízení. Provozovatel je povinen bezodkladně oznámit krajskému úřadu každou změnu v pojištění.

Poskytování informací o vzniku a dopadech závažné havárie

Právnícká osoba nebo podnikající fyzická osoba, v jejímž objektu nebo zařízení došlo k závažné havárii, je povinna tuto skutečnost bezodkladně ohlásit příslušnému krajskému úřadu, dotčeným orgánům veřejné správy podle zvláštního právního předpisu a dotčeným obcím v případě, že následky závažné havárie splňují kritéria stanovená v příloze č. 3 k zákonu č. 59/2006 Sb., je právnícká osoba nebo podnikající fyzická osoba povinna doručit krajskému úřadu písemné hlášení o vzniku závažné havárie do 24 hodin od jejího vzniku; konečnou písemnou zprávu o vzniku a dopadech závažné havárie je povinna doručit krajskému úřadu nejpozději do 3 měsíců od vzniku závažné havárie.

Státní správa a dozor

Státní správu na úseku prevence závažných havárií vykonávají:

- Ministerstvo životního prostředí.
- Ministerstvo vnitra.
- Česká inspekce životního prostředí.
- Krajské úřady.
- Český báňský úřad.
- Správní úřady odborného dozoru nad bezpečností práce a technických zařízení (Státní úřad inspekce práce prostřednictvím svých oblastních inspektorátů).
- Správní úřady na úseku požární ochrany.
- Krajské hygienické stanice.

5.1.6 Prevence závažných havárií z pohledu provozovatele technologie s identifikovaným rizikem

Technici, kteří pracují s chemickými látkami v laboratoři i ve výrobě, si riziko havárie vždy uvědomovali a vždy si kladli otázky: „K jaké nehodě nebo havárii může při dané činnosti dojít, co může nehodu nebo havárii způsobit, jak se dá riziková situace včas rozpoznat, jaké může mít důsledky, jak je možné havárii či nehodě zabránit, či jak je možné důsledky havárie zmírnit?“ Podat odpovědi na tyto otázky je podstatou analýzy a hodnocení rizika spojeného s provozováním dané hodnocené výroby a je podstatou činností spojených s analýzou rizika. Úloha analýzy rizika byla v minulosti „interní záležitostí“ techniků. V současné době se stala analýza rizika legislativním úkonem. Důvody k vypracování analýzy a hodnocení rizik lze tedy z pohledu provozovatele shrnout následovně:

- Analýza a hodnocení rizika je předepsána zákonem, její forma je určena vyhláškou a metodickými pokyny; výsledek musí být projednán a schválen státními správními orgány.
- Analýzu rizika vyžadují někdy i pojišťovny, u nichž se musí výrobce pojistit proti havárii (pojištění je povinné, plyne ze současné legislativy). I pojišťovny někdy předepisují způsob provádění analýzy a hodnocení rizika havárie, a podle výsledku analýzy rizika někdy upravují poplatky za pojištění (předepisována je někdy metoda HAZOP).
- Analýza a hodnocení rizika havárie je významným podkladem pro jednání výrobců (provozovatelů) s veřejností v okolí výroby.
- Analýza a hodnocení rizika jsou podkladem k jednání s aktivistickými organizacemi.

V uvedených povinnostech vypracovat analýzu a hodnocení rizika se často ztrácí skutečnost, že na zabránění vzniku havárie má zájem především výrobce, protože každá havárie představuje finanční a morální ztrátu. Současně je nutné si uvědomit, že postup analýzy rizika a formu prezentace analýzy rizika je nutné přizpůsobit cíli analýzy. Není tedy možné vypracovat jednotné schéma analýzy rizika. Klíčovým a nejobtížnějším problémem analýzy a hodnocení rizik, který řadí analýzu a hodnocení rizika na pomezí mezi technickou prací a věštěním, je nutnost zpracovávat údaje dramaticky se odlišující v úrovni spolehlivosti.

Klasifikace zdrojů ohrožení podle mechanismu možné havárie

Možný účinek zdroje ohrožení je extenzivní veličinou, malý reaktor představuje menší zdroj rizika než reaktor velký. Přesto je výhodné klasifikovat zdroje ohrožení podle mechanismu havárie, kterou mohou vyvolat. Následující mechanismy jsou přibližně seřazeny podle nebezpečnosti daného mechanismu. Při hodnocení je účelné hodnotit:

- Možnost včas vznik havárie rozpoznat.
- Možnost vývoj havárie zastavit.
- Možný externí domino efekt.
- Možný účinek na obyvatele.
- Možný účinek na životní prostředí.

Odhad účinku možné havárie – analýza scénářů

Pro analýzu průběhu a účinku havárie je zaveden termín „scénář havárie“. Což je představa o tom, jak by mohla havárie probíhat, a jaký by mohla mít účinek. Analýza scénářů je pomůckou pro odhad možných účinků havárie. Problém analýzy rizika je v tom, že vytváření scénářů je někdy závislé na technických znalostech, technických zkušenostech a fantazii technika, který rizika analyzuje. Pro stejný typ mechanismu havárie v daném zařízení je možné často vytvořit sérii scénářů od zcela neškodných, až po katastrofické. Příkladem může být únik hořlavého plynu ze zásobníku zkapalněného plynu. V takovém případě připadají v úvahu tyto možnosti:

- Plyn uniká velmi pomalu a rozptýlí se v ovzduší bez významných škodlivých důsledků.
- Plyn nebo disperze (oblak, mlha) uniká rychle a vytvoří hořlavý oblak málo promíchaný se vzduchem, který po případné iniciaci shoří formou ohňové koule, která působí na okolí sáláním tepla a může iniciovat další požáry.
- Plyn nebo disperze unikají rychle a vytvoří explozivní oblak dokonale promíchaný se vzduchem, který po případné iniciaci exploduje a působí na okolí destruktivní tlakovou vlnou.

Nejistota v spektru uvažovaných scénářů může být sporným bodem diskuse mezi výrobcem a veřejností či aktivistickými organizacemi, kdy výrobce dává přednost méně nebezpečným scénářům (tzv. scénáře nejpravděpodobnější), zatímco aktivistické organizace často dávají přednost scénářům katastrofickým (tzv. scénáře nejzávažnější). Řešení sporu je velmi složité, protože vytváření scénářů a jejich hodnocení je proces, který je možné označit termínem „co kdyby“.

5.2 Analýza a hodnocení technologických rizik

5.2.1 Výklad pojmů nebezpečí a zdroj rizik

Každé zařízení, zvláště pak takové, ve kterém probíhá určitý fyzikální nebo chemický proces spojený s výměnou nebo transformací energie anebo se změnou chemické podstaty vstupujících látek, představuje určité **nebezpečí**. Může-li toto nebezpečí (které již není jen latentní vlastností vyplývající ze samotné existence daného zařízení, nýbrž z podstaty v něm probíhajících fyzikálních a chemických procesů) vést ke vzniku mimořádné události s nežádoucími následky na životy a zdraví lidí, hospodářských zvířat, na složky životního prostředí a na majetek, je dané zařízení považováno za **zdroj (technologických) rizik**.

S pojmy nebezpečí a zdroj rizik se ale můžeme setkávat v mnoha různých souvislostech napříč mnoha obory. Aby se čtenář lépe v tomto směru orientoval, je v tabulce 38 uveden výčet definic tohoto pojmu, které byly čerpány z různých oficiálních i neoficiálních a českých i zahraničních zdrojů, které jsou zde uvedeny.

Pojem nebezpečí je podle očekávání definován několika způsoby v závislosti na zdroji, resp. oboru. Obecně lze rozlišovat různé definice tohoto pojmu podle typu očekávaných následků, jež s konkrétním nebezpečím souvisí. Tento rozdíl je patrný například u formulací č. 1 (popřípadě č. 24) a č. 6 uvedených v tabulce 36, kdy v jedné je bráno nebezpečí jako zdroj potenciálního zranění nebo poškození zdraví a v další formulaci jako zdroj škody, kde nejsou dané následky dále specifikovány. Nebezpečí je také odlišně definováno jako vnitřní vlastnost látky (viz položky č. 3 a č. 8) a dále pak jako situace nebo činnost (viz položka č. 25). Tento rozdíl je možné přisuzovat odlišnému pohledu na zdroj daného nebezpečí, kterým může být v praktickém životě téměř jakýkoliv předmět, látka či situace, jak je bohužel někdy patrné až při vzájemné kombinaci několika definic pojmu nebezpečí. Výše uvedené nesrovnalosti potvrzuje následující mezioborové porovnání definic tohoto pojmu. Podle očekávání byly ve výkladu určité rozdíly. První dvě formulace se týkají toxikologického hlediska (viz položky č. 18 a č. 19), dále pak definice z oblasti strojního průmyslu podle normy ČSN EN ISO 14121-1 o bezpečnosti strojních zařízení (viz položka č. 22) a závěrem definice používána Hasičským záchranným sborem České republiky (viz položka č. 17). Z porovnání je zřejmé, že v rámci toxikologického pohledu je nebezpečím vlastnost látky, u strojních zařízení je zdrojem nebezpečí nějaká mechanická nebo elektrická složka zařízení a hasiči definují nebezpečí jako

Tabulka 38: Definice pojmu nebezpečí.

Číslo	Definice	Zdroj
1	Zdroj možného zranění nebo poškození zdraví.	[1]
2	Zdroj potencionálního poškození nebo situace s potencionální možností úrazu, zranění nebo jiného poškození zdraví, je to zdroj ohrožení.	[1]
3	Vnitřní (vrozená) vlastnost látky, zdroje energie nebo fyzikální situace, které mají potenciál způsobit nežádoucí následky (zranění lidí, škodu na majetku, škodu na životním prostředí nebo jejich kombinaci). Nebezpečí je zdrojem rizik. ^a	[1]
4	Stav nebo podmínky, ve kterých je zranění nebo poškození zdraví nebo majetku nebo prostředí bezprostřední.	[1]
5	Používáno ve slovních spojeních typu „nebezpečná látka – dangerous substance“.	[1]
6	Potenciální zdroj škody.	[1]
7	Vnitřní vlastnost činitele nebo situace mající potenciál způsobit nepříznivé jevy, pokud je organismus, systém nebo část populace vystavena tomuto činiteli.	[2]
8	Vnitřní vlastnost nebezpečné látky nebo fyzické/fyzikální situace, s možností vzniku poškození lidského zdraví anebo životního prostředí.	[2] ^a
9	Chemická nebo fyzická/fyzikální podmínka (stav, okolnost), která má potenciál způsobovat škodu lidem, životnímu prostředí nebo na majetku.	[2]
10	Zdrojem nebezpečí může být cokoli – pracovní materiály, technické zařízení, pracovní metody nebo postupy – vše, co může způsobit újmu.	[3]
11	Potenciální zdroj poškození. Poznámka: Termín zahrnuje jak nebezpečí pro osoby, ke kterému dochází v časově krátké době (např. požár a výbuch), tak i nebezpečí s dlouhodobým účinkem na zdraví (např. uvolnění toxických látek).	[4]
12	Jakákoliv existující nebo možná podmínka, která může způsobit úraz, onemocnění nebo smrt obsluhy, ztráty nebo poškození systému, zařízení nebo majetku nebo poškodit prostředí. Možné nebezpečné podmínky mají za následek poruchy, selhání, vnější události, chyby nebo jejich kombinace.	[5]
13	Zdroj možného zranění nebo poškození zdraví. Poznámka: Pojem „nebezpečí“ je obvykle používáno ve spojení s dalšími slovy, která definují původ nebo charakter očekávaného zranění nebo poškození zdraví – např. nebezpečí zasažení elektrickým proudem, nebezpečí stlačení, nebezpečí otravy, atd.	[6]
14	Vlastnost nebezpečné látky nebo fyzická či fyzikální situace vyvolávající možnost vzniku závažné havárie. Nebezpečí je vlastnost látky nebo jevu/děje/faktoru způsobit neočekávaný negativní jev – latentní vlastnost objektu. Jako objekty je třeba zahrnovat veškeré technické zařízení, látky a materiály, organizaci práce a jiné činnosti, které mohou ohrozit zdraví a životy lidí, způsobit materiální škody anebo poškodit životní prostředí. Je to vlastnost „vrozená“ (daný subjekt jí nelze zbavit), projev se však pouze tehdy, je-li člověk jejímu vlivu vystaven (je exponován). Synonymem je pojem zdroj rizika.	[7]

^a Vnitřní vlastnost je taková vlastnost, která je vrozená, látce vlastní, která je s existencí látky neoddělitelně spojena. Výsledné „chování“ látky je tedy dáno jejími fyzikálními, chemickými a toxikologickými vlastnostmi [2].

Číslo	Definice	Zdroj
15	Bezprostřední rizika, která způsobí vážné narušení zdraví nebo smrt.	[8]
16	Nenadálé ohrožení života nebo majetku či nepřipustnou kombinaci nebezpečnosti/risku, která vznikla porušením opatření o bezpečnosti.	[9]
17	Situace, která může být příčinou škody nebo poškození zdraví člověka.	[10]
18	Soubor chemických, fyzikálních a biologických vlastností látek determinuje nebezpečnost chemické látky, tj. její schopnost mít nepříznivý (toxický) účinek na živé organismy. Nebezpečnost je neoddělitelně spojena s existencí chemické látky. Je latentní vlastností každé chemické substance či jejich směsí, ale projevit se může pouze tehdy, jestliže je jejímu působení vystaven živý organismus, tedy dojde-li k expozici organismu chemickou látkou. Pojem nebezpečnost je ovšem širší než pojem toxicita. Chemické látky mohou být nebezpečné i jiným způsobem než tím, že jsou toxické. Nebezpečné mohou být hořlaviny výbušniny, žíraviny apod.	[11]
19	Nebezpečností škodliviny se označuje její schopnost vyvolat poškození zdraví. Toto nebezpečí je tím větší, čím je menší rozdíl mezi neúčinnou a účinnou dávkou, čím je účinná dávka nižší, čím jsou účinky ireverzibilnější a obtížněji léčebně zvládnutelné a čím jsou menší (nebo žádné) varovné příznaky škodliviny (zákeřnost působení).	[12]
20	Obecně představuje nebezpečí zdroj, situaci nebo činnost s potenciálem způsobit vznik škody (poranění člověka, poškození jeho zdraví, poškození životního prostředí atd.).	[13]
21	Nebezpečí (příp. někdy uváděný pojem nebezpečnost) je vlastnost látky nebo fyzikálního či biologického jevu/děje/faktoru nebo stav systému, který působí nepříznivě na zdraví člověka, životní prostředí a materiální hodnoty. Je to vlastnost „vrozená“ (daný subjekt jí nelze zbavit), projeví se však pouze tehdy, je-li člověk nebo jiný cíl jejímu vlivu vystaven (je exponován). Nebezpečí je zdrojem rizika	[14]
22	Potencionální zdroj škody. Termín „nebezpečí“ může být blíže určen tak, aby byl definován jeho původ (např. mechanické nebezpečí, elektrické nebezpečí) nebo druh potencionální škody (např. úraz elektrickým proudem, nebezpečí říznutí, nebezpečí otravy, nebezpečí požáru). Nebezpečí může být buď nepřetržitě přítomné během předpokládaného používání stroje, nebo se může objevit neočekávaně.	[15]
23	Potencionální zdroj škody. Termín nebezpečí může být doplněn přívlastkem tak, že definuje svůj původ nebo povahu očekávané škody (např.: nebezpečí elektrického šoku, nebezpečí stlačení, nebezpečí stříhu, toxické nebezpečí, nebezpečí požáru, nebezpečí utopení).	[16]
24	Vnitřní potenciál, který může způsobit fyzické zranění nebo poškození zdraví lidí.	[17]
25	Zdroj, situace nebo činnost s potenciálem způsobit vznik poranění člověka nebo poškození zdraví nebo jejich kombinaci.	[18]
26	Nebezpečí je definováno jako potencionální schopnost způsobení škody (poškození, zranění). Např. pohyb je nebezpečí. Zdrojem nebezpečí je vozidlo a škoda je smrtelný úraz způsobený srážkou. Nebezpečí nemusí nutně znamenat skutečný výskyt škody (ublížení) nebo vysokou pravděpodobnost škody.	[19]

Číslo	Definice	Zdroj
27	Nebezpečí definujeme jako potenciální škodu vyplývající ze skutečných vlastností nebo uspořádání něčeho k tomu, aby způsobilo škodu.	[19]
28	Nebezpečí představuje potenciál pro nějakou činnost, stav, okolnost nebo změnu podmínek vedoucí ke škodlivým účinkům.	[20]
29	Nebezpečí je „předpoklad/stav nebo změna sady okolností, které představují potenciál pro zranění, nemoc nebo škodu na majetku“. To je „potenciální nebo základní charakteristický rys nějaké činnosti, stavu nebo okolnost, která může způsobit nepříznivé či škodlivé následky“.	[20]
30	Nebezpečí je situace, která představuje určitou úroveň ohrožení života, zdraví, majetku nebo životního prostředí. Největší nebezpečí jsou skrytá nebo potenciální, pouze s teoretickým rizikem škody. Nicméně jednou se stane nebezpečí „aktivním“, což může způsobit nehodovou situaci.	[21]
31	Nebezpečí je potencionálním zdrojem škody.	[22]
32	Nebezpečí je často zaměňováno s termínem riziko. Vysoké napětí a vzorek radioaktivního materiálu nebo toxická chemikálie mohou představovat nebezpečí, což znamená, že představují potenciální zdroj škody. Nebezpečí představuje u karcinogenu a koncentrované kyseliny nebo výbušniny základní vlastnosti těchto materiálů. ^b	[23]

^b Riziko (ang. risk) je kombinace pravděpodobnosti výskytu škody a závažnosti této škody [1].

situaci. Za zamyšlení stojí také značná podobnost formulací č. 22 a č. 23, které jsou převzaty z materiálů Českého normalizačního institutu. Ač se jedná o dva rozdílné materiály, je zde zřejmá pozitivní podobnost formulací pojmu nebezpečí v rámci jedné organizace.

V souvislosti s definicí č. 3, která říká, že „Nebezpečí je zdrojem rizik“, respektive č. 14 „Synonymem je pojem zdroj rizika“, bychom zde měli zvážit také výklady pojmu zdroj rizika. V tabulce 39 jsou opět prezentovány definice, se kterými se můžeme setkávat v provozní praxi nejčastěji.

Důležitým poznatkem je, že definice č. 1, (viz tabulka 39) uvádí jako nebezpečí i jednání člověka, řízení a sociální podmínky, na což by mělo být v průmyslové praxi pamatováno a tyto podmínky zohledňovány i v analýze a hodnocení rizik.

Z definic uvedených v tabulce 38 je patrné, že s nebezpečím úzce souvisí i pojmy **nebezpečná látka** a **nebezpečnost chemické látky**. Jelikož tento pojem se v průmyslové bezpečnosti hojně využívá, je na místě shrnout příslušné definice také k tomuto pojmu (viz tabulka 40).

Tabulka 39: Definice pojmu zdroj rizik.

Číslo	Definice	Zdroj
1	Všechny jevy, předměty, skutečnosti atd., které zvyšují nebezpečnost systému. Jsou to příčiny i zdroje úrazů, jednání člověka, nebezpečné faktory, sociální podmínky, řízení, motivace, konstrukce apod.	[1]
2	Podstatná (vnitřní) vlastnost nebezpečné látky nebo fyzikální situace, která má potenciál způsobit škodu lidskému zdraví, životnímu prostředí nebo na majetku, popř. jejich kombinace. Zdroj rizika může realizovat svůj potenciál např. vznikem požáru, výbuchu, toxického úniku, zamoření životního prostředí nebo jiného nežádoucího projevu.	[1]
3	Zdrojem rizika (nebezpečím) je vlastnost nebezpečné látky nebo fyzická či fyzikální situace vyvolávající možnost vzniku závažné havárie.	[24]

Tabulka 40: Definice pojmu nebezpečná látka.

Číslo	Definice	Citace
1	Látka, která je svými fyzikálními, chemickými a toxickými vlastnostmi schopna nebezpečně působit na osoby, živé organismy, životní prostředí a majetek (látka výbušná, podporující hoření, lehce vznětlivá, hořlavá, jedovatá, žíravá, dráždivá atd.).	[1]
2	Jakýkoliv chemický nebo biologický prostředek, který je nebezpečný zdraví, například látky nebo preparáty klasifikované jako velmi toxické, toxické, škodlivé, leptavé (žíravé), dráždivé, senzitivní (senzibilující), karcinogenní, mutagenní, teratogenní, patogenní, dusivé.	[1]
3	Nebezpečná chemická látka nebo chemický přípravek, které vykazují jednu nebo více nebezpečných vlastností klasifikovaných podle zákona o chemických látkách.	[1]
4	Látka, která na základě svých fyzikálních nebo chemických vlastností vytváří riziko.	[1]
5	Nebezpečné látky nebo nebezpečné přípravky jsou látky nebo přípravky, které za podmínek stanovených tímto zákonem mají jednu nebo více nebezpečných vlastností, pro které jsou klasifikovány jako: výbušné, oxidující, extrémně hořlavé, vysoce hořlavé, hořlavé, vysoce toxické, toxické, zdraví škodlivé, žíravé, dráždivé, senzibilující, karcinogenní, mutagenní, toxické pro reprodukci a nebezpečné pro životní prostředí.	[25]

Tabulka 41: Uvedení příslušných odkazů na zdroje citované v tabulkách 38 až 40.

Zdroj	Citace
[1]	Encyklopedie BOZP [online]. Praha: Výzkumný ústav bezpečnosti práce, 2008- [cit. 2009-05-07]. Dostupný na www: < http://www.bozpinfo.cz/knihovna-bozp/encyklopedie/ >
[2]	PALEČEK Miloš et al., Prevence rizik. 1. vyd. Praha: Oeconomica, 2006. 256 s. ISBN 80-245-1117-7.
[3]	Evropská agentura pro bezpečnost a ochranu zdraví při práci. Definice [online]. 2007 [cit. 2009-05-05]. Dostupný z WWW: < http://osha.europa.eu/cs/topics/riskassessment/definitions >.
[4]	ČSN EN 61511-1: Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových procesů – Část 1: Požadavky na systémy hardwaru a softwaru, struktura, definice.
[5]	ERICSON A. C. Hazard Analysis Techniques for System Safety, New Jersey: John Wiley and sons, Inc., 2005.
[6]	ČSN EN 292-1: Bezpečnost strojních zařízení. Základní pojmy, všeobecné zásady pro projektování. Část 1: Základní terminologie, metodologie.
[7]	BERNATÍK Aleš. Prevence závažných havárií I. 1. vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2006. 86 s. ISBN 80-86634-89-2.
[8]	Multi klima s. r. o. Multi klima: Ke stažení [online]. 2003-2009 [cit. 2009-05-05]. Dostupný z WWW: < http://www.multiklima.cz/wp-content/uploads/File/ke-stazeni/klimatizace-pro-firmy/R407C/Manual.Utopia.pdf >.
[9]	Tlak s. r. o.: oborový portál pro vyhrazená tlaková zařízení – kotle, tlakové nádoby, potrubí a nízkotlaké kotelní – Právní a technické předpisy [online]. 2005-2008 [cit. 2009-05-05]. Dostupný z WWW.
[10]	Hasičský záchranný sbor Královéhradeckého kraje: Sbírka interních aktů řízení generálního ředitele hasičského záchranného sboru České republiky [online]. 2006 [cit. 2009-05-06]. Dostupný z WWW: < http://www.hzshk.cz/priloha/prilohy/rad_technicke_sluzby.doc >.
[11]	PATOČKA Jiří. Úvod do obecné toxikologie [online]. Jihočeská univerzita v Českých Budějovicích, [cit. 2009-05-06]. Dostupný z WWW: < http://www.zsf.jcu.cz/struktura/katedry/radio/informace-pro-studenty/ucebni_texty/obec_toxi/obecna_toxikologie_i.htm >.
[12]	RUSEK Vlastimil. Základy toxikologie a úvod do problematiky hygieny a bezpečnosti práce v chemické laboratoři [online]. Univerzita Pardubice – Ústav ochrany životního prostředí, 2001 [cit. 2001-05-06]. Dostupný z WWW: < http://webak.upce.cz/~uozp/skripta/uozp-skripta-tox-rusek.pdf >.
[13]	HOREHLEDOVÁ Šárka. Management nebezpečných chemických látek v průmyslu. Zpráva projektu „Rozvoj sítě environmentálních poradenských a informačních center Moravskoslezského kraje“. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2007. 20 s.
[14]	BABINEC F. Management rizika: učební text. Brno: Slezská univerzita v Opavě, Ústav matematiky, 2005.

Zdroj	Citace
[15]	ČSN EN ISO 14121-1. Bezpečnost strojních zařízení – Posouzení rizika – Část 1: Zásady. Praha: Český normalizační institut, 2008.
[16]	ČNI Pokyn ISO/IEC 73:2002. Management rizika – Slovník – Směrnice pro používání v normách. Praha: Český normalizační institut, 2008.
[17]	ILO-OSH 2001: Metodické návody pro systémy řízení bezpečnosti a ochrany zdraví při práci. Praha: Českomoravská konfederace odborových svazů, 2001.
[18]	ČSN OHSAS 18001:2008. Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky. Praha: Český normalizační institut, 2008.
[19]	KUMAMOTO, Hiromitsu. Satisfying Safety Goals by Probabilistic Risk Assessment. Hoang Pham. 1st edition. London: Springer, 2007. 253 s. ISBN 978-1-84628-681-0.
[20]	BRAUER Roger. Safety and health for engineers. 2nd edition. [s.l.]: John Wiley and Sons, 2006. 756 s. ISBN 0-471-29189-7.
[21]	Wikipedia, the free encyclopedia: Hazard [online]. 2009 [cit. 2009-05-07]. Dostupný z WWW: < http://en.wikipedia.org/wiki/Hazard >.
[22]	AGIUS, Raymond. Health, Environment & Work: Hazard and Risk, Definition [online]. 2005-2009 [cit. 2009-05-07]. Dostupný z WWW: < http://www.agius.com/hew/resource/hazard.htm >.
[23]	The Physical and Theoretical Chemistry Laboratory: Chemical and Other Safety Information [online]. 2009 [cit. 2009-05-06]. Dostupný z WWW: < http://msds.chem.ox.ac.uk/glossary/risk.html >.
[24]	Zákon č. 59/2006 Sb., O prevenci závažných havárií, v platném znění.
[25]	Zákon č. 356/2003 Sb., O chemických látkách a přípravcích, v platném znění.

5.2.2 Technologická zařízení

Objekty nebo zařízení s nebezpečnými látkami

Základním údajem pro analýzu je přehled objektů nebo zařízení s uvedením druhu a množství v nich umístěných nebezpečných látek. Procesy probíhají v zařízeních, která můžeme rozdělit na **operační jednotky** a **operační síť**. Operační jednotky můžeme rozdělit podle druhu dějů, které v nich probíhají, na tři druhy:

- **Reaktory**, ve kterých vedle fyzikálních jevů probíhají i chemické reakce, např. různé reaktory trubkové, míchané, kolonové, fluidní, zkrápěné, dále elektrolyzéry, zařízení na zneškodňování odpadů založené na chemické reakci, apod.
- **Aparáty**, v nichž probíhají pouze fyzikální děje (hydrodynamické pochody, tepelné pochody, difúzní pochody, mechanické pochody), např. čerpadla, kompresory, odstředivky, míchadla, výměníky tepla, vařáky, kondenzátory, odparky, destilační a rektifikační kolony, absorbéry, extraktory, mísiče v potrubní síti apod.

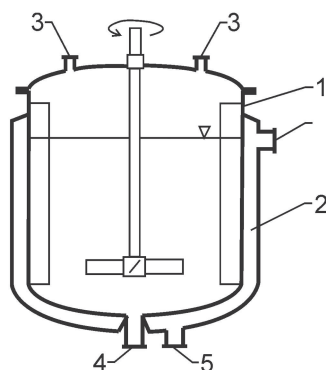
- **Rezervoáry**, ve kterých dochází pouze k akumulaci hmoty nebo energie, např. zásobníky, rekuperátory, stabilní a dočasné sklady, zařízení spojená se skladováním, usazovací nádrže apod.

Operační síť je tvořena potrubím, které spojuje aparáty mezi sebou nebo jednotky s okolím. Jednotky v procesu jsou spojeny sériově, paralelně, recyklem nebo obtokem. Znázornění spojení je provedeno různými schématy, např. proudovým (blokovým) schématem, strojně-technologickým schématem (Process Flow Diagram – PFD), provozním schématem toku energií a pomocných látek, potrubním schématem s údaji o měření a regulaci (Piping and Instrumentation Diagram – P&ID) apod. Pomocí těchto diagramů je třeba určit, popř. zkontrolovat, všechna z hlediska zákona důležitá zařízení, která jsou potřeba pro provozování činnosti provozovatele. Nesmí se zapomenout ani na situace, kdy z různých důvodů se mohou vyskytnout různá množství nebezpečných látek přítomných v automobilových a železničních cisternách dočasně přítomná na parkovištích a železničních vlečkách v objektu provozovatele, a na provozy, které se zabývají shromažďováním, úpravou nebo zneškodňováním odpadů.

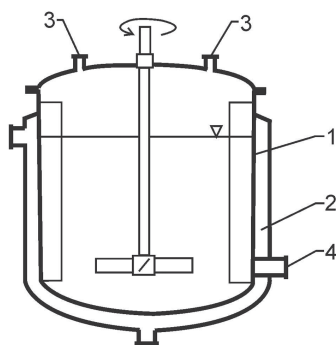
Chemické reaktory

Reaktor je zařízení, ve kterém se průmyslově realizují chemické reakce. V praxi se používá velké množství různých typů chemických reaktorů. Používané reaktory lze dělit podle různých hledisek:

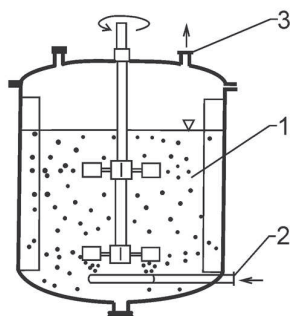
- Podle výskytu fází reagujících složek se dělí na:
 - Homogenní – reagující složky jsou přítomny jen v jedné fázi (kapalné, plynné, tuhé) a výchozí složky i produkty reakce jsou navzájem mísitelné.
 - Heterogenní – reagující složky jsou přítomny minimálně ve dvou fázích (plyn – kapalina, plyn – tuhá látka, kapalina – tuhá látka).
- Podle způsobu provozu se dělí na:
 - Reaktory vsádkové – (diskontinuální), s přetržitým provozem (viz obrázek 87).
 - Reaktory průtočné – (kontinuální), s nepřetržitým provozem (viz obrázek 88).
 - Reaktory poloprůtočné – jedna z reagujících složek je přiváděna kontinuálně (viz obrázek 89).
 - Reaktory s cirkulací – ke vstupnímu proudu je přidávána část výstupního proudu (viz obrázek 90).



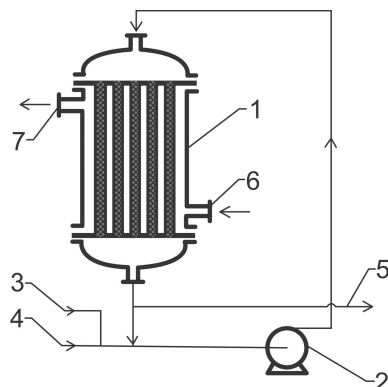
Obrázek 87: Vsádkový míchaný reaktor, 1 – nádoba reaktoru, 2 – plášť, 3 – reaktanty, 4 – produkty (po reakci), 5 – přívod teplosměnného média, 6 – odvod teplosměnného média.



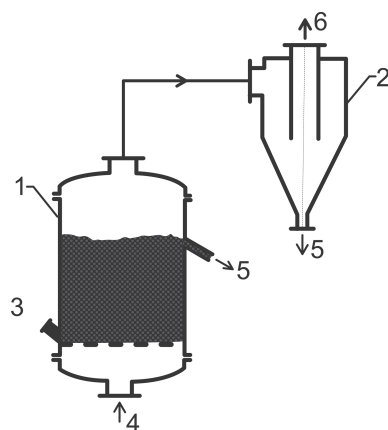
Obrázek 88: Průtočný míchaný reaktor, 1 – nádoba reaktoru, 2 – plášť, 3 – reaktanty (kontinuálně), 4 – produkty (kontinuálně).



Obrázek 89: Poloprůtočný míchaný reaktor, 1 – látka A v kapalné fázi, 2 – přívod látky B v plynu, 3 – odvod nezreagovaného plynu.



Obrázek 90: Průtočný reaktor s pevným ložem, 1 – trubkový reaktor, 2 – cirkulační čerpadlo, 3 – přívod složky A, 4 – přívod složky B, 5 – odvod produktů, 6 – přívod teplotnosného média, 7 – odvod teplotnosného média.



Obrázek 91: Reaktor s fluidním ložem, 1 – fluidní reaktor, 2 – vírový odlučovač, 3 – reaktanty, 4 – nosný plyn, 5 – produkty, 6 – odvod nosného plynu.

- Podle způsobu urychlení reakce dělíme reaktory na:
 - Nekatalytické – prostým smíšením reagujících složek dojde k dostatečně rychlé reakci.
 - Katalytické – rychlost probíhající reakce je urychlena pomocí vhodného katalyzátoru.
 - Tuhé katalyzátory se používají v podobě různě velkých částic. Podle uspořádání tuhé fáze v heterogenním reaktoru rozeznáváme reaktory s pevným ložem (viz obrázek 90) a reaktory s fluidním ložem (viz obrázek 91).

- Podle tepelných podmínek v reaktoru dělíme reaktory na:
 - Izotermické reaktory – v reaktoru je udržována konstantní teplota. U průtočných reaktorů je teplota v reaktoru rovna teplotě nástřikové reakční směsi. U promíchávaného reaktoru musí být teplo vyměněné přes stěnu reaktoru (pomocí chladicího nebo topného systému) rovno reakčnímu teplu.
 - Adiabatické reaktory – jsou reaktory se zanedbatelným přenosem tepla jejich stěnou, tj. teplota v reaktoru se mění v závislosti na probíhající chemické reakci.
- Podle počtu a způsobu zapojení:
 - Samostatně pracující reaktory.
 - Soustavy reaktorů – používají se při zajištění vyšších objemových výkonů, než je schopen poskytnout samostatný reaktor. Jednotlivé základní typy reaktorů mohou být zapojeny paralelně či sériově.

Vsádkové reaktory

Vsádkové reaktory byly prakticky jediným typem reaktorů používaných v začátcích průmyslového zavádění chemických technologií. I přes technický pokrok jsou vsádkové reaktory poměrně často používány i v současně zaváděných technologiích. Reaktory jsou tvořeny nádobou obvykle vybavenou míchacím zařízením. Ohřev nebo chlazení vsádky v reaktoru je možno zabezpečit několika způsoby: cirkulací teplotnosného media pláštěm reaktoru, cirkulací reakční směsi skrz venkovní výměník tepla, zabudováním výměníku tepla (spirálový nebo svislý had, trubkovnice) do reaktoru. Tyto reaktory pracují cyklicky a mohou být otevřené (reakce pouze v kapalně fázi při atmosférickém tlaku) nebo uzavřené (reakce se účastní plynná fáze). Uzavřený vysokotlaký vsádkový reaktor se nazývá autokláv.

Nejčastěji se ve vsádkových reaktorech uskutečňují homogenní i nehomogenní reakce, při kterých je alespoň jedna složka v kapalném stavu. Přednosti těchto reaktorů jsou následující:

- Vhodné pro pomalé chemické reakce (použití kontinuálních promíchávaných reaktorů vyžaduje velký objem reaktoru, nebo neúnosné snížení průtoku).
- Jednoduchá konstrukce a snadné čištění mezi jednotlivými cykly (důležité např. při polymeračních reakcích).
- Mnohoúčelové zařízení – používá se při malotonážních výroбах. Na jednom typu reaktoru lze vyrábět podle různých technologických reglementů (např. výroba farmaceutických substancí).
- Provozní pružnost – jednoduché uvedení do chodu a odstavení, snadná regulace;

K nevýhodám vsádkových reaktorů patří jejich relativně malý výkon a nízké využití pracovní doby v důsledku nutných přípravných operací (plnění, ohřev, chlazení, vypouštění produktu, popř. čištění).

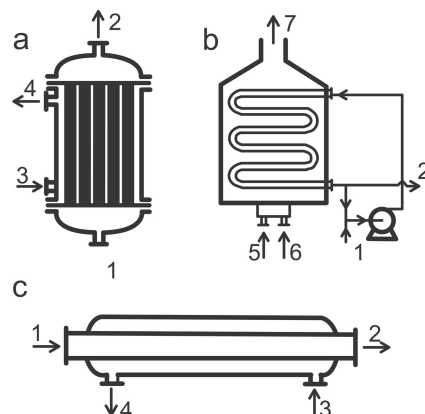
Průtočné reaktory

Do průtočného reaktoru jsou trvale přiváděny suroviny (nástřík) obvykle s konstantní rychlostí a kontinuálně jsou odebírány produkty, které se za reaktorem obvykle separují a čistí. Podle charakteru proudění rozlišujeme reaktory s pístovým tokem a reaktory promíchávané.

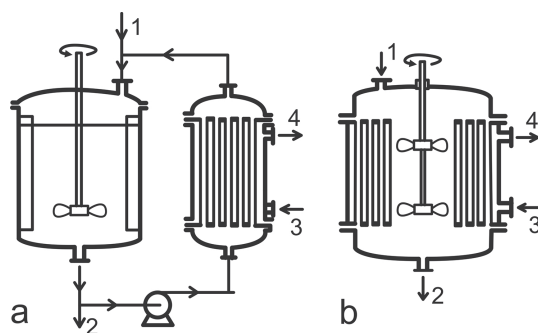
Reaktory s pístovým tokem se používají všude tam, kde je vysoká reakční rychlost a požadované konverze lze dosáhnout v relativně krátkém čase (řádově v minutách). Používají se pro reakce probíhající v plynné fázi, nebo pro reakce probíhající za vysokého tlaku (v plynné nebo kapalně fázi). Jako příklad lze uvést pyrolyzní pec pro pyrolyzu etanu. Zvláštní skupinu tvoří průtočné kontaktní reaktory, ve kterých plynná směs reaguje v přítomnosti pevného katalyzátoru. Na obrázku 92 jsou uvedeny některé základní typy těchto reaktorů. Promíchávané průtočné reaktory se používají u pomalých reakcí v kapalně fázi. Další oblast použití je u reakcí, kdy je nutné kontrolovat odvod tepla, aby nedošlo k překročení maximálně přípustné teploty (nebezpečí rozkladu produktů, popř. výbuch). Dostatečný odvod tepla se zajistí buď pomocí vnějšího výměníku, nebo instalováním vnitřního výměníku (trubkovnice) do prostoru reaktoru (viz obrázek 93). Promíchávané průtočné reaktory se také používají pro heterogenní kontinuální reakce, kdy použití průtočného trubkového reaktoru je technologicky obtížné. Jedná se o heterogenní reakce v kapalném prostředí, kde jednou z fází heterogenního systému je katalyzátor, který musí být homogenně rozptýlen v kapalině (např. některé polymerační reakce). Výhoda průtočných reaktorů spočívá v nižších provozních nákladech na jednotkové množství vyrobeného produktu oproti vsádkovým reaktorům. Po dosažení ustáleného chodu je produkováána rovnoměrnější kvalita produktu (oproti vsádkovým reaktorům). Při dostatečně exotermní reakci je možno uspořít energii na ohřev surovin (nastříkující surovina se ohřeje reakčním teplem probíhající reakce). Mezi hlavní nevýhody patří to, že reaktory jsou stavěny nejen jednoúčelově (pro určitý typ reakce), ale i na určité množství produkce (jejich zatížení lze měnit pouze v úzkém rozmezí). Při jejich spouštění a odstavování kladou vysoké nároky na obsluhující personál, protože společně s reaktorem se zpravidla musí spouštět nebo odstavovat i část výrobní linky.

Reaktory pro heterogenní katalytické reakce

První heterogenní katalytické reaktory se objevily na počátku 20. století. V současné době je na heterogenní katalytické reakci založena většina velkotonážních chemických výrob. Jedná se zejména o reakce plynů katalyzované tuhými katalyzátory. Podle konstrukčního uspořádání je možné rozdělit tyto reaktory do následujících typů:

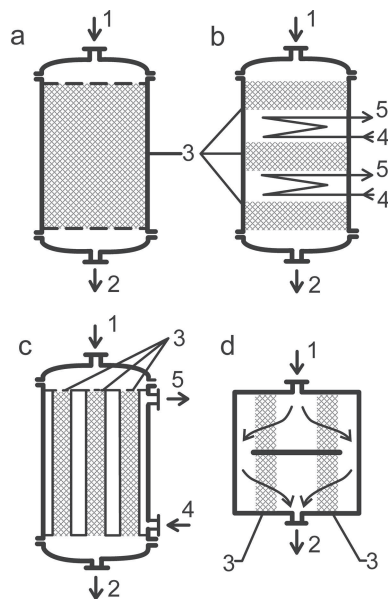


Obrázek 92: Některé typy průtočných reaktorů s pístovým tokem, a) průtočný trubkový reaktor výměňkového typu b) průtočný trubkový reaktor umístěný v peci c) průtočný reaktor „trubka v trubce“; 1 – reaktanty, 2 – produkty, 3 – vstup teplotnosného média, 4 – výstup teplotnosného média, 5 – vzduch, 6 – zemní plyn, 7 – spaliny.

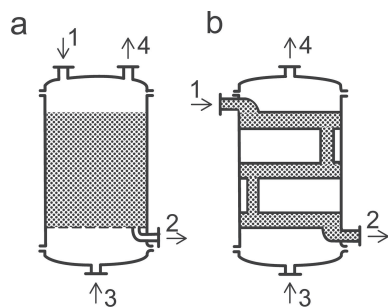


Obrázek 93: Chlazený promíchávaný průtočný reaktor, a) s vnějším výměníkem tepla b) s vnitřním výměníkem; 1 – reaktanty, 2 – produkty, 3 – vstup teplotnosného média, 4 – výstup teplotnosného média.

- **Reaktory s nehybnou vrstvou** – patří mezi nejrozšířenější reaktory a základní typy jsou znázorněny na obrázku 94. Nejjednodušší typ je reaktor naplněný sypaným katalyzátorem v celém objemu (viz obrázek 94a). Dalším typem jsou etážové reaktory s odvodem tepla pomocí výměníků vestavěných přímo do reaktoru (viz obrázek 94b). Tyto reaktory se používají pro exotermické reakce. U trubkového reaktoru (viz obrázek 94c) je katalyzátor uložen uvnitř trubek a v mezitrubkovém prostoru proudí teplotnosné médium. Jsou vhodné pro endotermické reakce, protože se dá pomocí teplotnosného média dobře zajistit přívod tepla do vrstvy katalyzátoru. Jestliže se používají při exotermických reakcích, jako teplotnosné médium slouží čerstvá studená reakční



Obrázek 94: Základní typy reaktorů s nehybnou vrstvou katalyzátoru, a) reaktor naplněný sypaným katalyzátorem, b) etážový katalytický reaktor s odvodem tepla, c) trubkový katalytický reaktor, d) katalytický reaktor s radiálním prouděním; 1 – reaktanty, 2 – produkty, 3 – katalyzátor, 4 – vstup teplonosného média, 5 – výstup teplonosného média.



Obrázek 95: Reaktory s fluidní vrstvou, a) fluidní reaktor, b) fluidní kolona; 1 – přívod tuhé fáze, 2 – odvod tuhé fáze, 3 – přívod plynu, 4 – odvod plynu.

směs, která zchladí katalyzátor a současně se ohřeje na reakční teplotu. Reaktory s radiálním tokem se používají při vysokých tlacích (viz obrázek 94d), protože mají malou tlakovou ztrátu a náklady na kompresi plynů významně ovlivňují provozní náklady. U těchto reaktorů musí být vyřešen rovnoměrný průtok plynu vrstvou katalyzátoru.

- **Reaktory s fluidní vrstvou** – nejjednodušší uspořádání je na obrázku 95. Pevný katalyzátor je udržován ve vznosu nad děrovaným dnem, skrz které proudí zpracovávané suroviny. Fluidní reaktory se používají u velmi exotermních reakcí, které vyžadují citlivou regulaci teploty (změna selektivity reakce s teplotou). Intenzivní výměna tepla ve fluidním loži umožňuje realizovat prakticky izotermní proces. Dále se používají u reakcí, kde dochází k rychlému zanášení a tím i k dezaktivaci katalyzátoru. Fluidní reaktory umožňují nepřetržitý provoz, protože katalyzátor se ze zařízení nepřetržitě odebírá k regeneraci a po zregenerování se opět vrací do reaktoru. Při použití reaktorů s pevnou vrstvou se musí při poklesu aktivity katalyzátoru reaktory přepnout z výrobního cyklu na regenerační cyklus. Hlavní nevýhodou těchto reaktorů jsou vysoké nároky na mechanickou pevnost katalyzátoru.
- **Reaktory s pohyblivou vrstvou** – vrstva tuhé látky (reagující pevná látka nebo pevný katalyzátor) je nepřetržitě dávkována a odebírána z reaktoru. Jako příklad lze uvést šachtové pece, kde pohyb tuhých částic je zajištěn gravitačním sesuvem materiálu do reakční zóny. Dalším příkladem jsou rotační pece, kde k transportu tuhé fáze dochází kombinací mechanického a gravitačního působení.

Copyright: Část věnovaná chemickým reaktorům včetně obrázků byla se svolením Vydavatelství VŠCHT Praha převzata s publikace *Technologie chemických látek*, jejímž autorem je Ing. František Hovorka, CSc. (citace uvedena v seznamu literatury).

Aparáty



Obrázek 96: Soubor aparátů ve výrobně parciální oxidace (foto: Unipetrol RPA, s. r. o.).



Obrázek 97: Soustava kolon určená pro parciální oxidaci při zplyňování mazutu (foto: Unipetrol RPA, s. r. o.).



Obrázek 98: Celkový pohled na výrobu parciální oxidace (foto: Unipetrol RPA, s. r. o.).

Rezervoáry a zásobníky

Zásobníky se skládají z vlastního pláště a přivařených podpěr (noh), připevňovacích ploten a trubek přístrojového vybavení. Nádoby a zásobníky mohou být podzemní (též částečně), nebo nadzemní, umístěné v budovách nebo venku. Zásobníky mohou být použity ke skladování pevných, kapalných a plyných látek. Mohou být mobilní nebo stacionární. Skladovací zásobníky mohou mít uvnitř tlak stejný, jako je tlak atmosférický (101,3 kPa), nebo výrazně vyšší (tzv. tlakový zásobník). Podle konstrukce pak dále dělíme zásobníky na (Guidelines for Quantitative Risk Assessment, 1999):

- **Atmosférické zásobníky s jednoduchým pláštěm** – tvoří jej základní nádoba na kapalinu. Vnější plášť buď existuje, nebo neexistuje, ale pokud existuje, je určen pro zdržení (retenci) a pro ochranu izolace. Není zamýšlen k zachycení kapaliny v případě poruchy základní nádoby (viz obrázek 100).
- **Atmosférický zásobník s ochranným vnějším pláštěm** – tvoří jej základní nádoba na kapalinu a vnější ochranný plášť. Vnější ochranný plášť je určen k zachycení kapaliny v případě poruchy základní nádoby, ale není určen k zachycení žádné páry. Vnější plášť není rovněž schopen odolat všem možným zatížením, např. explozí (statické tlakové zatížení 0,3 atmosféry během 300 milisekund), pronikání úlomků a tepelným (nebo chladovým) zatížením.
- **Atmosférický zásobník se zesíleným pláštěm** – tvoří jej základní nádoba na kapalinu a druhá vnější nádoba. Druhá nádoba je určena k zachycení kapaliny v případě poruchy první nádoby a k tomu, aby odolala všem možným zatížením, jako explozi (statické tlakové zatížení 0,3 bar během 300 ms), pronikání úlomků a tepelným (nebo chladovým) zatížením. Druhá nádoba není určena pro zachycení jakéhokoli druhu par (viz obrázek 99).
- **Plně opláštěný atmosférický zásobník** – tvoří jej základní nádoba na kapalinu a druhá vnější nádoba. Tato druhá nádoba je určena k zachycení jak kapaliny, tak páry v případě poruchy první nádoby a k tomu, aby odolala všem možným zatížením, jako explozi (statické tlakové zatížení 0,3 atmosféry během 300 milisekund), pronikáním úlomků a chladu. Vnější klenba je podepřena druhou nádobou a je určena k tomu, aby odolala zatížení, např. explozí.
- **Membránový zásobník** – tvoří jej základní nádoba a druhá nádoba. Základní nádoba je tvořena nesamonosnou membránou, která udržuje kapalinu a její páru v rámci normálních reakčních podmínek. Druhá nádoba je betonová a podpírá základní nádobu. Druhá nádoba má kapacitu pro zachycení veškeré kapaliny a pro uskutečnění řízeného odtahu par, pokud se porouchá vnitřní nádoba. Vnější klenba je neoddělitelnou součástí druhé nádoby.



Obrázek 99: Válcový stojatý zásobník určený pro skladování ropy (foto: Petr Skřehot).



Obrázek 100: Kulový zásobník pro skladování 550 tun amoniaku (foto: Aleš Bernatík).



Obrázek 101: Pohled na železniční cisterny určené pro přepravu zkapalněných plynů. (foto: Spolek pro chemickou a hutní výrobu, a. s.).



Obrázek 102: Pohled na správné skladování chemických látek v malých obalech. Látky jsou uskladněny podle chemické nebezpečnosti v regálech s požadovanou nosností a uskladněné látky jsou popsány. (foto: Spolek pro chemickou a hutní výrobu, a. s.).

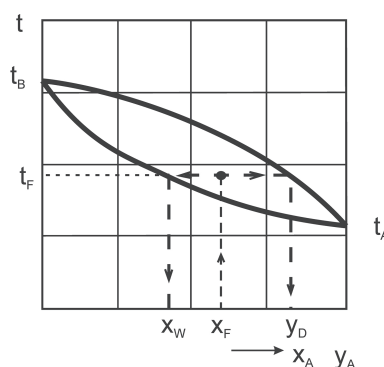
- **Podzemní atmosférický zásobník** – je skladovací zásobník, v němž se hladina kapaliny nachází na úrovni nebo pod úrovní okolního terénu.
- **Zasypaný atmosférický zásobník** – je skladovací zásobník zcela pokrytý vrstvou zeminy, v němž se hladina kapaliny nachází nad úrovní okolního terénu.

Mezi zásobníky lze považovat i nádoby obsahující malá množství chemických látek, pakliže mají pevný nedeformovatelný obal, jakými jsou přepravní nádrže, cisterny, sudy a kontejnery (viz obrázky 101 a 102).

5.2.3 Základní chemické procesy

Destilace a rektifikace

Destilace a rektifikace jsou difúzní operace, které se používají k rozdělení kapalných směsí látek s různou teplotou bodu varu (těkavosti). Čistá látka destiluje při jediné teplotě tj. při svém bodu varu. Výše bodu varu je funkcí tlaku. S klesajícím tlakem klesá také hodnota teploty bodu varu. Destilací za sníženého tlaku se předchází tepelné destrukci látek. Při destilaci směsi látek se využívá toho, že při přechodu části směsi z kapalného skupenství do plynného skupenství mají páry jiné složení než kapalina, s kterou jsou v rovnováze. Páry obsahují vyšší koncentraci těkavější složky a jejich zkapalněním se získá směs obohacená o těkavější složku (tj. s nižším bodem varu a s vyšší tenzí par). Na obrázku 103 je pro ilustraci zobrazen izobarický rovnovážný diagram dvousložkové směsi $A+B$ (složka B má vyšší bod varu než složka A). Na ose y je vynesena teplota a na ose x molární koncentrace méně těkavější složky A v kapalně (x_A) a v parní fázi (y_A). Spodní křivka (křivka varu) vyjadřuje závislost teploty bodu varu na složení kapalné směsi (x_A) a horní křivka (křivka kondenzace) vyjadřuje závislost teploty kondenzace na složení parní fáze (y_A). V oblasti pod křivkou varu se nachází pouze kapalná fáze, v oblasti nad křivkou kondenzace se



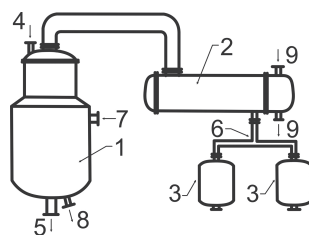
Obrázek 103: Rovnovážný izobarický t - x - y diagram směsi $A+B$.

nachází pouze parní fáze. V oblasti vymezené křivkou varu a kondenzace existuje rovnováha mezi kapalnou a parní fází. Jestliže zahřejeme směs o složení x_F na teplotu t_F , získáme kapalinu o složení x_W a páry o složení y_D . Jejich zkondenzováním dostaneme destilát o složení $x_D = y_D$.

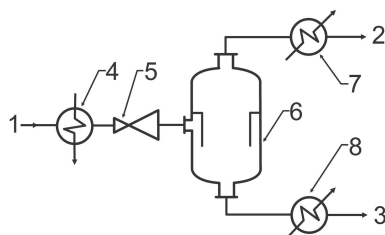
Pojem **destilace** označuje jednorázové částečné odpaření kapaliny s následným zkondenzováním vzniklých par. Podle způsobu provedení rozeznáváme diferenciální a rovnovážnou destilaci. **Rektifikace** je víceetapňová destilace, která je prováděna bez přerušení v jediném destilačním zařízení – rektifikační koloně.

Destilací a rektifikací není možno rozdělit azeotropické směsi. V těchto případech se používá azeotropická nebo extrakční rektifikace. Při azeotropické destilaci se k původní směsi přidá pomocná kapalná látka, která s některou ze složek vytvoří azeotrop s minimální teplotou bodu varu. Při rektifikaci přejde tento azeotrop do destilátu a ten se vhodným postupem rozdělí na požadovanou složku a pomocnou kapalnou látku (např. ochlazením). Při extrakční rektifikaci se k původní směsi přidá rozpouštědlo, které má vyšší bod varu než složky ve směsi. Toto rozpouštědlo působí selektivně na jednu z původních složek směsi, extrahuje ji a tím snižuje její těkavost. Zbývající složky lze potom oddělit rektifikací.

- **Diferenciální destilace** – jedná se o přetržitou operaci. Používané zařízení je schematicky zobrazeno na obrázku 104. Skládá se z destilačního kotle (vařáku), v kterém se ohřívá destilovaná směs k bodu varu. Vzniklé páry jsou vedeny do kondenzátoru (chladiče), který bývá obvykle spojen s chladicím destilátu. Vzniklý destilát se jímá do nádrží na destilát. Koncentrace těkavější složky se v destilátu postupně zmenšuje. Protože odcházející páry jsou bohatší na těkavější složku, dochází v destilačním zbytku ke zvyšování koncentrace méně těkavé složky a tím i k růstu teploty jeho bodu varu. Tato změna koncentrace v destilačním zbytku se projev i na okamžitém složení vzniklého destilátu. Diferenciální destilaci je možné použít při frakcionaci vícesložkové směsi, tj. destiláty se odebírají odděleně, v určitém rozsahu koncentrací nebo teplot varu.

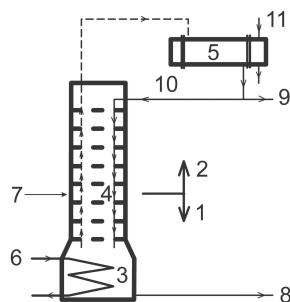


Obrázek 104: Schéma diferenciální destilace, 1 – destilační kotel, 2 – kondenzátor, 3 – předloha, 4 – surovina, 5 – zbytek, 6 – destilát, 7 – topná pára, 8 – kondenzát, 9 – chladící voda.



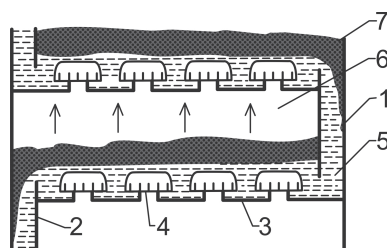
Obrázek 105: Schéma rovnovážné destilace, 1 – nástřík, 2 – destilát, 3 – zbytek, 4 – předehříváč, 5 – regulační ventil, 6 – separátor, 7 – kondenzátor, 8 – chladič zbytku.

- Rovnovážná destilace** – je nepřetržitá operace. Schéma zařízení je na obrázku 105. Nástřík 1 (surovina) se ohřívá pod tlakem ve výměníku tepla 4 a přes regulační ventil 5 se nastříkuje do separátoru 6 s nižším tlakem, kde se oddělí pára od kapaliny. Parní fáze se zkondenzuje v kondenzátoru 7 a získá se destilát 2. Kapalná fáze odcházející ze spodní části separátoru se ochladí v chladiči zbytku 8. Na rozdíl od diferenciální destilace je rozdělení směsi při rovnovážné destilaci méně účinné a pro dané složení nástříku je složení destilátu a zbytku jednoznačně určeno teplotou destilace.
- Rektifikace** – je mnohonásobná rovnovážná destilace spojená s deflegmací a prováděná bez přerušení v jednom destilačním zařízení – rektifikační koloně. Rektifikační kolona pracuje protiproudým způsobem, nahoru stoupají páry, proti kterým stéká kapalina. Mezi parou a kapalinou dochází k výměně hmoty a tepla. Pára, která je teplejší, ohřívá kapalinu, se kterou přichází do styku a dodaným teplem dojde k odpaření prchavějších složek z kapaliny. Pára, která ohřála kapalinu, se sama ochladí a zkondenzují méně těkavé složky, které stékají společně s kapalnou fází. Stoupající páry se postupně obohacují těkavějšími složkami a stékající kapalina složkami méně těkavými. Teplota na dně kolony je maximální a jsou zde látky s maximálním bodem varu, teplota v hlavě kolony je minimální, protože jsou zde látky s nízkým bodem varu. Část kolony nad nástřikovým patrem se nazývá obohacovací, neboť jsou zde větší koncentrace prchavějších složek než v nástříku. Spodní část kolony, tj. pod nástřikovým patrem se nazývá ochuzovací (viz obrázek 106).

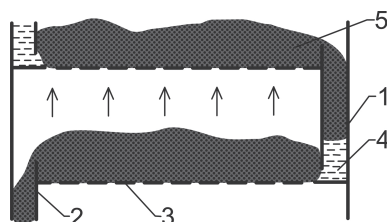


Obrázek 106: Patrová rektifikační kolona, 1 – ochuzovací část kolony, 2 – obohacovací část kolony, 3 – vařák, 4 – nástřikové patro, 5 – kondenzátor, 6 – topná pára, 7 – nástřík, 8 – zbytek, 9 – destilát, 10 – zpětný tok, 11 – chladicí voda.

Pro dobrou účinnost rektifikační kolony je třeba zabezpečit intenzivní styk mezi kapalnou a parní fází, dosáhnout maximální plochu styku obou fází. Kapalina se stýká s párou při probublávání vrstvou kapaliny na patrech, pak mluvíme o patrových kolonách, nebo při kontinuálním povrchovém styku, ke kterému dochází na nehybné vrstvě náhodně sypaných tělísek (náplni), a potom se mluví o plněných kolonách. Patro v koloně je tvořeno vodorovnou deskou opatřenou otvory pro průchod páry. Na patře se udržuje pomocí přepadu konstantní vrstva kapaliny několik centimetrů vysoká, skrz kterou probublává pára. Typickým představitelem těchto pater jsou kloboučková patra (viz obrázek 107) a síťová patra (viz obrázek 108).



Obrázek 107: Kloboučkové patro, 1 – plášť kolony, 2 – přepadová trubka, 3 – patro s nátrubky, 4 – klobouček s otvory, 5 – kapalina, 6 – pára, 7 – pěna.



Obrázek 108: Síťové patro, 1 – plášť kolony, 2 – přepadová trubka, 3 – síťové patro, 4 – kapalina, 5 – pěna.



Obrázek 109: Typy výplní kolon.

U plněných kolon se používají různě tvarovaná tělíska – výplně, která zajišťují dostatečnou plochu mezi kapalnou a pevnou fází a jsou zhotoveny z keramiky, kovu nebo plastických hmot. Některé nejznámější typy výplní jsou na obrázku 109.

Volba konstrukčního řešení rektifikační kolony závisí na vlastnostech zpracovávané směsi. Patrové kolony se používají při zpracování velkého množství suroviny (např. při zpracování ropy) a plněné kolony se používají při zpracování pěnících systémů a kdy je nutné pracovat za nižšího tlaku.

Copyright: *Tato kapitola byla se souhlasem Vydavatelství VŠCHT Praha převzata z publikace Technologie chemických látek, jejímž autorem je Ing. František Hovorka, CSc. (citace uvedena v seznamu literatury).*

5.2.4 Bilancování systému

Bilancováním systému rozumíme aplikaci vět o zachování. Jejich využití v oblasti modelování chemických procesů probíhajících uvnitř zařízení je s ohledem na jejich důležitost časté, přičemž bilancovat lze jen tzv. **extenzivní veličiny**. Především se jedná o zákony zachování hmoty a energie – hovoříme tak o látkových a energetických bilancích. Bilancovat můžeme pouze uzavřený systém, který má definované hranice s okolím. Důležitá je volba hranic systému. Vycházíme při ní jednak ze skutečného (konstrukčního) tvaru systému, jednak z toho, zda chceme vytvořit model systému se soustředěnými parametry (v matematickém popisu nefigurují souřadnice jako nezávisle proměnné), nebo s rozloženými parametry (alespoň jedna souřadnice je v matematickém popisu použita jako nezávisle proměnná). Extenzivní veličiny, které v chemickém inženýrství bilancujeme, jsou celková hmotnost m (hmotnost směsi), hmotnost složky m_i , celkové látkové množství n (počet molů směsi), látkové množství složky n_i , hybnost mv , energie E a entalpie H .

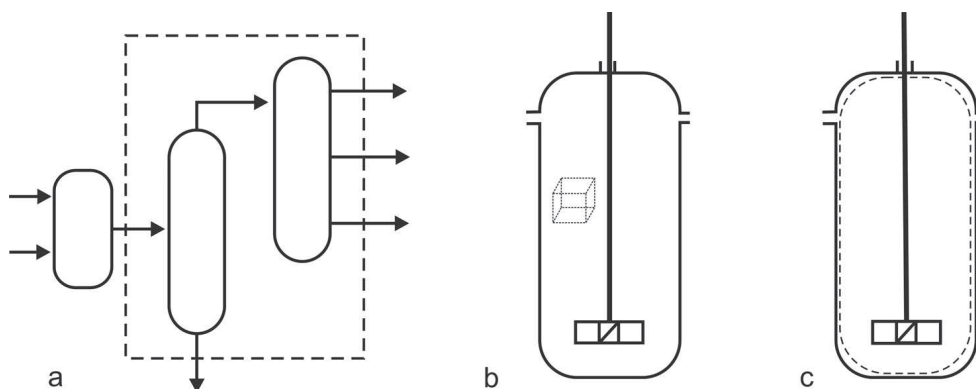
Uveďme si příklad jednoduché bilance. Smísíme-li 0,9 kg vody a 0,1 kg kuchyňské soli, získáme 1 kg roztoku NaCl. Jedná se o bilanci hmotnosti. Uveďme příklad i nesprávné, absurdní bilance. Smísíme 1 kg vody o teplotě 25 °C a 1 kg vody o teplotě 50 °C. Výsledná teplota je 25 + 50 = 75 °C? Tato rovnice samozřejmě neplatí, protože teplota patří mezi intenzivní veličiny, které bilancovat nelze. Jaká bude výsledná teplota těchto dvou kilogramů vody je otázka ne zcela jednoduchá, v rámci přiměřené přesnosti však na ní můžeme získat odpověď za použití bilance entalpie. Jiný příklad absurdní bilance. Smísíme hromadu písku a druhou hromadu písku. Kolik hromad písku získáme? To, že jakékoliv množství písku může být uspořádáno do jedné či více hromad, je informace kvalitativní. Odpověď není jednoznačná a takové úlohy nepatří do problému bilancování. Bilancování se týká kvantity, velikosti či množství.

Bilanční systém

Bilancujeme množství bilancované veličiny v **bilančním systému**. V přírodních a technických vědách obecně definujeme bilanční systémy tak, že část světa (bilanční systém) vymezíme od zbytku světa (okolí bilančního systému) skutečným nebo myšleným rozhraním (hranicí bilančního systému). V chemickém inženýrství je bilančním systémem část prostoru, ve kterém se odehrává sledovaný proces, např. jedno zařízení (reaktor, sušárna, filtr, odparka apod.), soustava zařízení (výrobní linka, více vzájemně propojených zařízení), část zařízení nebo pomyslný diferenciální objem uvnitř zařízení.

Hranice systému mohou být reálné (např. stěny zařízení) nebo pomyslné, na obrázku 110 jsou pomyslné hranice vyznačeny přerušovanými čarami. **Otevřený systém** vyměňuje hmotu a/nebo energii s okolím, hranice systému jsou propustné. Bilancované veličiny vstupují do systému vstupními proudy a ze systému do okolí odcházejí proudy výstupními. Pokud systém nevyměňuje hmotu s okolím, jedná se o **systém uzavřený**. V případě, že systém s okolím nevyměňuje hmotu ani energii, jedná se o **systém izolovaný**. Hranice systému volíme podle účelu bilančního výpočtu.

Strukturu systému pro bilancování vyjadřujeme pomocí **blokového** (proudového) **schématu**. Blokové schéma vystihuje strukturu systému a bloky (uzly) představují jednotlivá zařízení nebo skupiny zařízení. Bloky jsou propojeny **proudy**. Prostřednictvím proudů popisujeme všechny nezanedbatelné interakce uzlu s okolím a/nebo jinými uzly. Příkladem proudu může být např. trubka, kterou se dopravují bilancované látky (abstraktněji, bilancované extenzivní veličiny) z jednoho uzlu do uzlu jiného. Proud se graficky většinou zobrazuje jako rovná nebo lomená čára spojující uzly a označená šipkou směřující do uzlu, do kterého vstupuje. Zde budeme předpo-



Obrázek 110: Příklady bilančních systémů. a) Soustava zařízení, otevřený systém, pomyslná hranice vymezuje dva aparáty. b) Pomyslná hranice určuje diferenciální objem. c) Reálné hranice systému.

kládat, že vlastnosti proudu se nemění podél jeho délky, tedy co vstupuje na začátku proudu, to okamžitě vystupuje na konci proudu. Neuvažujeme tedy akumulace a časová zpoždění v proudech.

Při bilančních výpočtech budeme užívat dva typy proudů – reálné a fiktivní. **Reálnými proudy** jednotlivé materiály (látky) vstupují do studovaného systému nebo z něj reálnými proudy vystupují. V chemii často popisujeme látky jako směsi složek. V chemických reakcích některé složky zanikají a některé vznikají. Pro každou chemickou reakci budeme zánik některých složek (reaktantů) nahrazovat **výstupním fiktivním proudem**, zatímco vznik jiných složek (produktů) v dané reakci nahradíme **vstupním fiktivním proudem**. Těmito proudy vystupuje a vstupuje hmotnost a látkové množství složek (ale také např. entalpie). Každou chemickou reakci tak můžeme popsat pomocí dvojice fiktivních proudů.

Bilance za konečné bilanční období

Základní bilanční rovnici pro obecnou bilancovanou veličinu B za konečné bilanční období zapíšeme ve tvaru:

$$\begin{aligned} \text{počáteční množství} + \text{součet vstupů} + \text{součet zdrojů} = \\ = \text{koncové množství} + \text{součet výstupů} + \text{součet propadů} \end{aligned}$$

$$B_{po} + \sum_j^{\text{vstupy}} B_j + \sum_j^{\text{zdroje}} B_j = B_{kon} + \sum_j^{\text{vstupy}} B_j + \sum_j^{\text{propady}} B_j \quad (5-2)$$

nebo

$$\text{vstup} + \text{zdroj} = \text{výstup} + \text{akumulace}$$

$$\sum_j^{\text{vstupy}} B_j + \left(\sum_j^{\text{zdroje}} B_j - \sum_j^{\text{propady}} B_j \right) = \sum_j^{\text{vstupy}} B_j + (B_{kon} - B_{po}) \quad (5-3)$$

kde *počáteční množství* je množství bilancované veličiny, které se nachází v bilančním systému v okamžiku začátku bilančního období; *koncové množství* je množství bilancované veličiny, které se nachází v bilančním systému v okamžiku konce bilančního období. *Akumulace* je množství bilancované veličiny, které v bilančním systému v průběhu bilančního období přibude.

Tedy jedná se o rozdíl, který získáme tak, že od množství bilancované veličiny v bilančním systému v okamžiku konce bilančního období odečteme množství bi-

lancované veličiny v bilančním systému v okamžiku začátku bilančního období:

$$akumulace = koncové množství - počáteční množství = B_{kon} - B_{po}.$$

Jiné slovo pro akumulaci je například **přírůstek**. Akumulace může mít kladnou, nulovou nebo zápornou hodnotu. Pokud množství bilancované veličiny ubývá, je akumulace záporná. Absolutní hodnotu záporné akumulace můžeme nazývat **úbytkem**. V případě, že se stav systému nemění v čase, říkáme, že systém je v **ustáleném (stacionárním) stavu** a akumulace je nulová.

Vstup je množství bilancované veličiny, které se v průběhu bilančního období přemístí z okolí bilančního systému přes hranice bilančního systému do bilančního systému. V bilančních rovnicích představuje vstup často souhrnnou veličinu, která je tvořena součtem dílčích vstupů.

Výstup je množství bilancované veličiny, které se v průběhu bilančního období přemístí z bilančního systému přes hranice bilančního systému do okolí bilančního systému. V bilančních rovnicích představuje výstup často souhrnnou veličinu, která je tvořena součtem dílčích výstupů. Pokud nejsou ve formálním zápisu bilancí výstupy explicitně uvedeny, předpokládáme, že jsou zahrnuty mezi vstupy se záporným znaménkem.

Zdroj je množství bilancované veličiny, které v bilančním systému během bilančního období vznikne, např. hmotnost nějaké sloučeniny může vznikat chemickými reakcemi za současného zániku jiné či jiných sloučenin. V bilančních rovnicích představuje zdroj často souhrnnou veličinu, která je tvořena součtem dílčích zdrojů.

Propad je množství bilancované veličiny, které v bilančním systému během bilančního období zanikne, např. hmotnost nějaké sloučeniny může zanikat chemickými reakcemi za současného vzniku jiné či jiných sloučenin. V bilančních rovnicích představuje propad často souhrnnou veličinu, která je tvořena součtem dílčích propadů. Pokud nejsou ve formálním zápisu bilancí propady explicitně uvedeny, předpokládáme, že jsou zahrnuty mezi zdroje se záporným znaménkem.

Bilance za diferenciální bilanční období

V praxi se často setkáváme s případy, kdy se stav bilancované veličiny uvnitř bilancovaného systému mění v průběhu času. Proces je neustálený a musíme bilancovat za diferenciální (velmi krátké, infinitezimální) bilanční období $d\tau$. Podobně, pokud se stav bilancované veličiny mění uvnitř aparatury v závislosti na místě, musíme pro bilancování volit systémy o diferenciální velikosti (viz obrázek 110b).

Při bilancích za diferenciální bilanční období vydělíme všechny členy základní bilanční rovnice velmi krátkou délkou bilančního období $d\tau$. Získáme bilanci vztaženou

na jednotku času (lokalizovanou v čase): Rozsah (velikost) procesu, který probíhá po nějakou dobu $d\tau$, můžeme kvantitativně charakterizovat pomocí změny množství nějaké veličiny dB , která je tímto procesem jednoznačně způsobena. Rychlost procesu je pak definována jako rozsah procesu za jednotku času. Rychlost akumulace je akumulace za jednotku času. Vstup, výstup, zdroj a propad můžeme také vyjádřit za jednotku času jako rychlost vstupu (přítok veličiny), rychlost výstupu (odtok veličiny), rychlost zdroje a rychlost propadu. Bilanční rovnici pro diferenciální bilanční období $d\tau$ pak můžeme vyjádřit ve tvaru (viz rovnice 5-4):

$$\begin{aligned} \text{vstup za jednotku času (přítok)} + \text{zdroj za jednotku času (rychlost vzniku)} = \\ = \text{výstup za jednotku času (odtok)} + \text{akumulace za jednotku času} \\ \text{(rychlost akumulace)} \end{aligned}$$

$$\sum_j^{\text{vstupy}} \dot{B}_j + \left(\sum_j^{\text{zdroje}} \dot{B}_j - \sum_j^{\text{propady}} \dot{B}_j \right) = \sum_j^{\text{vstupy}} \dot{B}_j + \frac{dB}{d\tau}. \quad (5-4)$$

Materiálové bilance

K materiálovým bilancím patří zejména bilance hmotnosti a látkového množství. Bilancujeme celkovou hmotnost m (hmotnost směsi), hmotnost složek m_i , celkové látkové množství n (počet molů směsi) a látkové množství složek n_i . Podobně bychom postupovali při objemových bilancích, které jsou však méně časté z důvodu možných objemových změn, které mohou nastat případnou změnou teploty, tlaku a směřování nebo oddělováním složek. Složky jsou látky, které bilancujeme (například voda, vzduch, kyslík, popel, OH^-), tj. sloučeniny, směsi sloučenin, prvky, ionty. Volba složek v bilančním systému je velmi důležitá. Rozhoduje účelnost z hlediska bilančních výpočtů.

Někdy je užitečné redukovat počet složek tak, že zanedbáme látky přítomné v nepatrných množstvích. Příkladem může být suchý vzduch. Vzduch může být samostatnou složkou, která do systému vstupuje a následně ze systému vystupuje, aniž by se změnilo jeho chemické složení, např. u konvekčního sušení. Vzduch se však může dělit na složky, nejčastěji na kyslík a dusík, jejichž obsah je ve vzduchu největší. Při zanedbání ostatních plynů pak předpokládáme, že vzduch tvoří 79 obj. % dusíku a 21 obj. % kyslíku. Rozdělení vzduchu na složky kyslík a dusík děláme např. při spalování, kdy do systému přichází vzduch, ale dochází k reakci mezi vzdušným kyslíkem a složkou, kterou spalujeme, např. uhlíkem. Redukci počtu složek nelze dělat v případech, kdy jsou tyto složky (látky) důležité i v malých množstvích, např. chemické katalyzátory a inhibitory, katalytické či obecné jedy, látky velmi drahé či nebezpečné, látky, které se mohou nějakým procesem koncentrovat a hromadit.

Každý proud v bilančním systému obsahuje jednu nebo více složek, které tvoří směs. Pro účely bilancování je důležité vyjádření složení směsí. Zopakujme si některé základní definice:

Hmotnostní zlomek je definován vztahy 5-5 a 5-6:

$$w_{i,j} = \frac{m_{i,j}}{m_j}, \quad (5-5)$$

$$w_{i,j} = \frac{\dot{m}_{i,j}}{\dot{m}_j}, \quad (5-6)$$

kde $w_{i,j}$ je hmotnostní zlomek i -té složky v j -tém proudu (směsi), $m_{i,j}$ je hmotnost ($\dot{m}_{i,j}$ – hmotnostní tok) i -té složky v j -tém proudu a m_j je celková hmotnost ($\dot{m}_j$ – hmotnostní tok) j -tého proudu (směsi). Součet hmotnostních zlomků složek v proudu (směsi) je vždy roven jedné.

Molární zlomek je definován analogicky:

$$x_{i,j} = \frac{n_{i,j}}{n_j}, \quad x_{i,j} = \frac{\dot{n}_{i,j}}{\dot{n}_j}, \quad (5-7)$$

kde $x_{i,j}$ je molární zlomek i -té složky v j -tém proudu (směsi), $n_{i,j}$ je látkové množství ($\dot{n}_{i,j}$ – tok látkového množství) i -té složky v j -tém proudu a n_j je celkové látkové množství ($\dot{n}_j$ – tok látkového množství) j -tého proudu (směsi). Součet molárních zlomků složek v proudu (směsi) je roven jedné.

V případě plyné směsi lze vyjádřit molární zlomek $x_{i,j}$ pomocí parciálního tlaku $p_{i,j}$ (Pa) a celkového tlaku p_j (Pa) v proudu j (viz rovnice 5-8).

$$x_{i,j} = \frac{p_{i,j}}{p_j} \quad (5-8)$$

Přepočty složení pak provádíme podle níže uvedených rovnic 5-9 až 5-11:

$$x_{i,j} = \frac{\frac{w_{i,j}}{M_i}}{\sum_{i=1}^{N_S} \frac{w_{i,j}}{M_i}}, \quad (5-9)$$

$$w_{i,j} = \frac{x_{i,j} \cdot M_i}{\sum_{i=1}^{N_S} x_{i,j} \cdot M_i}, \quad (5-10)$$

$$\bar{M}_j = \sum_{i=1}^{N_S} x_{i,j} \cdot M_i = \frac{1}{\sum_{i=1}^{N_S} \frac{w_{i,j}}{M_i}}, \quad (5-11)$$

kde M_i je molární hmotnost i -té složky, N_S je počet složek v j -tém proudu (směsi) a $\bar{M}_j$ je střední molární hmotnost proudu j .

V hmotnostních a látkových bilancích se často setkáváme s pojmem **výtěžek**, **výtěžnost**, **účinnost** či **účinek**. Jedná se o poměr mezi skutečným výsledkem procesu (např. množstvím produktu) a teoretickým výsledkem za nějakých ideálních okolností bez ztrát (vypočteným např. z množství vstupující suroviny pomocí stechiometrických vztahů).

Copyright: *Tato kapitola včetně obrázků byla se souhlasem Vydavatelství VŠCHT Praha převzata z publikace Chemické inženýrství I, jejímž autorem je prof. Ing. Pavel Hasal, CSc. a kolektiv (citace uvedena v seznamu literatury).*

5.2.5 Analýza technologických rizik

Obsahové principy analýzy rizik

Analýza rizika je analytický proces, který se zaměřuje na zjištění relevantních „slabých míst“ při určité činnosti v pracovním (technickém) systému, které by mohly vést k nežádoucím následkům. Analýza rizika zahrnuje také vyjádření rizika (kvalitativně, semikvantitativně nebo kvantitativně) a odhad (ocenění) úrovně identifikovaného rizika s ohledem na nežádoucí dopady na lidi, životní prostředí (včetně hospodářských zvířat) a majetek. Výsledky analýzy rizika pak lze použít pro hodnocení rizika.

Analýza rizik vyžaduje systematický postup při použití dostupných informací pro určité činnosti v určitém systému. Pro zpracování analýzy a hodnocení rizik nelze poskytnout detailní a univerzální metodický postup, neboť rozdílnost používaných technologií a činností, různá projekční a stavební řešení, rozdílná lokalizace objektů nebo zařízení v místě, rozdílné vlivy jiných objektů nebo zařízení v okolí a další proměnné faktory vytvářejí specifické situace na jiných místech a v jiných podmínkách neopakovatelné. Zpracovatel analýzy a hodnocení rizik musí využít znalosti daného objektu nebo zařízení, prováděné činnosti, legislativních požadavků, metod a postupů bezpečnostního inženýrství, založeného na chemickém inženýrství a dalších souvisejících vědních oborech k objektivnímu zhodnocení všech významných aspektů, které přispívají k bezpečnosti daného objektu nebo zařízení. Výsledky analýzy a hodnocení rizik musí být srozumitelné a dostatečně dokladované, neboť se používají pro řízení rizika (Ministerstvo životního prostředí, 2007).

Analýza rizika je prováděna v různých fázích životního cyklu objektu nebo zařízení a při provádění jakýchkoliv změn, kterými by mohla být ovlivněna bezpečnost, jako např. změny výrobní technologie, personálního obsazení, pracovních předpisů, dále změny v pracovním režimu (najíždění, odstavování, údržba a opravy zařízení). Podle cíle je stanovena hloubka analýzy a také požadavky na databázi vstupních údajů, které by měly být v nutné míře uvedeny i v dokumentaci. Hloubka analýzy by měla být úměrná nebezpečí, které nakládání s nebezpečnými látkami v příslušném objektu nebo zařízení představuje. Nebezpečnost chemických látek a chemických přípravků, které jsou ve skupenství pevném, kapalném nebo plynném, se může projevit různě v závislosti na vlastnostech chemické látky nebo přípravku (druh nebezpečné vlastnosti), stavu, v jakém se nachází (skupenství, tlak, teplota, množství), druhu úniku a následného možného scénáře rozvoje úniku, a také na dalších okolnostech, jako např. meteorologických podmínkách při úniku apod. Podle toho je třeba volit i vhodně kombinovat metody pro analýzu. Výběr metody se řídí nejen účelem hodnocení rizika a jeho předpokládaným charakterem, ale i dostupností údajů, historií mimořádných událostí v daném objektu nebo zařízení nebo jiných podobných objektech a zařízeních, předpoklady a omezeními použité metody. Je třeba také sledovat vývoj v této oblasti a podle toho adekvátně reagovat při výběru metod a opustit používání metod, které jsou méně účinné, nebo jsou určeny pro jiný účel. Analýza musí být prováděna v úzké spolupráci analytiků s procesním personálem. Při analýze musí být identifikovány a analyzovány všechny zdroje rizik závažné havárie.

Analýza může být kvalitativní, semikvantitativní a kvantitativní. Kvalitativní analýza je typ analýzy, ve které se používá kvalitativní odhad rizika určité události, tj. nečíselný popis skládající se z identifikace a popisu zdrojů rizik, relativního ocenění závažnosti zdrojů rizik, identifikace, sestavení a popisu scénářů havárií. Semikvantitativní analýza je typ analýzy, ve které se používá semikvantitativní odhad rizika určité události, tj. kategorie frekvencí a následků pro scénáře jsou definovány určitými stupni závažnosti slovně i kvantitativně (např. číselným rozpětím). Míra rizika je vyjádřena obdobně jako u kvalitativní analýzy s upřesněním kategorií závažnosti následků a frekvencí scénářů. Kvantitativní analýza je typ analýzy, ve které je použit systematický postup numerického vyčíslení očekávané četnosti a následků potenciálních havárií spojených se zařízením nebo provozem, založený na inženýrském odhadu, vyhodnocení a matematických metodách. Postup analýzy rizika pro účely prevence havárií obecně obsahuje tyto části (Sluka a kol., 2005):

- Definice analýzy rizika, stanovení hloubky studie.
- Popis analyzovaného systému, objektu a zařízení a vymezení jeho hranic.
- Identifikace a popis nebezpečí (zdrojů rizika).
- Relativní ocenění závažnosti zdrojů rizika, výběr zdrojů rizika.
- Identifikace možných příčin havárie – určení příčin poruch, podmínek a situací s potenciálem způsobit havárii.

- Identifikace a definice možných scénářů nehod (nebezpečných událostí), které mohou vyústit v havárii, výběr reprezentativních scénářů havárie.
- Odhad (ocenění) následků scénářů havárií.
- Odhad (ocenění) pravděpodobnosti scénářů havárií.
- Odhad (ocenění) rizika (stanovení míry rizika).
- Prezentace rizika.

Aby bylo možné provést všechny výše uvedené procedurální kroky, vyžaduje si zpracovávání analýzy rizika široké znalosti, zejména o:

- Daném objektu nebo zařízení.
- Prováděné činnosti.
- Legislativních požadavcích.
- Metodách a postupech bezpečnostního inženýrství.

Analýza rizik musí být postavena na objektivním zhodnocení všech významných aspektů, které přispívají k bezpečnosti daného objektu nebo zařízení. Výsledky analýzy rizik musí být srozumitelné a dostatečně dokladované, neboť se dále používají pro vyhodnocení rizik a následné definování požadavků pro management rizik.

Typy analýzy rizika

Analýzu rizika je možno provést několika způsoby a za využití různých přístupů, z nichž každý nabízí různý záběr i hloubku studie. Podle charakteru výstupů, které daná analýza nabízí, rozlišujeme tři typy:

- **Kvalitativní analýza** – typ analýzy rizika, kde se používá kvalitativní odhad rizika určité události, tj. nečíselný popis skládající se z identifikace a popisu zdrojů rizik, relativního ocenění závažnosti zdrojů rizik, identifikace, sestavení a popisu scénářů havárií až do kroku vytvoření scénářů (například pomocí metody HAZOP – viz příloha P-4).
- **Semikvantitativní analýza** – typ analýzy rizika, kde se používá semikvantitativní odhad rizika určité události, tj. kategorie frekvencí a následků pro scénáře jsou definovány určitými stupni závažnosti slovně i kvantitativně (např. číselným rozpětím). Míra rizika je vyjádřena pak obdobně jako u kvalitativní analýzy rizika s upřesněním kategorií závažnosti následků a frekvencí scénářů (například pomocí metody FMEA – viz příloha P-5).
- **Kvantitativní analýza** – typ analýzy rizika, kde je použit systematický postup numerického vyčíslení očekávané frekvence a následků potenciálních havárií spojených se zařízením nebo provozem založeným na inženýrském

odhadu, vyhodnocení a matematických metodách. Skládá se obvykle z těchto základních úloh:

- Identifikace a definice možných nebezpečných událostí (scénářů havárií) a jejich možných konečných stavů.
- Odhad pravděpodobnosti výskytu každého možného konečného stavu každé nebezpečné události.
- Výpočet následků každého možného konečného stavu každé nebezpečné události.
- Kombinace pravděpodobností a následků pro odhad individuálního a společenského rizika.

Komplex metod použitý v logickém procesu hodnocení rizika chemických procesů pomocí míry rizika, která je výsledkem sumarizace rizik všech vybraných nehodových událostí, pak nazýváme **kvantitativní analýza rizika chemických procesů**. Její řešení probíhá po etapách a směřuje k ocenění následků a pravděpodobností všech koncových stavů scénářů vybraných nehodových událostí. Zároveň obsahuje návrhy pro snížení rizika. Pro kvantifikaci následků se používá modelování fyzikálně chemických procesů a jevů, které se objevují v událostech a výsledcích událostí (úniky, rozptyly, požáry, výbuchy, zranitelnost příjemce rizika – modely dávek a odezvy: koncentrace, probit funkce, tepelná radiace, přetlak) (Ministerstvo životního prostředí ČR, 2007).

Nebezpečné látky a chemické procesy probíhající v zařízení

Základním předpokladem pro analýzu je bilance systému – **hmotnostní bilance** a **energetická bilance** na základě zákonů o zachování hmoty a energie. Pro provedení bilančních výpočtů, tvorbu scénářů potenciálních havárií, pro provádění analýzy, i pro ekonomické zhodnocení apod. jsou potřebné v různé míře tyto údaje:

- Kvalitativní údaje všeobecného charakteru pro představu o probíhajících dějích, což jsou všeobecné znalosti o chemických procesech, výrobních postupech, surovinách, meziproduktech a výrobcích.
- Kvantitativní údaje (data) pro konstrukční, technologické a bilanční výpočty, což jsou stechiometrie probíhajících chemických reakcí, termodynamika chemických reakcí a fyzikálních procesů, kinetika chemických reakcí, chemicko-inženýrské údaje (data o přestupu hmoty, tepla a hybnosti), údaje potřebné pro konstrukci aparátů, údaje potřebné pro kontrolu, měření a regulaci procesu.
- Doplnující informace pro analýzu, jako např. informace o meteorologické situaci, vodohospodářské, hydrogeologické a geologické charakteristiky okolí objektu.

Základní chemické procesy využívané v chemických výroбах byly blíže představeny v kapitole 5.2.3 a o principech a způsobech bilancování systému bylo pojednáno v kapitole 5.2.4.

V analýze rizika musí být proto uveden přehled všech nebezpečných látek v objektu nebo zařízení, uvedou se maximální množství, přítomná nebo potenciálně přítomná (mohou vzniknout při závažné havárii), pro která jsou objekty nebo zařízení kolaudovány, klasifikace nebezpečných látek a vlastnosti potřebné k analýze.

Chemické látky a přípravky mohou mít takové vlastnosti, které jsou nebezpečné pro okolí. Tyto vlastnosti se klasifikují podle zákona č. 356/2003 Sb., o chemických látkách a chemických přípravcích a o změně některých zákonů, ve znění pozdějších předpisů. Identifikačními údaji nebezpečných látek jsou název podle nomenklatury IUPAC, číslo CAS, ES číslo, indexové číslo, chemický vzorec, chemické složení směsi, klasifikace, stupeň čistoty a nejdůležitější příměsi. Údaje o vlastnostech nebezpečných látek zahrnují fyzikální (včetně požárně-technických), chemické, toxikologické (včetně ekotoxikologických) a ostatní specifické vlastnosti (např. vlastnosti týkající se koroze), které mohou mít vliv na posouzení bezpečnosti. Tyto údaje lze získat z bezpečnostního listu a příslušných databází chemických látek. Vzhledem k možné nejistotě dat je vhodné data kontrolovat pomocí jiného zdroje. Je třeba sledovat i změny v závazné klasifikaci látek.

Pro účely analýzy rizika je třeba uvést i rozčlenění nebezpečných látek do produktových kategorií (surovina, meziprodukt, hotový výrobek, vedlejší produkt, odpadní a pomocný produkt, produkt vzniklý jako důsledek neřízených chemických procesů). Pokud se v objektu nebo zařízení nachází velký počet různých nebezpečných látek, je vhodné pro účely jejich klasifikace seskupovat tyto látky do kategorií podle druhu nebezpečných vlastností. V takovém případě musí být uvedeno vysvětlení systému seskupování látek do kategorií (Ministerstvo životního prostředí ČR, 2007).

Nebezpečné (nestandardní) chemické reakce

Každý chemický proces se zakládá na určitém chemizmu v určitém technologickém zařízení za definovaných podmínek. Pod pojmem **chemizmus** rozumíme soubor všech vlastností dané látky, chemické změny nebo jevu, spojený s bližším výkladem jevu, tedy druh chemických reakcí, stechiometrii reakcí a termodynamické poměry, vlastnosti reagujících látek při požadovaných parametrech procesu, ale i za mimořádných podmínek, kdy může dojít ke změnám, které mohou vést ke vzniku závažné havárie. Chování nebezpečných látek za normálních a předvídatelných nehodových podmínek zahrnuje provozní teploty a tlaky v průběhu najíždění, regenerace, běžných provozních podmínek a v případě odstávky nebo za jiných okolností; dále chování reakční směsi v průběhu a následně po přerušení technologického procesu; chování skladovaných materiálů za normálních provozních podmínek, následně po selhání funkce nebo poškození zařízení a následně změně skladovacích podmínek; kontami-

naci produktů; selhání funkce ochranné obálky zařízení (loss of containment), které má za následek únik přítomných chemických látek do okolí apod.

Při zkoumání procesní bezpečnosti je znalost nebezpečných chemických reakcí základním předpokladem. Pro vyhodnocení možných dopadů mimořádných provozních podmínek na procesní bezpečnost je třeba znát fázové změny látek, dopady změn složení vstupních látek, proces stárnutí látek, možnost jiného průběhu reakce v jiných částech nedostatečně homogenizované reakční směsi, problém akumulace nečistot, chování katalyzátorů, iniciátory nežádoucích reakcí, dopady koroze, vhodnost či nevhodnost konstrukčních materiálů pro daný účel, možnost elektrostatického nabíjení při manipulaci, vliv předávkování nebo nedostatečného dávkování surovin, nežádoucí interakce s jinými látkami, chybný vstup látek do jiných částí zařízení, vlastnosti vznikajícího prachu, zanášení částí zařízení shlukováním částic (krystalizací, tuhnutím, vylučováním povlaků nebo polymerací), absorpce vlhkosti, možnost samovznícení nebo exploze při zahřátí atd. Chybná manipulace s chemickými látkami, jako např. nedodržení technologického předpisu ohledně pořadí vnášení chemických látek do reakčního prostředí, záměna vstupních látek, přítomnost nežádoucích nečistot v dodaných chemických látkách, nedostatečné míchání a odvod reakčního tepla atd. může být příčinou nežádoucí události. Zvláštní pozornost by měla být věnována tzv. „**ujetí**“ **reakce** (runaway reaction), čímž se myslí tepelně nestabilní reakční systém, který vykazuje zrychlující se zvyšování teploty a reakční rychlosti. „Ujetí“ reakce může v konečném důsledku vést až ke ztrátě integrity zařízení. Lepší poznání procesu umožňuje zvyšování vnitřní bezpečnosti chemického procesního zařízení (inherent safety) (Ministerstvo životního prostředí ČR, 2007).

Nebezpečné situace v objektu nebo zařízení

Popis nebezpečných činností (procesů nebo skladování) uvedených v analýze rizik musí ukazovat účel a základní charakteristické rysy příslušných provozů v objektu nebo zařízení, které jsou důležité pro bezpečnost a mohou být zdrojem nebezpečí a vytvořit nebezpečné situace v objektu nebo zařízení. Tyto situace zahrnují:

- Základní provozy a činnosti.
- Chemické reakce, fyzikální a biologické přeměny a transformace.
- Dočasné skladování na pozemcích objektu nebo zařízení.
- Ostatní se skladováním související činnosti, tj. nakládku a vykládku, přepravu včetně přepravy potrubními systémy.
- Vypouštění, jímání pro usazování a ukládání, opětovné použití a recyklaci, nebo zneškodňování zbytků a odpadů.
- Vypouštění a úpravu či zpracování odpadních plynů a odplynů.
- Ostatní fáze procesu, zvláště činnosti a provozy úpravy a zpracování surovin a výrobků.

Nebezpečné situace mimo objekt nebo zařízení

Činnosti, objekty nebo zařízení mimo areál analyzovaného objektu nebo zařízení mohou být nejen předmětným objektem nebo zařízením ovlivněny, ale také jej mohou ovlivňovat. Výsledky analýzy by měly podat přiměřený důkaz, že byly identifikovány a analyzovány obě možnosti. Proto je třeba uvážit jak průmyslové činnosti prováděné mimo analyzovaný objekt nebo zařízení (tj. povahu ostatních objektů nebo zařízení a jejich vzdálenosti, omezení vyvolaná ostatními objekty nebo zařízeními, atd.), tak přepravní trasy a hlavní dopravní střediska (tj. silnice, železniční tratě, plavební dráhy, přístavy, letiště, shromaždiště, atd.).

Domino efekt

Samostatnou kapitolou v analýze rizik je posouzení kumulativních a synergických jevů a domino efektu, popř. jejich kombinací⁴⁵. Domino efektem se v analýze rizika rozumí možná eskalace událostí, kdy událost u jednoho objektu / zařízení může být příčinou události u jiného objektu / zařízení, a tím může dojít ke zvýšení pravděpodobnosti vzniku závažné havárie a ke zvýšení jejích následků v důsledku umístění podniků nebo skupiny podniků a jejich nebezpečných látek (např. ztráta obsahu jednoho zařízení vede ke ztrátě obsahu jiného zařízení, a tím k rozšíření havárie).

Příčinou vzniku domino efektu mohou být také často podceňované a přehlížené emise z netěsných komponent technologických zařízení⁴⁶, tzv. **fugitivní emise**. Únik provozního média z jedné netěsné komponenty bývá malý, ale vzhledem k jejich velkému počtu v zařízení i v celém podniku jsou tyto emise značné. U větších výroben dosahují i stovek tun za rok a běžně převyšují evidované emise z bodových zdrojů, jako jsou výduchy skladovacích nádrží, rekuperačních jednotek apod. Nemalé provozní ztráty byly jedním z důvodů, že fugitivní emise z netěsností byly řešeny nejprve z pohledu strojařského (těsnicí materiály a způsob utěsnění) a teprve následně z pohledu environmentálního (Eisler a Rousová, 2009). Jelikož ale mohou být problémem i z hlediska bezpečnostního, zaměřuje se na ně postupně pohled i v tomto směru. Fugitivní emise jsou tvořeny těkavými organickými látkami, ale může se jednat i o emise plynného vodíku. Na rozdíl od vodíku, jsou organické páry těžší než vzduch, takže v uzavřených nevětraných prostorách mají tendenci usazovat se v prohlubních, jako jsou kanály nebo šachty. V delším časovém horizontu pak v těchto místech může narůst jejich koncentrací až k dolní mezi zapálení. V případě, že jsou iniciovány, dochází k jejich mžikovému vyhoření v podobě jevu Flash fire.

45 Těmto jevům je věnován zvláštní metodický pokyn Ministerstva životního prostředí ČR pro hodnocení možnosti vzniku kumulativních a synergických účinků závažné havárie a domino efektu pro účely zákona č. 59/2006 Sb.

46 Komponenty zařízení jsou například potrubní spoje, ucpávky vřeten armatur, hřídeli čerpadel apod.

Identifikace zdrojů rizik, relativní ocenění jejich závažnosti a výběr zdrojů rizik pro podrobnou analýzu

Identifikace zdrojů rizik je vytvoření množiny zdrojů rizik na základě vlastností a množství nebezpečných látek, umístěných v objektu nebo zařízení, způsobu provozování a možných konkrétních situací uvnitř i vně objektu nebo zařízení, které mohou způsobit závažnou havárii. Je třeba také využít údaje z minulosti o předešlých výskytech nežádoucích událostí a skoronehod, havárií a závažných havárií. Analýza rizik musí dát dostatečné podklady k **hodnocení rizik** (viz kapitola 5.2.10), které s analýzou vytvářejí komplexní studii. Ta musí především prokázat, že byly identifikovány nejen všechny zdroje rizik v objektu nebo zařízení (vnitřní zdroje rizik) ve všech fázích provozu (najíždění, běžném provozu, odstavování, nakládce či vykládce, atd.), ale i vnější zdroje rizik, u kterých může dojít např. k požárům, výbuchům a únikům toxických látek ze sousedních objektů nebo zařízení a přepravy mimo objekt nebo zařízení. Rovněž je třeba vzít v úvahu i funkční závislosti na sousedních objektech nebo zařízeních, jako jsou potrubní soustavy, společné rozvody energií, vody a telekomunikací. Významnou roli hraje také nebezpečí způsobené přírodními vlivy, jakými jsou (mimořádné) srážky, vítr, extrémní teploty, blesky a statická elektřina, záplavy, sesuvy půdy a poddolování, lesní či jiný přírodní požár a obecně vzato i seismická činnost. Vždy je také třeba sledovat úlohu **lidského činitele**, a to i v podmínkách možných selhání řídicích mechanismů, která mohou vyústit v události, při kterých se uvolní nebezpečné látky a popř. energie, a které mají potenciál poškodit zdraví člověka, hospodářská zvířata, životní prostředí a majetek.

Pro identifikaci zdrojů rizik existuje řada postupů. Volba určité techniky pro identifikaci zdrojů rizik závisí na druhu objektu nebo zařízení a na charakteru rizika. Identifikace zdrojů rizik se nejlépe provádí v pracovní skupině, jejíž členové mají rozsáhlé dovednosti, technické a odborné znalosti získané z provozů objektů nebo zařízení daného či podobného typu, z provádění analýzy, z inspekční činnosti atd. Ve skupině musí být chemičtí inženýři, kteří mají zkušenosti s procesní bezpečností. Obvykle se používají tyto techniky (blíže viz tabulka 42):

- Bezpečnostní prohlídka (*Safety Review – SR*).
- Analýza pomocí kontrolního seznamu (*Checklist Analysis – CA*).
- Metody relativní klasifikace (*Relative Ranking – RR*).
- Předběžná analýza nebezpečí / zdrojů rizika (*Preliminary Hazard Analysis – PHA*).
- Analýza „Co se stane, když...“ (*What-If Analysis – W-I*).
- Studie nebezpečí a provozuschopnosti (*Hazard and Operability Analysis / Study-HAZOP*).
- Analýza způsobů a důsledků poruch (*Failure Mode and Effects Analysis – FMEA*).

- Analýza stromem poruch (*Fault Tree Analysis – FTA*).
- Analýza stromem událostí (*Event Tree Analysis – ETA*).
- Analýza příčin a následků (*Cause – Consequence Analysis – CCA*).
- Analýza spolehlivosti lidského činitele (*Human Reliability Analysis – HRA*).

Nejlépeších výsledků však lze dosáhnout kombinací několika technik. Příručka „Guidelines for Chemical Process Quantitative Risk Analysis“ doporučuje strukturovanou techniku jako je HAZOP nebo FMEA, a to jako doplněk k obecnějším technikám (jako je „bezpečnostní prohlídka“). Obecnějším přístupem budou identifikovány frekvencovanější nehodové události a náhodný výběr méně častých událostí. Kombinací obou přístupů se docílí kompletnější seznam zdrojů rizika. Pro jednotlivé fáze životního cyklu zařízení se doporučují k použití např. techniky uvedené v tabulce 42.

Volba postupů a technik použitých pro identifikaci zdrojů rizik musí být v dokumentu vysvětlena a dokladována.

Relativní ocenění závažnosti zdrojů rizik a výběr zdrojů rizik pro podrobnou analýzu je dalším krokem analýzy. V této části je provedeno ocenění zdrojů rizik a jejich výběr pro podrobnou analýzu s ohledem na vliv jednotlivých zdrojů rizika k celkovému riziku analyzovaného objektu nebo zařízení. Je třeba volit takovou metodu, která dovolí ocenit a vybrat ty zdroje rizika, které významně přispívají k celkovému riziku, a které budou pak dále řešeny podrobnou kvantitativní analýzou.

Pro účely výběru jednotlivých zařízení pro kvantitativní analýzu je nutné analyzovaný objekt nebo zařízení rozdělit na řadu tzv. oddělených (technologických) zařízení. Toto je základní úkol, který má naprosto zásadní dopad na celou další analýzu. Kritériem pro definici „odděleného“ zařízení je předpoklad, že porucha integrity pláště (obálky kontejnmentu – loss of containment) jednoho zařízení nezpůsobí významný únik látek z jiných zařízení. Současně lze považovat dvě zařízení za oddělená, pokud je možné oddělit (odpojit) je navzájem během velmi krátké doby po začátku události. Toto rozdělení je velice náročná a odpovědná záležitost a chybné provedení může výsledky následné analýzy silně ovlivnit.

Pro výběr zdrojů rizika, jejichž škodlivý potenciál je v oblasti působení na životní prostředí, existují nebo jsou dále vyvíjeny různé metody a přístupy. Jako příklad lze uvést např. metody ENVITech 03 a H & V index, uvedené v metodickém pokynu pro stanovení zranitelnosti životního prostředí ve Věstníku MŽP č. 3/2003, dále švédský index nebezpečí pro životní prostředí (Environment-Accident-Index), holandský model PROTEUS aj.

Tabulka 42: Přehled technik identifikace zdrojů rizika a jejich použití v jednotlivých fázích životního cyklu zařízení.

	SR	CA	RR	PHA	W-I	W-I + CA	HAZOP	FMEA	FTA	ETA	CCA	HRA
Výzkum a vývoj	○	○	●	●	●	○	○	○	○	○	○	○
Koncepční návrh	○	●	●	●	●	●	○	○	○	○	○	○
Poloprovoz	○	●	○	●	●	●	●	●	●	●	●	●
Detailní inženýring	○	●	○	●	●	●	●	●	●	●	●	●
Konstrukce / Najíždění	●	●	○	○	●	●	○	○	○	○	○	●
Běžný provoz	●	●	●	●	●	●	●	●	●	●	●	●
Rozšíření / Modifikace	●	●	●	●	●	●	●	●	●	●	●	●
Vyšetřování událostí	○	○	○	○	●	○	●	●	●	●	●	●
Vyřazení provozu	●	●	○	○	●	●	○	○	○	○	○	○

● Technika běžně používaná

○ Technika používaná buď výjimečně, nebo nevhodná pro určitou fázi životního cyklu zařízení

5.2.6 Identifikace možných scénářů událostí a jejich příčin, které mohou vyústit v závažnou havárii

Identifikace a popis možných příčin závažné havárie – dějů nebo stavů, které iniciují škodlivý potenciál zdroje rizika – je základním předpokladem identifikace a popis scénářů závažných havárií, což je sestavení posloupností nehodových událostí, které vedou k závažné havárii. Posloupnost je sestavena od základní události přes rozvíjející události až do koncové události scénáře. Množina všech možných nehodových událostí se sestaví bez ohledu na jejich důležitost nebo základní událost.

Závažnou havárií se rozumí „mimořádná, částečně nebo zcela neovladatelná, časově a prostorově ohraničená událost, například závažný únik, požár nebo výbuch, která vznikla nebo jejíž vznik bezprostředně hrozí v souvislosti s užíváním objektu nebo zařízení, v němž je nebezpečná látka vyráběna, zpracovávána, používána, přepravována nebo skladována, a vedoucí k vážnému ohrožení nebo k vážnému dopadu na životy a zdraví lidí, hospodářských zvířat a životní prostředí nebo k újmě na majetku“. V této souvislosti je nutno upozornit, že kritéria uvedená v příloze č. 3 k zákonu č. 59/2006 Sb. o prevenci závažných havárií vymezují závažnou havárii podle jejích následků pro účely zpracování informace o vzniku a následcích závažné havárie. Nejedná se tedy o definiční kritéria, která vymezují předěl mezi havárií a závažnou havárií, jak je často mylně uváděno. Dalším důležitým pojmem je scénář, kterým se pro účely zákona rozumí „variantní popis rozvoje závažné havárie, popis rozvoje příčinných a následných na sebe navazujících a vedle sebe i posloupně probíhajících událostí, a to jednak spontánně probíhajících, a jednak událostí probíhajících jako činnosti lidí, které mají za účel zvládnout průběh havárie“.

Při zpracování scénáře se provede výběr počátečních (iniciačních) událostí – příčin závažné havárie. Iniciační událost může mít vnitřní nebo vnější příčinu. Vnitřní příčinou může být porucha technologického zařízení (např. únik kapalného amoniaku z otvoru v potrubí následkem koroze, havárie dopravního prostředku s poškozením produktovodu), porucha řídicího zařízení (např. selhání blokování čerpadla po dosažení limitního naplnění zásobníku), nežádoucí reakce v systému (např. působení energetického impulsu na směs par hořlavé látky se vzduchem v mezích hořlavosti/výbušnosti, ujetí reakce), lidská chyba, atd. Vnější příčinou mohou být havárie objektů nebo zařízení v okolí, havárie transportních prostředků převážejících nebezpečné látky, pád letadla do areálu objektu nebo zařízení, porucha v dodávkách energií, terorismus, aj. Existují generické seznamy vnitřních a vnějších příčin, existují také různé metody pro jejich stanovení.

Počáteční (iniciační) událost je rozvíjena dalšími událostmi až do koncového bodu scénáře. Další událost buď pomáhá k vývoji nebo zabrání události nebo vede ke zmírnění následků události (např. selhání zastavení počátečního úniku kapalného amoniaku vede ke kontinuálnímu úniku amoniaku, který dále vede svým rozsahem k výsledné nežádoucí události – úniku celého přítomného množství amoniaku). Rozvíjející události scénáře, které ve scénáři předcházejí vzniku nehody, jsou selháním nebo úspěchy preventivních opatření. Rozvíjející události scénáře, které následují po vzniku nehody, jsou selháním nebo úspěchy následných opatření.

Zdroj rizika ve stavu odpovídajícím koncovému bodu scénáře působí na své okolí určitými fyzikálními nebo chemickými účinky (projevy), kterým odpovídají určité následky (ve smyslu škodlivých účinků nazývané také dopady), ale také se mohou vyskytnout fyzikální účinky bez škodlivých dopadů. V centru pozornosti je vždy taková nežádoucí událost, kdy dojde k úniku nebezpečné látky (zádrže) následkem ztráty soudržnosti zařízení, popř. poruchy integrity pláště zařízení (obálky kontejnmentu), jako je např. vznikající toxický oblak plynného amoniaku odpařováním unikajícího kapalného amoniaku z potrubí. Únik (uvolnění, emise) nebezpečné látky může být jednorázový (v podstatě okamžité uvolnění obsahu nebezpečné látky), kontinuální nebo časově omezený. Typ úniku závisí na způsobu, jakým je kontejnment (obálka) porušen, na vlastnostech přítomné chemické látky a na podmínkách skladování nebo zpracování. Pro kvalitativní popis a grafické znázornění scénářů je výhodné grafické zpracování ve tvaru „motýlek“ (bow-tie). Na levé straně tohoto grafického zobrazení jsou pomocí stromu poruch určeny příčiny kritické nežádoucí události, která je umístěna v centru zobrazení. Tato kritická nežádoucí událost je pak základní událostí rozvíjeného stromu událostí, umístěného na pravé straně tohoto grafického zobrazení, s koncovými stavy a následky a dopady těchto scénářů. Zde je možno dále rozvíjet analýzu v duchu zavedených nebo zaváděných bezpečnostních bariér (ochrany) v jednotlivých větvích logického diagramu. Jedná se o analýzu vrstev ochrany, tzv. bezpečnostních bariér, pod zkratkou LOPA (Layer of Protection Analysis), což je semikvantitativní technika použitelná po předběžné analýze rizika a po použití techniky HAZOP před náročnějšími metodami kvantitativní analýzy.

5.2.7 Výběr reprezentativních scénářů závažných havárií

Výběr reprezentativních scénářů závažných havárií je omezený soubor scénářů podobného charakteru (fyzikálních projevů a následků) nehodových událostí s určenými koncovými stavy těchto scénářů s příslušnými fyzikálními projevy. Výběr musí pokrýt celé spektrum nežádoucích událostí. Pro typická zařízení bývají obvykle známy typické scénáře havárií. Patříčnou pozornost je také třeba věnovat scénářům, které mohou mít dopad na životní prostředí.

5.2.8 Odhad následků reprezentativních scénářů závažných havárií

Skutečný rozsah projevů závažné havárie je vyjádřen určitými dopady, jako jsou zdravotní následky (expozice, zranění, smrt), škody na majetku, dopady na životní prostředí, nutnost evakuace apod. Dále se může jednat o dosah pásem ohrožení tlakovou vlnou, dosah působení tepelné radiace pro zvolenou dobu expozice, dosah zamoření pro zvolenou toxickou koncentraci aj. Odhad těchto následků a dopadů na lidi, hospodářská zvířata, majetek a životní prostředí se stanoví pomocí modelování fyzikálně chemických procesů a jevů, které se objevují v událostech a koncových stavech určených scénářů. Hodnocení následků pomáhá stanovit opatření pro prevenci závažných havárií a zmírňování jejich následků. Dále se používá pro tvorbu havarijních plánů (vnitřních i vnějších) a pro územní plánování v okolí objektů nebo zařízení.

Modelování v kontextu analýzy je určitý zjednodušený popis vybraných vlastností studovaného objektu nebo zařízení a dějů v nich probíhajících, sestavovaný pro pochopení a zobecnění jejich zákonitostí. Obvykle bývá vyjádřen matematickými pojmy. Pro sestavení matematického modelu je nutná dobrá znalost požadovaných vstupních informací a příslušných zákonitostí. Každý matematický model zachycuje reálné jevy jen přibližně, ve zjednodušené formě. Základem pro modelování fyzikálně chemických procesů a jevů je materiálová bilance posuzovaného systému. V podrobnějším popisu postupu lze uvést, že prvním krokem je modelování zdroje úniku pro popis šíření nebezpečných látek. Dále to jsou fyzikální modely transportu nebezpečné látky (odpařování nebezpečné látky z kaluže a disperzní modely pro předpověď šíření nebezpečné látky). Následuje modelování následků a zranitelnosti – modely výbuchů a jejich účinků (např. přetlak, rozlet fragmentů zařízení po výbuchu, nepřímé účinky, jako je zhroucení budov atd.), modely požárů (tepelná radiace), modely účinků pro toxické látky a modelování dopadů na životní prostředí. Většinou je třeba volit konzervativní přístup k modelování, který je založený na předpokladu, že z důvodu bezpečnosti je nutno při odhadech a výpočtech zvážit takové vstupní údaje veličin, které vystihují nejméně příznivý případ. Skutečné riziko činnosti (systému) by nemělo být horší než výsledek ocenění konzervativním způsobem. Při zavedení odpovídajících preventivních opatření by měla být zajištěna nejvyšší dosažitelná bezpečnost. Nesmí se zapomenout i na nejistotu (neurčitost) dat, protože vstupní data mohou mít určitý rozptyl a mohou být zatížena náhodnými chybami. Výpočet proto vykazuje určitou míru nejistoty, což je třeba brát v úvahu při řízení rizika.

V okamžiku, kdy dojde ke ztrátě nebo porušení soudržnosti zařízení s nebezpečnou látkou, dochází k úniku této nebezpečné látky a je třeba určit kvalitativní a kvantitativní parametry tohoto úniku, což může být provedeno použitím softwarových produktů. Pro výpočet parametrů úniku je třeba znát vlastnosti nebezpečné látky, charakteristické údaje zařízení, ve kterém se nebezpečná látka nachází, místo a dobu trvání úniku. Po určení skupenství (fáze) uniklé nebezpečné látky se určí další potřebné údaje, jako jsou např. rychlost úniku, množství mžikového odparu kapaliny, množství stržené kapaliny do oblaku a následné odpaření, rychlost odparu kapaliny z vytvořené kaluže aj.

Pro každý reprezentativní scénář by měl být následně proveden odhad jeho pravděpodobnosti. Blíže o této části analýzy technologických rizik pojednává kapitola 5.2.9.

5.2.9 Odhad pravděpodobnosti reprezentativních scénářů

Pravděpodobnost reprezentativního scénáře je vyjádření míry výskytu mimořádné události a konkrétního nežádoucího následku, ke kterému může vést. Může být vyjádřena jako četnost (např. počet událostí s daným následkem za rok), jako pravděpodobnost výskytu mimořádné události během určitého časového intervalu, nebo jako **podmíněná pravděpodobnost** (např. jako pravděpodobnost výskytu události daná výskytem předchozí události za současného splnění jisté podmínky). Kvantitativně je tato pravděpodobnost vyjádřena hodnotou nacházející se v intervalu mezi 0 a 1.

V analýze a hodnocení rizika mimořádné události vyjadřuje odhad pravděpodobnosti reprezentativních scénářů v podstatě předpověď do budoucna, protože číselně vyjadřuje předpoklad, že nastanou uvažované následky. Ačkoli se jedná o odhady, vždy pracujeme s daty získanými zkušenostmi z minulosti, tzv. **generickými daty**, takže jejich vypovídací schopnost je poměrně dobrá (alespoň řádově). Příkladem vyjádření pravděpodobnosti úmrtí člověka následkem vybraných mimořádných událostí postaveném na statistickém zpracování generických dat shrnuje tabulka 43.

Pro sestavení scénáře uvažované vrcholové události se nejčastěji využívá metoda **Analýzy stromem událostí** (Event Tree Analysis – ETA), která umožňuje i provedení výpočtu pravděpodobnosti vzniku uvažovaných následků (nebo četnosti jejich vzniku za rok). Strom událostí je logický graf, který popisuje logický rozvoj scénáře od tzv. iniciační události směrem k možným závažným následkům. Jedná se o induktivní systematický postup rozvíjející iniciační událost postupnými logickými kroky (možnými sekvencemi), kterými se berou do úvah tzv. bezpečnostní funkce systému včetně úspěšnosti takové funkce/zásahu. Výsledkem je výpočet frekvence vzniku relevantních následků pro danou iniciační událost. Příklad stromu událostí pro iniciační událost, kterou je jednorázový únik veškerého množství benzínu z automobilové cisterny, je uveden na obrázku 111. Pravděpodobnost této iniciační události byla stanovena na $5,96 \cdot 10^{-4}$ (viz obrázek 112), a podmíněné pravděpodobnosti následných událostí pak vycházejí z odborné literatury (Guidelines for Quantitative

Tabulka 43: Pravděpodobnost úmrtí člověka následkem působení různých příčin.

Příčiny úmrtí	Pravděpodobnost úmrtí člověka (rok ⁻¹)
Úmrtí ze všech příčin:	
muži ve věku 55–64 let	$1,5 \cdot 10^{-2}$
ženy ve věku 55–64 let	$9,1 \cdot 10^{-3}$
muži ve věku 35–44 let	$1,7 \cdot 10^{-3}$
ženy ve věku 35–44 let	$1,2 \cdot 10^{-3}$
děti ve věku 10–15 let	10^{-4}
Kouření (20 cigaret denně)	$5 \cdot 10^{-3}$
Cestování automobilem	$1,7 \cdot 10^{-4}$
Cestování vlakem	$3 \cdot 10^{-5}$
Cestování letadlem	10^{-5}
Těhotenství	$8 \cdot 10^{-5}$
Kopaná	$4 \cdot 10^{-5}$
Užívání plynu v domácnosti	10^{-6}
Užívání elektřiny v domácnosti	10^{-6}
Protržení hráze vodního díla	10^{-7}
Havárie JE (úmrtí osoby v okruhu do 1 km od JE)	10^{-7}
Zásah bleskem	10^{-7}
Zásah meteoritem	10^{-11}

Risk Assessment: Purple Book, 1999) a jsou uvedeny v tabulce 6 (kapitola 4.4.2). Výpočet četností (tj. pravděpodobností vzniku daného následku za rok) se provádí formou prostého součinu hodnoty pravděpodobnosti vzniku iniciační události a hodnot podmíněných pravděpodobností uvedených v jednotlivých větvích scénáře, přičemž musí platit, že součet podmíněné pravděpodobnosti pro větev „ano“ (tj. uvažovaná událost nastane) a větve „ne“ (tj. uvažovaná událost nenastane) je vždy 1. Pro kontrolu pak provedeme součet všech vypočtených frekvencí, přičemž zjištěná hodnota musí být rovná hodnotě pravděpodobnosti vzniku iniciační události.

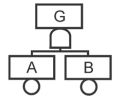
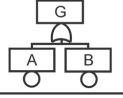
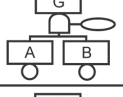
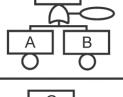
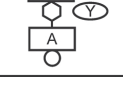
Výpočet pravděpodobnosti (četnosti za rok) vzniku nežádoucích následků pomocí ETA je podmíněn znalostí pravděpodobnosti vzniku iniciační události. Zvláště v případě průmyslových havárií je tuto skutečnost nutné akceptovat, protože každá taková iniciační událost může představovat následek působení mnoha rozličných příčin – poruch. Podobně jako strom událostí proto konstruujeme **strom poruch** (Fault Tree Analysis), který je logickým grafem sloužícím k odhalení cest, kterými se mohou v systému šířit a rozvíjet poruchy. Jde o postup deduktivní, který vychází zpětně z přesně definované konečné poruchy – vrcholové události („Top Event“) a hledají se příčiny nebo souběhy příčin, které mohou konečnou událost způsobit. Z hlediska modelování následků podle FTA je tato vrcholová událost událostí iniciační.

Frekvence jednorázového úniku veškerého množství benzínu z automobilové cisterny (rok ⁻¹)	Okamžitá iniciace	Opožděná iniciace oblaku par do 1 minuty		Další rozvoj události	Následek	Četnost (rok ⁻¹)
		od projíž- dějících motoro- vých vozidel	od pracovníků (celkem 5 osob na pracovišti)			
5,96.10 ⁻⁴	ano 0,4				BLEVE	2,38.10 ⁻⁴
	ne 0,6	ano 0,4		ano 0,4	mžikový požár (Flash fire) a požár kaluže	5,72.10 ⁻⁵
				ne 0,6	exploze oblaku par (VCE)	8,58.10 ⁻⁵
		ne 0,6	ano 0,05	ano 0,4	mžikový požár (Flash fire) a požár kaluže	4,29.10 ⁻⁶
				ne 0,6	exploze oblaku par (VCE)	6,44.10 ⁻⁶
			ne 0,95		rozptyl oblaku par	2,04.10 ⁻⁴
Suma:						5,96.10 ⁻⁴

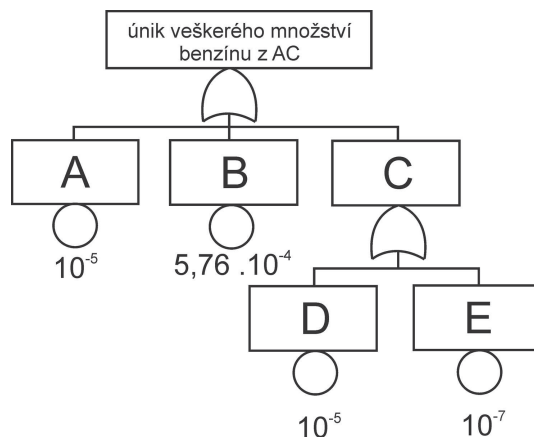
Obrázek 111: Strom událostí pro jednorázový únik veškerého množství benzínu z automobilové cisterny.

Vlastní sestavení stromu poruch má řadu kroků. Vychází se z vrcholové události, kterou analyzujeme. V dalších krocích se hledají možnosti předzvěsti vrcholové události/poruchy v jednotlivých subsystémech. Tato fáze analýzy je náročná na čas, znalosti a zkušenosti. Postupuje se tak, že se hledají dílčí události, které přispívají/vedou k vrcholové události. Závažným krokem je posouzení logického vztahu mezi dílčími událostmi a událostí vrcholovou – přiřazení logického operátoru. Pokud k vrcholové události dojde jen v případě současného výskytu všech dílčích událostí (paralelní řazení), jde o logický operátor „AND“; pokud má dílčí událost za následek vrcholovou událost (sériové řazení), jde o logický operátor „OR“ (Babinec, 2005). Hodnota pravděpodobnosti se dosazuje do příslušných logických větví ve vývoji scénáře příslušné dílčí pravděpodobnosti pro jednotlivé události, a pomocí Booleovy algebry se následně počítá výsledná pravděpodobnost pro koncové stavy scénářů (viz ČSN EN 61025). Základní matematické operace Booleovy algebry využívané ve stromech poruch zobrazuje tabulka 44.

Tabulka 44: Způsob výpočtu výsledných pravděpodobností podle Booleovy algebry.

symbol	operátor	popis / způsob výpočtu
	AND	Událost G nastává pouze tehdy, pokud se vyskytne událost A a současně i událost B.
	OR	Událost G nastává pouze tehdy, když se vyskytne buď událost A anebo událost B, popř. A i B současně.
	priority AND	Událost G nastává pouze tehdy, když nastane nejprve událost A a po té i událost B. Podmínky zaručující výskyt tohoto jevu jsou zapisovány do oválného políčka.
	exclusive OR	Událost G nastává tehdy, pokud se vyskytne buď událost A anebo událost B, ale nikdy nenastává tehdy, když se vyskytne A i B současně. Podmínky zaručující výskyt tohoto jevu jsou zapisovány do oválného políčka.
	inhibit	Událost G nastává pouze tehdy, pokud se vyskytne událost A a jsou zároveň splněny i nutné vedlejší podmínky (zapsané v oválném políčku), jejichž pravděpodobnost výskytu vyjadřuje symbol P_Y .

Pro výše uvedený příklad (viz obrázek 111) je zjednodušený strom poruch a způsob výpočtu vrcholových událostí znázorněn na obrázku 112.



$$P = (P_A + P_B + P_C) - (P_{AB} + P_{AC} + P_{BC}) + (P_{ABC}),$$

kde

$$P_C = P_D + P_E - P_{DE} = 10^{-5} + 10^{-7} - 10^{-5} \cdot 10^{-7} = 1,01 \cdot 10^{-5}$$

takže výsledná frekvence vzniku vrcholové události P je:

$$\begin{aligned} P &= (10^{-5} + 5,76 \times 10^{-4} + 1,01 \times 10^{-5}) - (10^{-5} \times 5,76 \times 10^{-4} + 1,01 \times 10^{-5} \times 1,01 \times 10^{-5} + \\ &\quad + 5,76 \times 10^{-4} \times 1,01 \times 10^{-5}) - (10^{-5} \times 5,76 \times 10^{-4} \times 1,01 \times 10^{-5}) = \\ &= 5,96 \times 10^{-4} + 1,16 \times 10^{-8} - 5,76 \times 10^{-14} \\ &= 5,96 \times 10^{-4} \end{aligned}$$

Obrázek 112: Strom poruch vedoucích k vrcholové události „Jednorázový únik veškerého množství benzínu z automobilové cisterny“.

5.2.10 Stanovení míry rizik a hodnocení jejich přijatelnosti

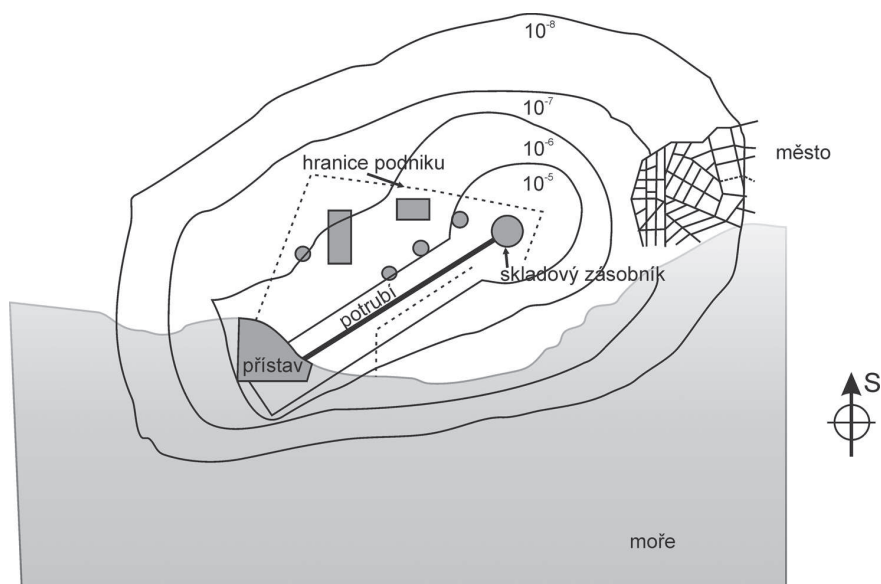
Pojem riziko vyjadřuje relaci mezi závažností následků události a neurčitostí spojenou s výskytem mimořádné události, například její pravděpodobností (nebo odhadovanou frekvencí výskytu) (Babinec a Vacek, 2008). Proces používaný pro stanovení ukazatele (míry) analyzovaných rizik pak nazýváme hodnocením rizik. To sestává z analýzy četnosti, analýzy následků a z kombinace odhadnutých následků a pravděpodobností ze všech vybraných (nežádoucích) událostí (Encyklopedie BOZP, online). Pro vyjádření míry rizika reprezentativních scénářů mimořádných událostí (závažných havárií) se nejčastěji používá stanovení individuálního a společenského rizika. Tyto dvě formy míry rizika jsou kvantitativními ukazateli, což ovšem s sebou zákonitě přináší požadavek na zavedení kritérií pro jejich hodnocení. Otázka kvantitativního posuzování rizik je předmětem celé řady prací. V historickém přehledu studií věnovaných hodnocení rizik však nejvýznamnější roli hraje Holandsko a Velká Británie (Babinec a Vacek, 2008).

Individuální riziko

Individuální riziko je riziko pro osobu v určitém místě v blízkosti zdroje rizika a představuje v podstatě pravděpodobnost (nebo frekvenci) události, při které v průběhu roku jednotlivec (někdo z veřejnosti) je postižen uvažovaným následkem (např. úmrtím, zraněním, obdržením nebezpečné toxické dávky apod.). Individuální riziko by vždy mělo být doplněno časovým úsekem, ke kterému se tato míra vztahuje (obvykle je to jeden rok). Geografické rozdělení individuálního rizika v různých bodech v okolí zdroje rizika je prezentováno izoliniemi rizika. Vypovídací hodnota tohoto zobrazení je taková, že uváděné kontury demonstrují „dosah rizika“ od jeho zdroje (viz obrázek 113). To znamená, že samotná hodnota individuálního rizika vůbec nezávisí na hustotě populace v okolí zdroje rizika. Pokud bychom jako následek uvažovali obdržení toxické dávky od nebezpečné plynné látky emitované z uvažovaného zdroje, pak izolinie představují spojnice míst, kde jednotlivec obdrží stejnou toxickou dávku.

Ačkoli vyhláška č. 8/2000 Sb., která stanovovala kritéria přijatelnosti rizika závažné havárie (individuálního i společenského) již není v platnosti, přesto se jako přijatelná četnost možného ohrožení života v důsledku vzniku závažné havárie pro jednu osobu (tj. hodnota pro přijatelnost individuálního rizika) stále doporučují hodnoty $F_p = 10^{-5}$ pro stávající objekt nebo zařízení, resp. $F_p = 10^{-6}$ pro nový objekt nebo zařízení.

Pro maximální vypovídací schopnost hodnoty individuálního rizika by měla být specifikována i povaha uvažovaného zranění, zdroj rizika a identita jednotlivce (napří-



Obrázek 113: Znáznornění izolinií individuálního rizika v okolí zdrojů rizik.

klad u zaměstnanců je to obvykle informace o pracovním místě a druhu vykonávané pracovní činnosti). Individuální riziko je obvykle používáno pro označení, jak významné je hrozící riziko ve srovnání s latentním („pozaďovým“) rizikem, kterému je jedinec vystaven. Často je však udávána pouze nejvyšší hodnota individuálního rizika, nebo individuální riziko v několika vybraných oblastech či místech okolo zdroje rizika. Někdy se také lze setkat s mírou rizika, které je považováno za tzv. **průměrné individuální riziko**. Statistiky individuálního rizika (např. statistika úmrtí na silnicích) jsou ale zprůměrnovány na celou populaci, takže vypovídací schopnost takovéto hodnoty je pak pro konkrétní místo naprosto zavádějící. V kontextu rizika u průmyslových provozů je pak průměrné individuální riziko vypočítáno obvykle dělením očekávané hodnoty rizika počtem lidí, kteří jsou danému riziku vystaveni, čímž dostaneme jediné číslo s jednotkami úmrtí na osobu a rok. Lákavost tohoto parametru je v tom, že poskytuje přímé porovnání se statistikami individuálního rizika ostatních provozovatelů zdrojů rizik. Jenže, často je problém definovat relevantní počet lidí, kteří jsou danému riziku skutečně vystaveni. Výpočet průměrného individuálního rizika tak může snadno vést ke zkresleným výsledkům (a následně i špatné interpretaci), protože z čistě matematického hlediska i pouhé zvýšení počtu lidí, kteří jsou prohlášeni, že jsou riziku vystaveni, může hodnotu individuálního rizika snižovat, což ale není zdaleka v souladu s realitou (Sadhra a Rampal, 1999).

Četnost smrtelných úrazů

Alternativní způsob, jak vyjádřit individuální riziko při práci, je četnost smrtelných úrazů (FAR – Fatal Accident Rate), což umožňuje srovnání s jednotlivými statistikami z různých průmyslových odvětví. Statistika je postavena na průměrném počtu úmrtí na 100 miliónů pracovních hodin, ale je-li použita jako nástroj pro zjišťování zhoršování úrovně prevence rizik, potom se FAR obvykle uplatňuje na jednotlivce nebo na pracovní místo (druh práce). Jako míra individuálního rizika se obvykle netýká havárií s mnoha úmrtími, ačkoli bylo její použití jako míry skupinového rizika příležitostně navrhováno. Je třeba pečlivě interpretovat význam toho, co je potom další forma vyjádření rizika mnohonásobného úmrtí ve tvaru jednoho čísla. Koncept FAR se prokázal jako užitečný nástroj pro zjišťování vysokého rizika a při poskytování praktických cílů pro konstrukci (projekci) při snižování rizik. FAR se může vztahovat na individuální riziko matematicky, což může být i výhodné.

Procesní průmysl ve Velké Británii (tj. těžba ropy a plynu, výroba energie a chemický průmysl) má dlouhodobou míru rizika FAR okolo 4 až 5. Tato míra se snížila v průměru na hodnotu 1, vyloučíme-li sektor těžby ropy a plynu (díky 167 mrtvých, kteří zahynuli při havárii na plošině Piper Alpha v roce 1988). FAR o hodnotě 1 se dá přibližně vyjádřit jako jeden smrtelný úraz na 1000 celoživotních pracovních dob nebo jeden smrtelný úraz na 50 let pro podnik s tisíci zaměstnanci (Sadhra a Rampal, 1999).

Společenské riziko

Společenské (skupinové) riziko je riziko, kterému je vystavena skupina lidí ovlivněných událostí (postižených následky havárie). Je vyjádřeno jako vztah mezi frekvencí a počtem lidí, kteří budou určitým způsobem poškozeni (Ministerstvo životního prostředí, 2007). Toto riziko se vztahuje k určité konkrétní skupině lidí žijících v blízkém okolí zdroje rizika, kteří mohou být ovlivněni uvažovanou mimořádnou událostí. Zákon definuje riziko jako pravděpodobnost vzniku nežádoucího specifického účinku, ke kterému dojde během určité doby nebo za určitých okolností. V analýze rizik se proto provádí popis rizika použitím tzv. rizikových tripletů (pro i -tou událost scénář s_i této události, pravděpodobnost jejího výskytu p_i a následky této události n_i). Riziko pak sestává z řady trojic: $R = \{s_i, p_i, n_i\}$. Míra rizika v kvantitativní analýze je tedy číselné vyjádření kombinace výsledku odhadu následků a odhadu pravděpodobnosti analyzovaného scénáře nežádoucí události.

Obvykle se hodnocení společenského rizika znázorňuje pomocí tzv. matice rizik, kde se hodnotí vztah mezi frekvencí mimořádné události F a jejími následky N . Pro odlišnou míru rizika událostí s nízkou frekvencí a vysokými následky oproti událostem s vysokou frekvencí, ale s nízkými následky, se používá tzv. **vážené riziko**, které zahrnuje mocninový koeficient. Tento vztah je vyjadřován ve tvaru:

$$k = F \times N^2, \quad (5-12)$$

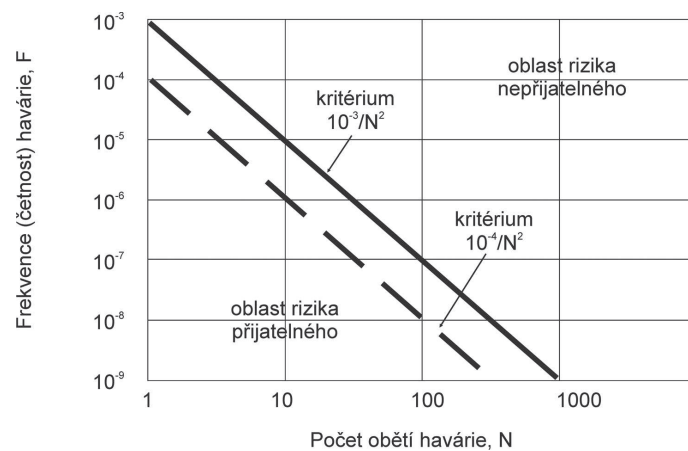
kde F je frekvence výskytu neočekávané mimořádné události, N je rozsah následků události (počet fatálních zranění) a k je konstanta (obvykle pro dané spektrum událostí a lokalitu). Na základě studií a analýz společenského rizika realizovaných v Holandsku v roce 1980 bylo kritérium (mez) nepřijatelnosti rizika stanoveno ve tvaru:

$$F \times N^2 = 10^{-3}, \quad (5-13)$$

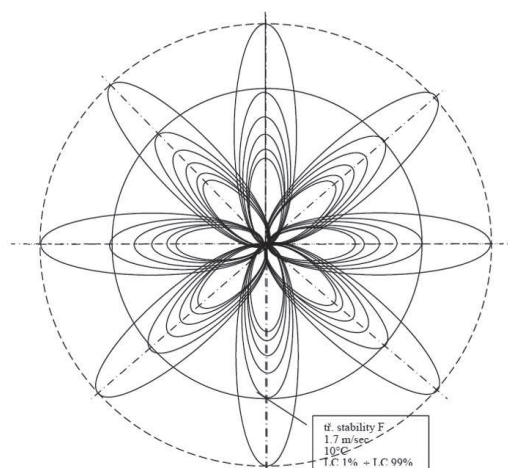
což platí pro stávající objekty nebo zařízení; pro nové objekty nebo zařízení je doporučováno kritérium přijatelnosti rizika ve výši 10^{-4} (viz obrázek 114), a jakožto kritérium zanedbatelnosti rizika některé zdroje považují hodnotu 10^{-5} , ovšem dlužno podotknout, že toto kritérium není všeobecně uznáváno.

Kumulativní riziko

Hodnocení kumulativního společenského rizika v případě hodnocení dopadů úniků toxických látek je úloha časově náročná, pokud není k dispozici nákladné programové vybavení. Nelze ji objektivně nahradit hodnocením několika vybraných scénářů. Hodnocení jevu popsáního větrnou růžicí vyžaduje výpočty pro úplné jevové pole.



Obrázek 114: Vyjádření kritérií přijatelnosti pro společenské riziko.



Obrázek 115: Modelování následků pro zvolenou třídu stability atmosféry, rychlost větru a zvolené hodnoty LC (Babinec a Vacek, 2008).

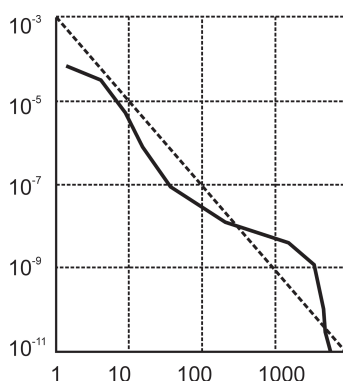
Růžice je charakterizována:

- šesti třídami stability ovzduší A až F podle Pasquillovy typizace,
- třemi třídami rychlosti větru a
- čtyřmi hlavními a čtyřmi vedlejšími světovými stranami.

Odhad ztrát vyžaduje výpočty pro letální koncentrace LC_1 až LC_{99} (tj. celkem 11 půdorysných stop oblaku) pro každou výše popsanou atmosférickou situaci. S ohledem

na rozložení osob v terénu jsou odhady ztrát neopakované. Složením těchto informací lze jednoduše získat představu o pracnosti hodnocení kumulativního rizika. Jistou představu o rozsahu prací dává obrázek s vyznačenými vybranými půdorysnými stopami oblaku orientovanými podle hlavních a vedlejších světových stran pro jedinou třídu stability ovzduší a jednu rychlost větru. Jen pro jedinou třídu stability ovzduší je potřeba pro tři charakteristické rychlosti větru sestavit tři takovéto obrazce (viz obrázek 115) (Babinec a Vacek, 2008).

Pokud se vybrané jednotlivé scénáře nachází v blízkosti kritéria přijatelnosti, je nutno počítat s tím, že při kumulaci účinků padne posuzovaný zdroj do oblasti nepřijatelnosti rizika. Případný výsledek hodnocení kumulativního rizika je patrný z následujícího obrázku 116.



Obrázek 116: Posouzení kumulativního společenského rizika (Babinec a Vacek, 2008).

Situace je navíc komplikovaná i tím, že jeden zdroj rizika bývá charakterizován zpravidla několika scénáři mimořádné události (v tomto případě závažné průmyslové havárie), a to minimálně okamžitým a kontinuálním únikem veškerého množství nebezpečné látky ze zařízení. K tomu přistupují i scénáře méně závažné (odfouknutí pojistného ventilu, unik poškozeným těsněním, utržení trubky malého DN, malý otvor na potrubí atd.). V praxi se stává, že několik zdrojů rizika ovlivňuje prakticky stejnou skupinu obyvatel, u každého zdroje rizika je nutno počítat s několika závažnými scénáři (Babinec a Vacek, 2008).

Na rozdíl od společenského rizika, se individuální riziko vyjadřuje ke všem relevantním scénářům mimořádné události. Odborná literatura (Guidelines for Quantitative Risk Assessment: Purple Book, 1999) ale uvádí, že pro výpočet individuálního rizika mohou být některé události zanedbány. Jedná se například o tlakové účinky události typu BLEVE, neboť účinky tepelné radiace způsobené ohňovou koulí (na nechráněné jednotlivce) výrazně převažují ve srovnání s účinky tlakové vlny. Tato úvaha je jistě oprávněná, avšak nelze ji automaticky aplikovat, zvláště pak v případě

společenského rizika. Výsledky experimentů totiž naznačují, že účinky tlakové vlny ve vzdálenostech odpovídajících tepelnému záření 35 kW.m^{-2} odpovídají přetlakům 10 až 30 kPa. Tento přetlak může způsobovat poškození oken, vznik střepů a snížení ochrany proti sekundárním následkům. Navíc sklo také částečně vede tepelné záření a může tedy praskat vlivem intenzivního tepelného záření. Jelikož jsou velmi často velké plochy stěn vyrobeny ze skla, zejména v kancelářských budovách, je sporné, zda předpoklad, že jsou lidé uvnitř těchto budov plně chráněni, ještě platí. Zmíněný předpoklad, že lidé uvnitř budov jsou plně chráněni, pokud intenzita tepelného záření je menší než 35 kW.m^{-2} , je založen na skutečnosti, že:

- lidé uvnitř jsou schopni nalézt úkryt uvnitř budovy během velmi krátkého času a
- lidé uvnitř neutrpí smrtelné zranění pořezáním střepinami skla.

Hodnocení přijatelnosti rizika

Hodnocení přijatelnosti rizika v oblasti prevence závažných havárií je komplexní proces vycházející z kvantitativního stanovení četnosti nebo pravděpodobnosti nežádoucích událostí a jejich následků, jak již bylo uvedeno výše. Podle dikce zákona o prevenci závažných havárií (zákon č. 59/2006 Sb. v platném znění) se jedná o zhodnocení dopadů na životy a zdraví lidí, hospodářských zvířat a dopadů na životní prostředí a majetek. Hodnocení musí být vždy doplněno rozhodnutím o závažnosti rizika nebo jeho složek podložených výsledky analýzy rizik, anebo jeho porovnáním s cílovým rizikem, ke kterému bychom se chtěli přiblížit v tzv. ideálním případě (tj. míra rizika, kterou provozovatel nebezpečné technologie nebo zařízení považuje za přijatelnou).

Objektivní hodnocení přijatelnosti rizika se provádí porovnáním hodnoty odhadnutého rizika závažné havárie v objektu nebo zařízení s hodnotami mezní přijatelnosti rizika (kritérii přijatelnosti rizik), což umožňuje svým způsobem poskytovat údaje, které jsou vzájemně srovnatelné s údaji od jiných provozovatelů. Tato skutečnost je důležitá pro orgány, které se vyjadřují k bezpečnostní dokumentaci a tedy i ke způsobu provedení a závěrům analýzy a hodnocení rizik (krajské úřady, Ministerstvo životního prostředí, Hasičský záchranný sbor, orgány ochrany veřejného zdraví apod.). Na základě odborných stanovisek dotčených orgánů, může krajský úřad (a pouze ten) vydat následné rozhodnutí o schválení či neschválení bezpečnostní dokumentace, což ale nelze zaměňovat s vyjádřením rozhodnutí o přijatelnosti či nepřijatelnosti rizika nebo jeho dílčích složek.

Dnes nám tento výše uvedený postup připadá jako rutinní a běžný a nepochybujeme o jeho správnosti, stejně jako o kritériích přijatelnosti rizik (viz výše). Jenže vývoj, který k tomuto systému vedl, byl složitý. Už v roce 1976, tj. v roce, kdy se stala havárie v italském Sevesu, navrhl v reakci na tuto událost Poradní výbor pro závažná rizika při Komisi pro zdraví a bezpečnost HSC (Health and Safety Commission

Advisory Committee on Major Hazards, 1976), aby hranice přijatelnosti pravděpodobnosti vzniku závažné průmyslové havárie byla jednou za 10 000 let. Je zajímavé poznamenat, že tato hodnota je totožná s kritériem, které je používáno v Holandsku pro určování výšky protipovodňových hrází. Norské úřady naproti tomu používaly pro hodnocení bezpečnosti a spolehlivosti koncepčních návrhů offshore konstrukcí hodnotu $9 \cdot 10^{-4}$ za rok, ale nyní požadují, aby si společnosti vypracovaly samy vhodná kritéria přijatelnosti rizik pro svá zařízení. V roce 1986 Holandské úřady publikovaly kvantitativní kritéria pro individuální a společenské riziko (Sadhra a Rampal, 1999). Lans a Bjordal prověřili řadu studií se závěrem, že v podniku procesního průmyslu, který byl projektován podle správných konstrukčních standardů a který je správně provozován a udržován, je nepravděpodobné, že by závažná havárie s katastrofálními následky vznikla častěji než jednou za 10 000 let (tj. 10^{-4} za rok) (Lans a Bjordal, 1985). Nicméně, některé události s velmi nízkou pravděpodobností vzniku mohou mít potenciálně rozsáhlé následky, což by mělo být výzvou k tomu, abychom se na ně připravili. Pasman pak s ohledem na tato fakta nedávno prověřil současné chápání toho, jak jsou technologická rizika společností vnímána, a jaká jsou kritéria pro jejich akceptování, resp. tolerování (Sadhra a Rampal, 1999).

Akceptování, resp. tolerování rizik

Je důležité si uvědomit, že přijetí činnosti určitého podniku či zařízení by nemělo být pouze na základě samotného rizika. To by mohlo vést k automatickému přijímání návrhů, které pouze splňují kritéria a k odmítání návrhů, které je nesplňují pouze těsně. Není pravděpodobné, že se dosáhne rozumného rozhodnutí, pokud se nevezme v úvahu nejistota v odhadu rizik, náklady na omezení rizik a ostatní náklady či výhody, které pro veřejnost daný provoz může mít. Ale může být užitečné stanovit cíle pro konstruktéry a projektanty a mít na paměti, že jsou jisté úrovně rizika, které veřejnost nepřejde bez ohledu na náklady na jejich omezení či na výhody, které by jejich akceptováním vznikly. Relativní význam kvantifikace odhadů rizika tak může být v podobě srovnání s ostatními riziky, se kterými se lidé setkávají ve svém každodenním životě. Je známo, že ochota jednotlivce přijímat riziko nezávisí pouze na velikosti tohoto rizika, ale na mnoha dalších, často složitých, faktorech. Je však možné v číselném řádu vyjádřit úroveň, na kterých dodatečné riziko působící na jedince je nutné považovat za nepřijatelné, protože by toto riziko bylo větší, než riziko při činnostech, které člověk podniká dobrovolně. Na této úrovni riziko může významně přispívat k průměrnému celkovému riziku úmrtí z jakýchkoli příčin v jednom roce. Stejně tak je také možné řádově vyjádřit úroveň rizika pro jednotlivce, které lze považovat za bezvýznamné, protože jsou mnohem nižší, než průměrné riziko smrti od nehod, a které jsou ve velikosti řádově podobné událostem, nad kterými jedinec nemá jakoukoli kontrolu. Tyto horní a dolní meze rizika určují obvykle rozsah dvou až tří řádů, ve kterém by mělo riziko být pečlivě zvažováno v souvislosti s mnoha dalšími faktory. Tyto faktory mohou zahrnovat hlediska environmentální, pracovní či faktory týkající se běžného občanského života ve společnosti (Sadhra a Rampal, 1999).

Přijatelnost rizika jednotlivců a společností se vyjadřuje v pojmech akceptovatelnost rizika a tolerovatelnost rizika. **Akceptovatelné riziko** je takové riziko, na které je jednotlivec pro účely vlastního života nebo práce připraven, bez jakéhokoliv ohledu na jeho řízení. **Tolerovatelné riziko** je naproti tomu takové riziko, se kterým je společnost ochotná žít pro zabezpečení svých příjmů a v důvěře, že toto riziko je správně řízeno, kontrolováno a dále redukováno. Již z těchto formulací je zřejmé, že filozofie přijatelnosti rizika záleží na sociálních, ekonomických a politických faktorech a na vnímaném prospěchu vznikajícím kladnou činností zdrojů rizik. Prospěch, resp. neprospěch (v jakémkoli pojetí) je nejčastěji posuzován z pohledu vynaložených nákladů společností vůči významnosti přínosů pro celou společnost.

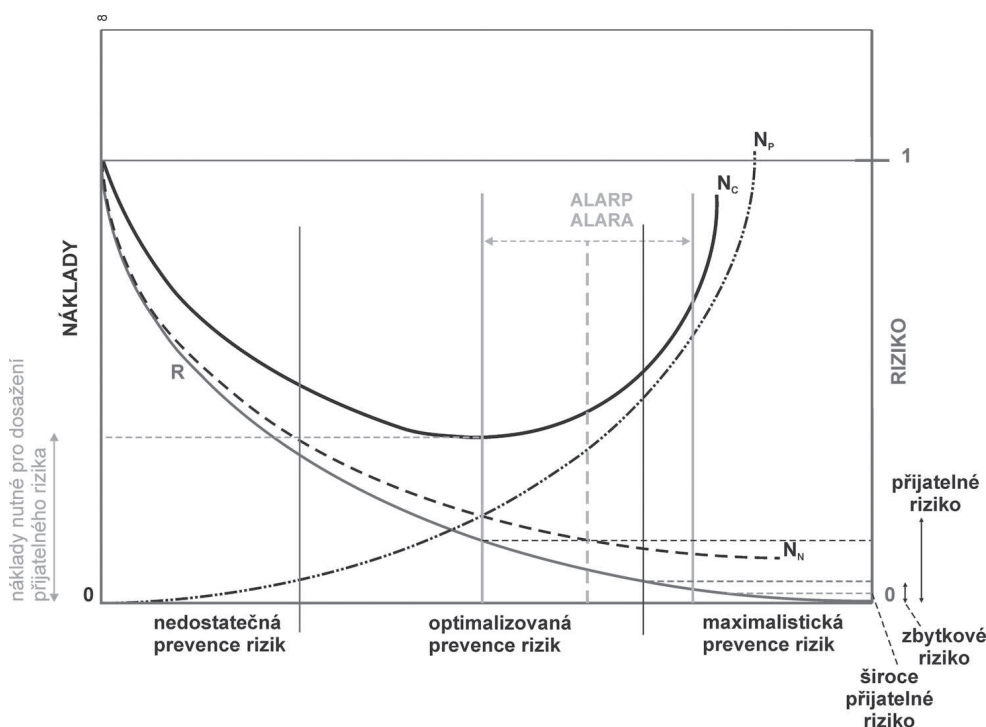
Je známo, že veřejnost ochotně akceptuje riziko až o tři řády vyšší, pokud toto riziko vyplývá z aktivit, kterých se zúčastňuje dobrovolně. Příkladem může být vnímání rizika obyvateli osady nacházející se v blízkosti chemické továrny, v níž se nakládá s nebezpečnými chemickými látkami, ale v níž je většina z těchto obyvatel zaměstnána. Tito lidé považují továrnu za zdroj svých příjmů a automaticky a ochotně přijímají riziko, které pro ně může představovat přítomnost nebezpečné látky nejen v areálu továrny, ale i mimo něj. Tito lidé, resp. jednotlivci, tedy akceptují stávající riziko v takové míře a podobě, v jaké již existuje a nemají tedy potřebu „tlačit“ na jeho snižování (a to z nejrozumnějších důvodů – např. aby se nevystavili hrozbě propuštění).

Jiným případem je tolerování rizika ze strany společnosti. Tolerovatelnost je nutno vztáhnout k obecnému vnímání prospěchu, na rozdíl od akceptování, které se vztahuje více k prospěchu individuálnímu. Pojem tolerovatelnost rizika byl převzat patrně z aplikované toxikologie, kde je v podobě tzv. „tolerovatelného horního limitu přívodu“ používán pro vyjádření maximální hladiny celkového chronického přívodu určité toxické látky za jednotku času a ze všech jeho zdrojů, přičemž se soudí, že je nepravděpodobné, aby tato hladina představovala riziko škodlivého zdravotního efektu pro člověka (člověka ve smyslu živočišného druhu nikoli jako jednotlivce). Z této formulace lze jednoznačně vyvodit, že se v případě rizika, které je vyvoláno kupříkladu provozem výrobní linky, jedná o takovou jeho úroveň, která je sice vyšší než míra rizika úmrtí vyvolaného přirozenými a neovlivnitelnými příčinami, avšak jehož úroveň (míra) ještě nepředstavuje žádné statisticky významnější negativní odchylky. Neboli teoretická četnost vzniku fatálních následků způsobených zmíněnou výrobní linkou u skupiny lidí žijících v blízkosti továrny statisticky nepřevyšuje hodnoty, na které je zdejší společnost zvyklá (např. i s ohledem na historický kontext, zkušenosti s provozovatelem továrny apod.). Zjednodušeně lze uvést příklad výskytu závažné havárie, při níž zemře někdo z lidí mimo areál továrny s průměrnou frekvencí jednou za 50 let, což zdejší společnost všeobecně přijímá jakožto frekvenci přijatelnou, protože ve srovnání s počty zdejších obyvatel, kteří za jeden rok zemrou na silnicích, je uvažovaný počet lidí usmrčených při průmyslové havárii přepočtený také na časový úsek jednoho roku naprosto nevýznamný. Lidé si tedy sice uvědomují nebezpečí, které továrna představuje, ale příliš tento fakt nevnímají, protože s ohledem na jejich životní zkušenosti nepředstavuje riziko nadmíru významné.

5.2.11 Snižování rizik

Každý provozovatel je povinen rizika nejen vyhledávat a vyhodnocovat, ale také cíleně snižovat. To je sice nejen jeho zákonná povinnost, ale také morální odpovědnost vůči společnosti, jíž se může jeho jednání dotýkat. Provozovatel však vždy při snižování rizik stojí před nutností vydávat nemalé finanční částky. Požadavky na bezpečnost ze strany veřejnosti či regulačních orgánů by tedy i kromě své oprávněnosti měly respektovat také další souvislosti, včetně ekonomických. Na jedné straně stojí provozovatel, který provozuje danou továrnu za účelem zisku (tedy profituje z jejího provozu), na druhé straně tentýž provozovatel je významným zaměstnavatelem v regionu, a je tak zdrojem finančních příjmů nejen pro místní obyvatele, ale také pro místní samosprávu (v podobě daní) a sekundárně i pro širší region (např. přidružené služby apod.). Proto je vždy potřeba provádět optimalizaci nákladů na řízení rizika.

Jelikož se opatření na snížení rizika hodnotí i po stránce jejich efektivnosti, tedy z pohledu toho, co vlastně přinesou, obvykle se v praxi aplikuje analýza poměru vynaložených nákladů k výslednému přínosu – tzv. **Cost-Benefit Analysis (CBA)** – analýza nákladů a přínosů (viz obrázek 117). Každý náklad se pochopitelně vztahuje ke konkrétnímu opatření, které je pro snížení rizika zavedeno. Může se jednat o opatření snižující rozsah následků potenciální mimořádné události (např. velká ná-



Obrázek 117: Zhodnocení nákladů a přínosů ve vztahu k přijatelnosti rizika.

drž s nebezpečnou látkou je nahrazena více nádržemi s menší zadrží, či používání menšího počtu nebezpečných látek), anebo o snížení pravděpodobnosti vzniku mimořádné události (např. zavedení záložního zařízení, potrubního obchvatu, alarmů a detekčních zařízení apod.). Kvantifikace je část analýzy, která vymezí všechny kvantifikovatelné „ocenitelné“ ukazatele projektu a převede je na hotovostní toky. Tím může docházet ke srovnávání. „Neocenitelné“ přínosy a náklady, které nelze žádným způsobem kvantifikovat, budou popsány slovně. V tomto ohledu může použití analýzy nákladů a přínosů narazit na velký problém, který se týká přiřazení pomyslné peněžní hodnoty za ztrátu lidského života. Cenu lidského života pochopitelně nelze určit z nějakých tabulek, nicméně pro snižování a optimalizaci rizik se bez této pomyslné hodnoty neobejdeme (blíže viz kapitola 4.9.2). Metody využívající tato data se užívaly po mnoho let zvláště v oblasti bezpečnosti silničního provozu při stanovování, které projekty na zlepšení stavu silnic by se měly zavést, a které mohou s ohledem na disponibilní finanční prostředky počkat. Navzdory dobrému úmyslu ale mohou nastat okolnosti, kdy tento přístup vzbudí prudkou veřejnou debatu. Klíčové při použití tohoto přístupu je, že se musí vzít v úvahu rozdíl mezi rizikem, kterému je vystaven zaměstnanec a rizikem, kterému je vystavena veřejnost. Zaměstnanci mají při akceptování rizika možnost volby a mohou mít jistý finanční prospěch prostřednictvím své mzdy. Naopak, veřejnost má při tolerování rizika obvykle jen velmi malou možnost volby a obvykle nezíská ani žádné bezprostřední finanční přínosy. Rozdíly v úrovni přijatelného rizika pro zaměstnance a pro veřejnost jsou nyní uvažovány při stanovování kritérií a je třeba je respektovat při analýze nákladů a přínosů (Sadhra a Rampal, 1999).

Smyslem CBA analýzy je tedy nalézt optimální poměr mezi požadovanou úrovní rizika, kterou považujeme již za přijatelnou (nikdy nelze ale docílit nulového rizika), a náklady nutnými k realizaci všech potřebných opatření v souvislosti se snižováním rizika na tuto úroveň. Velmi dobře tuto skutečnost rámcově zachycuje obrázek 117.

Do tohoto obrázku bylo zkomprimováno množství různých informací, proto je potřeba dobře pochopit všechny ukazatele. Na ose x je vynesena kvalitativní údaj o úrovni přístupu v prevenci rizik (od nedostatečné prevence až po přehnaně maximalistickou), na ose y vlevo pak náklady vynaložené na prevenci rizik (resp. snižování rizik), a vpravo pak celkovou míru rizika od 0 do 1. Čerchovaná křivka N_P znázorňuje závislost mezi přístupem k prevenci rizik a vynakládanými prostředky – čím více se snažíme snižovat rizika, tím více peněz nás to stojí. Naopak naprostá absence a nezájem o prevenci rizik je v tomto směru také nejlevnější. Čárkovaná křivka N_N naproti tomu ale znázorňuje vztah mezi přístupem k prevenci rizik a náklady, které je třeba vynaložit v případě vzniku mimořádné události (včetně pracovních úrazů, provozních odstávek, oprav apod.). I v tomto případě platí logická závislost, že čím více se snažíme snižovat riziko, tím méně peněz nás pak stojí řešení vzniklých problémů a nehod (nehod je méně a zároveň jejich následky nebývají tak závažné, jako v případě nízké úrovně prevence rizik). Spojením těchto křivek v jednu (prostým součtem) získáme černou křivku N_C , jejíž minimum nám po vynesení na osu nákladů (levá strana grafu) vyznačuje náklady nutné na dosažení přijatelného rizika (zde jsou

zahrnuty jak náklady na realizaci příslušných preventivních opatření, tak i náklady spojené s řešením případné nežádoucí události). Promítneme-li průsečík křivek N_P a N_N na osu rizika (pravá strana grafu), získáme informaci o úrovni rizika, které lze již považovat za přijatelné. Na ose x pak tento bod vymezuje střed oblasti optimalizované (rozumné) prevence rizik a zároveň nejnižší úroveň uplatňovaných v principech managementu rizik známých jako **ALARP** a **ALARA** (detailněji bude rozebráno níže). Přibližně ve třičtvrtině vymezené oblasti principů ALARP a ALARA se nachází pomyslná úroveň rizika, která je nazývána **zbytkové riziko**. Jelikož je každá věc na světě zdrojem určitého nebezpečí (je to latentní vlastnost dané věci vyplývající z její konstrukce, vnitřního uspořádání, složení, umístění, fyzikálních a chemických vlastností apod.), je s ním i spojeno riziko, že způsobí nežádoucí následky (jakékoli). V případě zdrojů rizik nacházejících se v průmyslu, představuje zbytkové riziko takové riziko, které zůstává i po uskutečnění všech bezpečnostních opatření a po implementaci žádoucích postupů řízení rizika. Při pohledu na osu x můžeme vidět, že zbytkové riziko vlastně vymezuje pomyslnou hranici mezi optimalizovanou a maximalistickou prevencí rizik. Z obrázku 117 a z uvedeného výkladu je ale také zjevné, že přístupy ALARP a ALARA jdou dokonce až za hranici přijatelného rizika, a spadají tak částečně až do oblasti maximalistické prevence rizik, která je značně finančně nákladná. Je však na straně bezpečnosti a pro mnohé firmy je ještě na horní hranici ekonomické odůvodnitelnosti.

Pokud se riziko dostane do oblasti neakceptovatelného rizika, pak musí být redukováno. Další možností je, že předmětné riziko se dostane do oblasti tolerance rizika, tudíž riziko je přijatelné, protože se dosahuje žádoucího užitku z provozované činnosti. Zde se může riziko přibližovat těsně k horní hranici přijatelnosti, pak je riziko tolerovatelné, jestliže redukce rizik je neproveditelná nebo její následky jsou očividně v disproporci k získanému zlepšení. Toto je třeba v dokumentu doložit. Pokud se předmětné riziko nachází v akceptovatelné oblasti rizika, pak nejsou potřeba dodatečná opatření k jeho snížení, ale je třeba doložit, že je udržován stav potřebný k udržení jistoty, že riziko zůstává v této úrovni. Uvedené principy sleduje i text § 2 vyhlášky č. 256/2006 Sb., kde v odstavci 4 je uvedeno: V případě, že výsledná hodnota rizika závažné havárie se jeví pro daný zdroj rizika jako nepřijatelná, provede se podrobnější analýza, a dle potřeby se stanoví a realizují organizační a technická opatření ke snížení tohoto rizika, prověřená opakovanou analýzou a hodnocením rizika. Přijatelnost nebo nepřijatelnost rizika pro daný objekt nebo zařízení je dána souhrnem výsledků provedené analýzy a hodnocení rizik a vyhodnocení dalších místních podmínek a faktorů, zejména sociálních, ekonomických, užívání území a dalších.

Z obrázku 117 je tedy zřejmé, že tam, kde jsou rizika méně závažná, tam se i méně vyplatí je snižovat. Na nižší úrovni, kde lze rizika považovat za široce přijatelná, jsou úrovně (hodnoty) rizik tak nevýznamné, že jejich další snižování není zapotřebí. Za **široce přijatelnou úroveň rizika** jsou považována taková rizika, která ve srovnání s riziky, kterým člověk ve společnosti obvykle čelí, jsou bezvýznamná – jejich míra je tedy ještě nižší než míra zbytkového rizika (Sadhra a Rampal, 1999).

Závěrem je potřeba ještě zmínit důležitou skutečnost, a to, že je nutné rozlišovat mezi principy ALARP a ALARA, v čemž se často chybuje. Z principu ALARP vyplývá, že při posuzování rizika mohou být celkové náklady i technické a organizační těžkosti spojené s jeho snižováním poměřovány s přínosy, které snížení rizika přinese, kdežto z principu ALARA vyplývá, že při snižování rizika by mělo být přijato přísnější prověření technické proveditelnosti tohoto snížení při současném uvážení, která opatření na snížení daného rizika budou vlastně přijata (Sadhra a Rampal, 1999).

5.2.12 Opatření k nepřijatelným zdrojům rizik

Pokud se analýzou a hodnocením rizik zjistí, že v objektu nebo zařízení existují zdroje rizik, které jsou v oblasti nepřijatelného rizika, popř. leží na hranici této oblasti, pak v dokumentu musí být uveden popis bezpečnostních opatření k eliminaci nepřijatelných zdrojů rizik, plán jejich realizace a systém kontroly plnění tohoto plánu. Stejný přístup se aplikuje v případě zjištění nedostatečnosti bezpečnostních a ochranných opatření.

Navržená opatření by měla být proveditelná a efektivní. Po navržení organizačních a technických opatření ke snížení rizika je třeba tato opatření podrobit dodatečné analýze za účelem zhodnocení jejich přínosu ke snížení daného rizika. Opatření pro prevenci závažných havárií a pro omezování a zmírňování jejich následků směřují zpravidla do následujících okruhů:

- Zvýšení spolehlivosti a zlepšení řídicího systému procesu včetně zavedení záložních systémů řízení a jejich monitoringu a systému pro rychlé odstavení operačních jednotek.
- Zavedení ochrany proti výpadkům energií, přístrojů bezpečných při poruše, zdvojování nejdůležitějších operačních jednotek a poplachových systémů včetně detekce plynů.
- Provedení stavebních úprav, jako je ochrana podpěr potrubí, ochrana kabelových lávek, zlepšení odolnosti zařízení proti korozi, umístění dalších čerpadel a ovládacích prvků.
- Zřízení havarijních jímek nebo sběrného zásobníku na uniklé látky, zařazení nouzových uzavíracích ventilů.
- Oddělení chemické, dešťové a splaškové kanalizace a zřízení akumulace pro zadržování a likvidace odpadní a hasební vody při likvidaci závažné havárie.
- Zavedení systémů protipožární ochrany a ochrany proti výbuchu, vyloučení zdrojů iniciace, dostatek hasicích přístrojů, použití bezpečné atmosféry, polní hořák, havarijní odvětrání včetně odrazných stěn pro svedení rázových vln výbuchů, odlehčení při výbuchu, výfukové konstrukce, dostatečná ventilace.

- Vybavení zařízeními pohlcujícími účinky havárií a k omezování velikosti havarijních úniků, absorpční soustavy, vodní rozprašovače a clony, drenáž, řešení pohyblivých spojení.
- Oddělené skladování nebezpečných látek podle vlastností, včetně stavby podzemních potrubí a zásobníků proti výbuchu.
- Zvláštní bezpečnostní opatření proti neoprávněným zásahům pro zabezpečení perimetru objektu nebo zařízení, a jiná opatření.

Obecně pro dané nakládání s nebezpečnou látkou mohou být vytvořeny různé typy ochranných či bezpečnostních bariér. Příklady těchto bariér jsou:

- Realizace vnitřně bezpečnějšího procesu a jeho účinná kontrola.
- Poplachové systémy a odezva lidského činitele.
- Aktivní ochranné prvky a automatická odezva na mimořádné stavy.
- Pasivní zařízení pro zadržení či směrování úniku, jako např. ochranné jímky, výfukové stěny, vodní stěny.
- Ochranné a zásahové prostředky v objektu nebo zařízení, jako např. požární jednotka.
- Ochranné a zásahové prostředky mimo objekt nebo zařízení.
- Při instalaci nebo opravách technických zařízení tvořících bezpečnostní bariéru je třeba dbát určitých zásad a postupů. Především se jedná o to, aby:
- Byla provedena kontrola správnosti zapojení a funkčnosti bezpečnostních zařízení.
- Byly použity vhodné hasební látky (podloženo na základě zkoušek).
- Byly použity postupy pro provádění instalace, revize a opravy (dle právních předpisů, pracovních postupů) v závislosti na oprávnění zaměstnanců provádět tyto práce vyžadující zvláštní odbornou způsobilost, oprávnění k provádění činnosti, proškolení nebo poučení údržbářů.
- Byla dostatečně kvalitní koordinace a komunikace mezi zaměstnanci specializovaných externích firem a vedoucími pracovníky majícími na starost daný úsek (seznámení s vnitřními předpisy firmy, která údržbu, revizi a opravu provádí, seznámení s procesem výroby a možnými riziky).

Při manipulaci s materiály, které mohou při přemisťování potrubím, skladování v sillech a nakládání vytvářet výbušnou atmosféru (zejm. obilí, mouka, cukr,...), je nutné instalovat požární bezpečnostní zařízení jako je:

- Detekce teploty – zařízení na její regulaci, teplotní čidla hlásící poruchu na zařízení k regulaci teploty (např. dříve nežli dojde k biologickému samozahřívání a následnému samovznícení).
- Kontrolní zařízení měřící pokles tlaku na ventilaci, odvětrání vlhkosti na odprašovacích zařízeních instalace zařízení k potlačení výbuchu, zejména v sušárnách a celém prostoru skladů a pásových dopravníků instalace stabilního hasicího zařízení.
- Detekce kovových částí (cizích těles) v přepravovaném materiálu (možná iniciace při kov na kov při manipulaci, potrubní dopravě pod tlakem, na pásových dopravnících, ucpání výsypek, atd.).

Během kontroly potrubí je žádoucí provádět i kontrolu stavu vnitřních stěn potrubí, reaktorů (kolon) a nádob, kde může docházet k reakcím s nánosy v potrubí (např. zkorodovaná vrstva, pevné částice vzniklé usazováním po řadu let atd.) – vytváření výbušných směsí, které mohou mít i nízkou iniciační energii, což může mít za následek výbuch a roztržení daného zařízení, popř. poškození celé technologie nebo dokonce devastaci celého objektu/podniku. Dalším problémem, ze kterého mohou nastat nepředvídatelné situace, je nedostatečné zaznamenávání a hlášení poruch na zařízení, ke kterým došlo v minulosti, to může vést až ke změnám na struktuře konstrukce např. zásobníku nebo potrubí.

Při výpadku elektrického proudu je v chemickém průmyslu nutné zajistit alespoň nouzový režim (napájení ze dvou nezávislých elektrických sítí), při kterém dochází ke stabilizaci výrobního procesu do stavu, ve kterém nehrozí žádná mimořádná situace. Například se musí neustále dochlazovat probíhající reakce (nesmí dojít k podcenění reakčního tepla), v těchto případech musí být ohřívací zařízení vyřazeno z provozu, ale v některých musí být ohřívací zařízení zapnuto, aby nedošlo k utuhnutí látky a ucpání technologie.

Pokud již k mimořádné situaci dojde anebo jí již nelze zabránit, postupuje se dle předepsaných postupů a dochází k provedení prvotních opatření vedoucích ke snížování následků (např. únik nebezpečné chemické látky do ovzduší – chlór – zkrápění vodní clonou, do doby než dojde k izolování úniku). V souladu s tímto souvisí i stanovení v rámci předpisů limitních hodnot koncentrace látek v povrchových i podzemních vodách, pro přesné určení chemické výroby, ze které pochází, a také stanovení nápravných opatření. Klíčové je, aby:

- Během provozu popř. před spuštěním provozu po odstávce a během odstávky, byla zajištěna funkčnost všech pojistných ventilů, detektorů teploty, nárůstu a poklesu tlaku, detekce přeplnění v návaznosti na regulaci přívodu, detekce koncentrace výbušné směsi,...
- Byly na základě kontroly množství látky na vstupu potrubí a na jeho výstupu odhaleny netěsnosti potrubí.

- Byla zajištěna funkčnost všech bezpečnostních opatření v případě úniku nebezpečných chemických látek a chemických přípravků (př. vodní clona k neutralizaci oblaku,...).
- Při odstavování nebo uzavírání potrubí byla dodržena určitá pravidla, dle druhu látky: sledování průběhu teploty, zamezit přísunu vlhkosti, odplynění do zásobníku k tomu určenému popř. uzavření potrubí i s plynem, ale ve zředěném stavu s plynem inertním (dusík),...
- Bylo zajištěno provádění pravidelné údržby na reaktoru chladicího zařízení a zajištění dvou nezávislých zdrojů chladicí vody, pro ochlazování probíhající reakce.
- Byl zajištěn náhradní zdroj energie během výpadku elektrického proudu způsobeného zkratem, požárem, atd.
- Byly prováděny pravidelné kontroly generátoru, preventivní údržba ochranných zařízení a ústředí, provádění pravidelných revizí a technických kontrol elektrických a s ním souvisejících zařízení, proškolení osob.
- Bylo zajištěno srozumitelné navádění na napojení jednotlivých čerpadel a odvzdušňovacích ventilů při přečerpávání látek, popř. proškolení a výcvik osob.
- Byly neustále zlepšovány znalosti zaměstnanců v oblasti výcviku a připravenosti na mimořádné situace, uplatňování a nacvičování částí havarijního plánu.
- Každá mimořádná situace vedoucí k mimořádné události byla důkladně analyzována za účelem předcházení nehod.

Při přepravě chemických látek potrubím je vhodné dbát určitých zásad již během navrhování a konstruování potrubních tras. Je třeba, aby jednotlivá spojení přírub byla dostatečná (kontrola kvality svarů), a aby nedocházelo k jejich namáhání a možnému následnému prasknutí. Při potrubním nadzemním/podzemním vedení je třeba zpracovat odhad znečištění v případě úniku chemické látky a možné následky, které tímto mohou být způsobeny, dále pak postupy a opatření vedoucí k zamezení šíření uniklé látky a ke snížení následků zejména na zdraví osob a životní prostředí. Při úniku nebezpečné látky ať už během přečerpávání, nebo potrubní dopravy, se ve většině případů zajišťuje rychlá aplikace vnitřního havarijního plánu, s tím související rozmístění potřebných prostředků k likvidaci vzniklé havárie (vodní clony, čerpadla,...) a zajištění zvukového varování zaměstnanců podniku, popř. zajištění informovanosti okolních zařízení a obyvatel v blízké oblasti (v rámci havarijního plánu města – obce) včetně následných pokynů a opatření.

Bezpečné vzdálenosti

V souvislosti s podmíněčně přijatelnými nebo nepřijatelnými zdroji rizik se často setkáváme s tzv. **bezpečnou vzdáleností**. Tu lze charakterizovat jako nejmenší vzdálenost, která vymezuje bezpečný prostor od prostoru nebezpečného. Pro pochopení tohoto pojmu je nutné ale vymezit nejprve pojmy bezpečný a nebezpečný prostor, což lze provést aproximací k individuálnímu riziku, kde se se zvyšující vzdáleností riziko pro jednotlivce postupně zmenšuje, až dojde k hodnotě přijatelné (z hlediska používaných kritérií, nikoli z hlediska tolerování, resp. akceptování rizika). Jelikož má bezpečná vzdálenost určovat vzdálenost od zdroje rizika, kde je již pravděpodobnost vzniku nežádoucího následku tak nízká, že riziko je již přijatelné, lze ji chápat jako určitou bariéru vymezenou volným prostorem. Tam, kde je zdroj rizika izolován od okolního prostoru (například chemický reaktor je umístěn v hale, která má výbuchu odolnou konstrukci a je hermeticky uzavřená), lze za bezpečnou vzdálenost považovat vzdálenost mezi zařízením a vnější stranou stěny budovy. Bezpečná vzdálenost je zde totiž zajištěna stavební bariérou, která znemožňuje vznik zranění lidí způsobného emisí toxické látky do vnějšího prostředí, tlakovou vlnou, tepelnou radiací nebo letícími fragmenty. V takových případech samozřejmě pozbývá pojem bezpečná vzdálenost svého smyslu. Ovšem tento příklad byl jen ilustrativní a v praxi se s ním téměř nesetkáme. V průmyslu je na volném prostranství umístěno velké množství zařízení obsahujících nebezpečnou látku (např. zásobníky, potrubí, otevřené sklady, jímky apod.), z nichž může docházet k úniku nebezpečných látek do prostředí. V takovém případě pak je stanovení bezpečné vzdálenosti velmi žádoucí, zvláště pak s ohledem k informování veřejnosti. Bezpečná vzdálenost, která by měla být určena odbornými výpočty, musí definovat minimální vzdálenost, která s ohledem na modelový výpočet i zkušenosti z praxe zaručuje, že zde již nežádoucí následky nedosáhnou⁴⁷.

Britská HSE vydala doporučení, ve kterém stanovila dosahy tří zón vyjadřujících různou úroveň ohrožení (rizika) pro nejnebezpečnější zdroj rizika (s ohledem na pravděpodobnost vzniku mimořádné události), kterým je zásobník s LPG. V poslední době jsme svědky toho, že malé zásobníky s LPG se stále častěji objevují nejen v průmyslu nebo na čerpacích stanicích, ale také na zahrádkách rodinných domů. S přihlédnutím k možnému ohrožení dosahy nežádoucích následků, byly příslušné vzdálenosti pro zásobníky s různým množstvím LPG odhadnuty takto (viz tabulka 45):

47 Něco jiného je to v případě zaměstnanců pracujících s daným zdrojem rizika, kteří musí při práci dodržovat přísná bezpečnostní pravidla (se kterými byli seznámeni), jež jsou postavena na předpokladu, že ačkoli se pracovníci pohybují v zóně zraňujících (často i fatálních) následků, je při dodržení všech bezpečnostních opatření míra rizika, kterému jsou zde vystaveni, pro ně akceptovatelná. Bezpečná vzdálenost je pak vzdálenost od zdroje rizika, kde ještě nemůže jejich činností a při dodržení všech pravidel bezpečné práce dojít ke zranění (např. se může jednat o maximální dosahy nebezpečných koncentrací dané látky v ovzduší – např. dolní mez výbuchu, LOAEL apod. – vznikající při běžných pracovních operacích nebo fugitivními emisemi).

Tabulka 45: Dosahy zón ohrožení pro zásobníky s LPG (Lees, 1996).

Zóna	Vzdálenosti zón ohrožení						
	Množství LPG v zásobníku (v tunách)						
	6–10	11–15	16–25	26–40	41–80	81–120	121–300
Zóna bezvýznamného rizika	150 m	175 m	250 m	300 m	400 m	500 m	600 m
Zóna mírného rizika	125 m	150 m	200 m	250 m	300 m	400 m	500 m
Zóna vysokého rizika	50 m	50 m	50 m	75 m	100 m	125 m	150 m

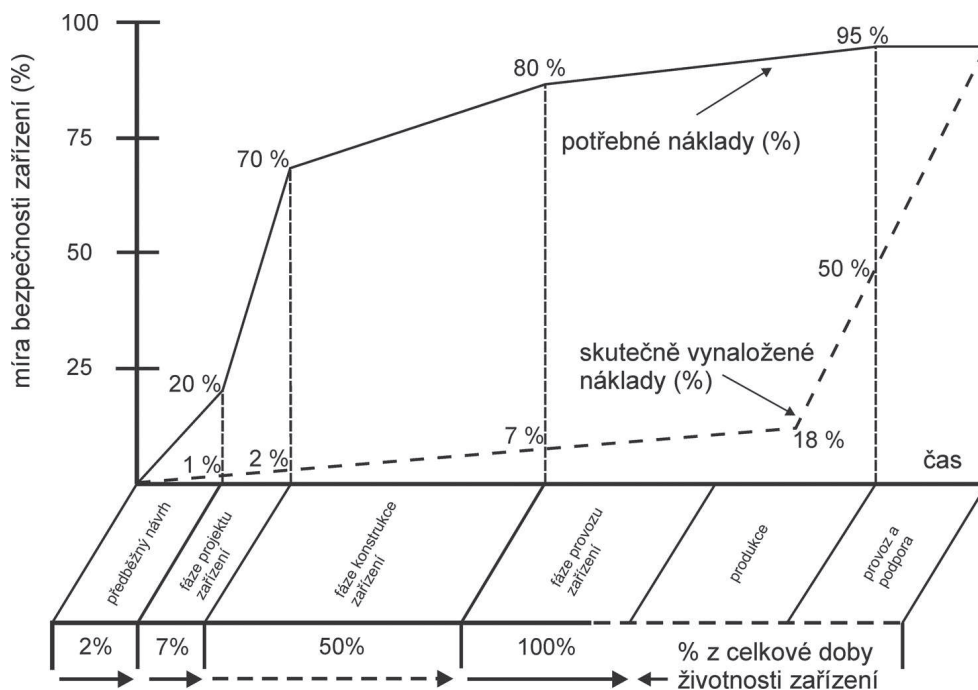
Zónu bezvýznamného rizika lze charakterizovat tak, že zde je hodnota rizika již blízká hodnotě „pozařadového“ rizika (cca 10^{-6} rok⁻¹), takže nežádoucí následky v případě mimořádné události spojené s unikem látky z daného zařízení, zde nelze očekávat. Tato vzdálenost je tedy zcela bezpečná. V zóně mírného rizika již ale možnost zraňujících dosahů při nejhorším možném scénáři události je nutné uvažovat, avšak pravděpodobnost takovéto mimořádné události je velmi malá. Individuální riziko se v této vzdálenosti pohybuje okolo hodnoty kritéria přijatelnosti, a pokud má část veřejnosti z existence tohoto zdroje rizik nějaký profit, pak lze toto riziko považovat za akceptovatelné. Zóna vysokého rizika je pak oblastí, kde je již pravděpodobnost dosahu zranitelných následků i při nejpravděpodobnějším scénáři velmi vysoká (obvykle dochází k malým únikům, ale nepoměrně častěji než v případě úniku veškerého množství zádrže). Pakliže je toto riziko dobře řízeno (z hlediska posouzení přijatelnosti spadá do kategorie podmíněně přijatelného), může být pro veřejnost ještě tolerovatelné, nicméně akceptovatelné je již jen pro ty jedince, kteří mají z existence daného zdroje rizik bezprostřední profit (např. zaměstnanci továrny, kde je zásobník provozován, majitel rodinného domku, který topí LPG ze svého zásobníku apod.).

Investice do vývoje nových zařízení, jejich zavádění a obsluhy

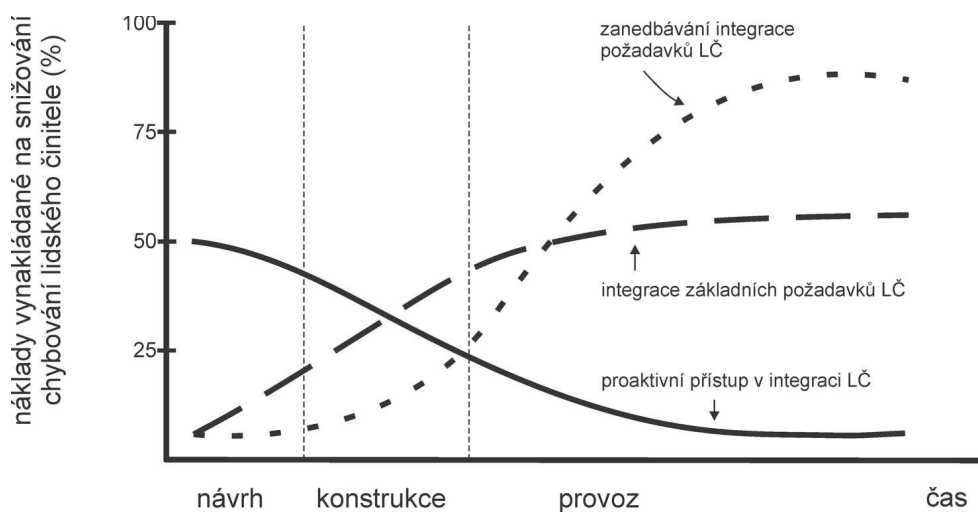
Prevence rizik samozřejmě není jen o investicích do údržby či do inovací stávajícího stavu, ale spočívá také v nahrazování „nebezpečných“ procesů a zařízení novými, méně nebezpečnými. Také sem spadá oblast lidského činitele, tedy péče o zaměstnance, zvyšování kvalifikace, dovedností, schopností správně reagovat při mimořádných událostech, správné komunikace apod. European Organisation for the Safety of Air Navigation zveřejnila v roce 1999 zajímavou studii, ve které byly vyjádřeny výpočty nákladů vynaložených na snižování rizika, které může zařízení při svém provozu představovat, během vybraných etap životního cyklu zařízení⁴⁸ (viz obrázek 118). V tomto směru se rozlišují tyto životní etapy zařízení:

- Myšlenkový koncept.
- Předběžný návrh projektu.

⁴⁸ Životním cyklem zařízení rozumíme časové údobí, které začíná už vážnou myšlenkou o daném zařízení a končí jeho likvidací.



Obrázek 118: Vypočítané náklady vynaložené na snižování rizik během životního cyklu zařízení (European Organisation for the Safety of Air Navigation, 1999).



Obrázek 119: Hodnocení nákladů nutných pro snižování chybování lidského činitele během jednotlivých životních fází zařízení (European Organisation for the Safety of Air Navigation, 1999).

- Tvorba projektu.
- Finalizace projektu, zapracování úprav a schválení konečné podoby projektu.
- Výroba zařízení.
- Najíždění zařízení.
- Provoz a údržba zařízení.
- Odstavení a likvidace.

Z uvedeného obrázku 118 vyplývá, že nejvíce lze bezpečnost a spolehlivost zařízení ovlivnit během fáze předběžného návrhu (až z 50 %), a to i přes to, že tato etapa trvá jen 7 % celkového času věnovaného návrhu zařízení. Naproti tomu během fáze konstrukce lze odstranit pouze zlomek nedostatků, které během svého provozu zařízení má (asi jen 10 %), a během fáze provozu pak již jen méně než 5 %. Je tedy zjevné, že klíčové je údobí, kdy se podoba zařízení teprve „rodí na papíře“. Obrázek 118 ukazuje ještě jednu zajímavou skutečnost – náklady, jaké jsou v praxi skutečně vynakládány. Ty ukazuje čárkovaná křivka a je vidět, že ve skutečnosti si mnoho konstruktérů a provozovatelů zařízení neuvědomuje důležitost fáze návrhu a nejvíce se zaměřují na fázi konstrukce zařízení a jeho uvádění do provozu. Zbytečně tak vynakládají prostředky, které ale již nejsou účelně vynaložené s ohledem na reálný přínos ve smyslu snížení rizika.

Podobně je tomu i v případě lidského činitele. Pakliže se již k fázi návrhu a konstrukce zařízení proaktivně přistupuje také s ohledem na lidského činitele (např. obsluha zařízení je průběžně seznamována s vývojem zařízení, provozní inženýři uplatňují své připomínky podložené zkušenostmi z praxe a potřebami provozovatele apod.), je možné ve finále docílit vyššího stupně bezpečnosti provozu a také snížit náklady vznikající například odstávkami, drahým školením personálu, dodatečnými technickými úpravami apod. Takový přístup se nazývá proaktivní a jeho trend v obrázku 119 znázorňuje plná čára. Naproti tomu pasivní přístup, podcenění role člověka již při fázi návrhu, pak vede ke zbytečně vysokým nákladům spojených s lidským činitelem, které s sebou nese samotný provoz zařízení (viz čárkovaná křivka).

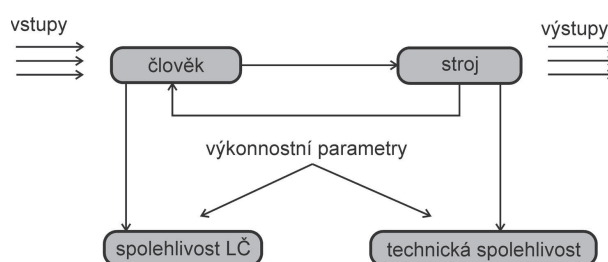
5.3 Vliv lidského činitele na průmyslovou bezpečnost

Lidský činitel je souhrn lidských vlastností a schopností, které mají v dané situaci vliv na výkonnost, efektivnost a spolehlivost pracovního systému a jsou hodnoceny z psychologického, fyziologického a fyzického hlediska. Tuto definici je třeba doplnit o zásadní poznatek. Většinou je o pojmu lidský činitel, či lidský faktor (tyto termíny jsou totožné, přeloženo z angličtiny z výrazu „human factor“), hovořeno v negativním smyslu. Nutno dodat, že vliv lidského činitele může být často velmi pozitivní. Situace, která není řešitelná pomocí počítače nebo stroje, může být „zachráněna“ člověkem. Je to způsobeno schopností lidského mozku jít přes předem vyhrazené hranice myšlenkových vzorců (programů), kterými je řízen stroj. Jinými slovy, člo-

věk je schopen kreativně myslet a flexibilně reagovat na situace kolem sebe. Ve stejné situaci se člověk nechová vždy stejným způsobem a stejný úkol může být vykonán různým způsobem, aniž by přitom byla snížena spolehlivost systému. Toto s sebou samozřejmě nese riziko, že jeho akce bude provedena chybně. Pod pojmem lidský činitel je třeba integrovat jak samotného člověka, tak i úroveň podnikové kultury, kultury bezpečnosti a celospolečenské kultury.

5.3.1 Systém člověk–stroj

Systémem člověk–stroj rozumíme soustavu, kterou tvoří pracovník (pracovní skupiny) a pracovní prostředky (stroje, technická zařízení) včetně pracovního předmětu, v níž jsou určitým způsobem rozděleny funkce mezi lidské a technické komponenty, jejíž cíl je přesně vymezen a realizuje se v daném pracovním prostředí (viz obrázek 120). Stroj v tomto případě představuje pracovní prostředek obecně, počínaje jednoduchým nástrojem či nářadím přes jedno či víceúčelový stroj, technické zařízení až po řídicí centrum.



Obrázek 120: Schéma systému člověk–stroj.

Mezi spolehlivostí stroje a spolehlivostí lidského činitele jsou identifikovány základní rozdíly především ve způsobu zpracování informací a ve způsobu dosažení cíle. Všechn hardware, kterým je uskutečněna interakce mezi člověkem a strojem, je nazýván interface. V české terminologii jej často označujeme jako sdělovače a ovládače (např. železniční návěstí, ukazatel měřicího přístroje, telefon, displej, siréna, ovládací panely, klávesnice, počítačová myš, zakončení nástrojů, atd.).

Mezi člověkem a hardwarem by mělo docházet neustále k oboustranné výměně informací. Poslední dobou je řešena otázka priority rozhodování (Havlíková, 2008, online). Jak již bylo uvedeno, člověk se při rozhodování neřídí předem stanovenými pravidly, na rozdíl od stroje. Jelikož je člověk kreativní prvek pracovního systému, při interakci člověka a stroje je používána pro něj specifická vlastnost a tou je myšlení a schopnost učit se novým věcem, získávat zkušenosti a dovednost poučit se z nezdaru. U stroje je vždy předem známo, jak bude jednat, což může mnohdy být, na rozdíl od člověka, i nesporná výhoda.

Výkonem dnešní výpočetní techniky jsou mnohonásobně překročeny možnosti lidského mozku v otázce rychlosti výpočtu a kapacity paměti. Otázkou, kterou je nutno se zabývat, například při návrhu řídicího systému v průmyslu, je, kdo má mít vyšší prioritu v rozhodování. Další pozitivní vlastností stroje je skutečnost, že jeho výkon není na rozdíl od výkonu člověka ovlivněn únavou. Činnost stroje totiž probíhá podle stále stejného předdefinovaného algoritmu. Každá jeho takto provedená operace je tudíž identická, a je-li algoritmus navržen správně, je vznik chyby téměř vyloučen. Je zřejmé, že této kvalitě se mentální výkon člověka zdaleka nevyrovná (Trpiš, 2009).

5.3.2 Spolehlivost lidského činitele

Termín spolehlivost lidského činitele je obvykle definován jako pravděpodobnost, že člověk bude správně provádět určitou činnost požadovanou systémem během časového úseku (pokud je čas omezujícím faktorem) bez konání jakékoliv vedlejší aktivity, která by vedla k poškození systému (Hollnagel, 2006b). Jedná se tedy o kvalitativní vlastnost lidského operátora, jež je specifická každému jedinci, a která je přímo závislá na jeho výkonových parametrech (fyzický stav, mentální úroveň, psychická odolnost apod.).

Spolehlivost lidského činitele není jednoduché stanovit, natož předpovědět. Důvodem je, že se nejedná o izolovaný krok nebo jednorázové rozhodnutí, ale o soubor různých vlivů, příčin a faktorů, kterými je tato vlastnost člověka utvářena. Zkoumání spolehlivosti lidského činitele je jeden z nejdůležitějších úkolů u pravděpodobnostního odhadu rizika (Probabilistic Risk Assessment – PRA⁴⁹) (Havlíková, 2009).

PRA je rozsáhlá, strukturovaná a logická analytická metoda, která je určena k identifikaci a odhadu rizika v komplexním technologickém systému (Foote, 2003). Jejím smyslem je nejen vyjádřit riziko v numerické hodnotě, ale díky jednoznačným kvantitativním údajům umožňuje přijímat rozhodnutí, zda navržená opatření (která vedou ke snížení míry rizika), jsou z hlediska finanční náročnosti efektivní. Tvrdé údaje tak dobře poslouží pro Cost-Benefit analýzu jakožto jednoznačný objektivní parametr (Skřehot, 2008b).

Lidský činitel a mimořádné události

V praxi se často stává, že vyšetřování vzniku průmyslové havárie je zakončeno hlášením, že „došlo k lidské chybě“, avšak není uvedena příčina jejího vzniku (Skřehot, 2008a). Je třeba se zaměřit na nalezení tzv. kořenových příčin, tedy příčin, které byly spouštěčem nehodového děje.

Problematika lidského činitele je značně obsáhlá. V této oblasti bylo v posledních letech dosaženo značného pokroku. Zatímco byly propracovány metody a postupy, jak s lidským činitelem pracovat, oblast lidské psychiky není doposud v tomto směru

49 Podobně je to u pravděpodobnostních analýz bezpečnosti PSA (Probabilistic Safety Assessment).

příliš prozkoumána. Další věcí, která je hodně diskutována, je nedostatečná kvalita a srozumitelnost výstupů prováděných analýz spolehlivosti lidského činitele. Jde například o dokumentaci k prevenci závažných havárií. Proto je v tomto směru v poslední době zvyšován tlak na zkvalitnění těchto dokumentů, což s sebou nese i stále sílící požadavek na aplikaci filozofie chybových módů, analýz úkolů či kvantitativní analýzy.

Lidský činitel se podle některých zdrojů (Ministerstvo životního prostředí, 2007) rozhodujícím způsobem podílí na vzniku závažných havárií. V mnoha případech to je právě lidský činitel, kterým byla daná nehoda způsobena. Jindy zase chybou lidského činitele daná nehoda eskaluje. Vyšetřování příčin vzniku nehod je v 80 % případů zakončeno zjištěním, že jejich vznik byl ovlivněn lidským činitelem (Skřehot a Malčíková, 2008). Při pohledu na celou věc jako na proces, tedy od samotného návrhu, technologického zpracování až po užívání dané průmyslové technologie, pak lidský činitel může až v 95 % případů za vznik nehody. Zbývajících 5 %, kdy se nejedná o chybu lidského činitele je možno zařadit do tzv. „zásahů vyšší moci“. Čím více je rozšířena množina možných vlivů lidského činitele, tím z větší míry se bude na výsledné pravděpodobnosti vzniku nehody podílet. Je zapotřebí předem stanovit pravidla, podle kterých se určí, zda se jedná o lidskou chybu anebo ne. Například selhání stroje může být zařazeno do technických příčin vzniku nehody, ale tento stroj byl navrhnut a vyroben člověkem, takže stejně tak může být na něj nahlíženo jakožto na produkt lidské chyby vzniklé v minulosti.

Historické souvislosti vývoje postojů k lidskému činiteli

Problematika lidského činitele, tj. interakce člověka se strojem a pracovním prostředím, je stále více chápána jako oblast s rozhodujícím vlivem na bezpečnost provozu zařízení a technologií (Skřehot a Malčíková, 2008). Vzhledem k ničivému potenciálu byla problematika lidského činitele v rovině a kontextech, jak je známe dnes, nejprve řešena v provozech, kde se užívalo jaderných technologií.

Ovšem přístup k člověku jakožto pracovní jednotce byl z pohledu zvyšování spolehlivosti jeho výkonu aplikován již mnohem dříve. Důraz byl tehdy kladen zejména na rychlost a efektivitu provádění pracovních úkonů ovšem bez zohlednění omezení a individuálních potřeb člověka. Jednalo se například o optimalizaci pracovního režimu vojáků v 18. století, aby bylo docíleno rychlejších přesunů na válečné frontě a budování opevnění (generál Vauban), nebo racionalizaci dílčích pracovních operací při manuálních pracích s ohledem na čas potřebný k jejich provedení a kvalitu výsledného produktu (v tomto směru jsou proslulé pokusy prováděné Gilbrethem na počátku 20. století) (Skřehot, 2008b).

Ve Spojených státech amerických byly moderní analýzy spolehlivosti lidského činitele použity počátkem 50. let 20. století (Skřehot a Malčíková, 2008). Jednalo se zpočátku o kvalitativní metody, kterými měla být odhadnuta, respektive předpovězena lidská chyba. Tyto metody, ač jsou stále hojně používány, nejsou pro dnešní

dobu postačující. Základy exaktního přístupu byly položeny při odhadu chybování montérů v Sandia National Laboratory. Tyto analýzy se staly základem pro vývoj metody THERP, která patří mezi nejpoužívanější metody současnosti.

Další oblast, kde bylo zapotřebí věnovat se lidskému činiteli, byl chemický průmysl. V chemickém průmyslu je obsažena největší hrozba pro společnost hned po jaderném. Mnohdy stačí selhání jediného pracovníka, které může vyústit k velké havárii, jako tomu bylo například v indickém Bhópálu v roce 1984. Podle direktivy Seveso II, která u nás vešla v platnost zákonem č. 353/1999 Sb. (nyní nahrazen zákonem č. 59/2006 Sb.), musí mít podniky, ve kterých je nakládáno s nebezpečnými chemickými látkami, zpracováno „posouzení vlivu lidského činitele na objekt nebo zařízení v souvislosti s relevantními zdroji rizik“. Tato analýza, jejíž součástí je analýza spolehlivosti a chybování lidského činitele, je nedílnou součástí analýzy a hodnocení (technologických) rizik.

Ve druhé polovině 20. století byl pozorován zvýšený zájem o vyšetřování nehod a zejména pak o identifikaci jejich příčin. Bylo to hlavně díky množství nápadných nehod ve složitých průmyslových systémech. Znamějšší z těchto událostí je nehoda, kdy došlo ke zhroucení aktivní zóny v jaderné elektrárně Three Mile Island (1979), k explozi celého bloku č. 4 v jaderné elektrárně v Černobylu (1986), ale také exploze raketoplánu Challenger (1986) či četné problémy na orbitální stanici Mir (1998) (Hollnagel, 2006a). Všeobecně je uváděno, že 90 % nehod v jaderném průmyslu je zapříčiněno selháním lidského činitele (Kotek a Vohralíková, 2008).

5.3.3 Moderní přístup k lidské chybě

Zda je nehoda způsobena člověkem anebo systémem řízení, je více patrné na těchto dvou případech (Sharit, 2006). V prvním je pracovník, jenž musí vykonávat úkol v omezeném prostoru. Když se pokusí dosáhnout na nástroj, jeho předloktí neúmyslně aktivuje vypínač. Výsledkem toho je emise tepla. Vizuální zpětná vazba, pokud jde o spuštění, není možná kvůli nemotorné pozici pracovníka, kterou byl nucen zaujmout. Hmatové vjemy není možno zaznamenat kvůli opatřením, jimiž je přikázáno nosit ochranný oblek. Ačkoliv sluchová zpětná vazba nastala, tak není slyšitelná díky velkému hluku v okolním provozu. Zbytkové páry pocházející ze zřídka prováděné procedury během předešlé směny se vznítí a vyústí v explozi. Ve druhém případě je pracovník nucen se přizpůsobit nerealistickým požadavkům, které jsou sepsány v pracovních předpisech. Musí totiž splnit požadavky, které jsou neustále požadovány ve formě úkolů směny omezením na zdrojích a změnách v plánech výroby. Pracovníkem je tedy změněn výrobní postup tak, aby byly požadavky splněny. Managementem jsou tyto úpravy mlčky přehlíženy. Avšak v případě, kdy dojde k nepředpokládanému scénáři a úpravou pracovníka byla způsobena nehoda, dává rychle management „ruce pryč“. Odvolává se na to, že pracovníkovi nebude poskytnuta podpora z toho důvodu, že jeho jednání bylo v rozporu s pracovními předpisy (Trpiš, 2009).

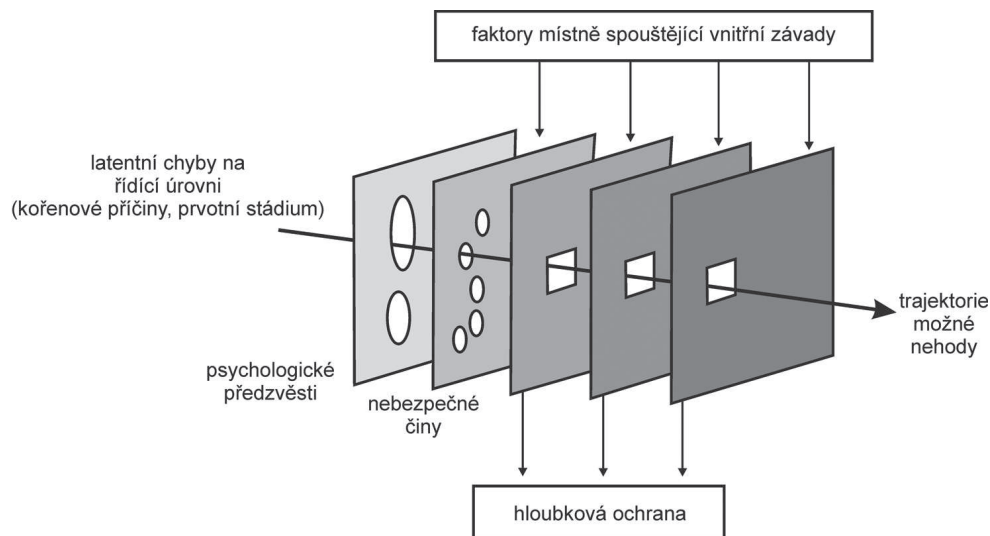
V prvním případě bylo jednání pracovníka, které vedlo k nehodě, neúmyslné, kdežto v druhém případě se jednalo o úmyslné, avšak vynucené jednání. V obou případech je rozporuplné, zda byla nehoda zaviněna pracovníkem. Jeden pohled je z pozice, kde je vina „přesunuta“ z pracovníka na management anebo designéra. Skrytými chybami managementu anebo designérů by byl pracovník zproštěn viny v obou těchto případech. Koneckonců pracovník konal svoji práci, jak nejlépe mohl a reagoval jen na změnu podmínek. Z druhého pohledu je za nehodu zodpovědný pracovník. Na základě znalostí z událostí (které mohou vyústit v nehodu), je vnější pozorovatel schopný vyvolat zpět sérii racionalizací a myšlenkových pochodů. Pokud jsou tato data správně zpracována a profiltrována, tak mohou být získány informace, které jsou klíčem, jak k dané nehodě došlo (Sharit, 2006). Zda k akcím (které vedly k chybě) došlo díky pohodlí pracovníka anebo jeho neschopnosti posoudit závažnost jeho akcí, není podstatné. Konečným výsledkem je vždy značné podcenění vlivu souvislostí. Jinými slovy pracovníkem byly vyhodnoceny jednotlivé kroky jeho činnosti a odceněn celkový význam všech jeho kroků dohromady.

V obou případech je dokonce oběma pracovníkům poskytnuta možnost zkoumat nebo zamyslet se nad jejich výkonem. Skutečností je, že v době, kdy se pochybení vyskytlo, byly pracovníkovi akce srozumitelné a ten je považoval za „rutinní práci“. Je nutno porozumět, jakým způsobem jsou posouzení a akce (z vnějšku se jevící jako chyby) ohodnoceny z vnitřku tak, že se jeví jako „rutinní práce“, která nestojí za pozornost.

Pohledy, u kterých je v podstatě odmítána lidská chyba (tedy alespoň ze strany pracovníka), jsou lákavé a v určité míře oprávněné. Avšak problémem není, zda by tyto pohledy měly být zamítnuty, ale zda by měly být naopak přijaty. Odmítnutím myšlenky, že chybu udělal pracovník, bude sice vzat relevantní ohled na základní lidské vlastnosti, avšak lidská chyba tak může být nebezpečně bagatelizována. Naopak je potřeba tomuto mechanismu porozumět, aby byly sníženy následky a výskyt lidských chyb (Sharit, 2006). Z tohoto pohledu mohou být chyby rozděleny na aktivní chyby (způsobené obsluhou) a skryté chyby (způsobené designem a managementem).

Aby došlo k nehodě vinou lidského činitele, je zapotřebí, aby byly překonány nejrůznější bariéry (viz obrázek 121). Pokud by se v těchto třech bariérách nevyskytovaly skryté chyby, tak by nedošlo k jejich překonání a tedy ani aktivní chybě a posléze nehodě (Reason, 1990). U některých klasifikací lidských chyb je rozlišeno mezi aktivní a skrytou chybou.

Není tedy vůbec jednoduché stanovit, kdy se přiklonit k variantě, že chyba byla způsobena opravdu člověkem, a kdy k ní byl donucen okolnostmi. Vyžaduje to mnoho zkušeností v daném oboru, aby byl posuzovatel schopen vyhodnotit, co se stalo, jak se to stalo a hlavně co je příčinou. Mnohdy mohou být obě možnosti považovány za správné a záleží na posuzovateli, jaká možnost jím bude zvolena.



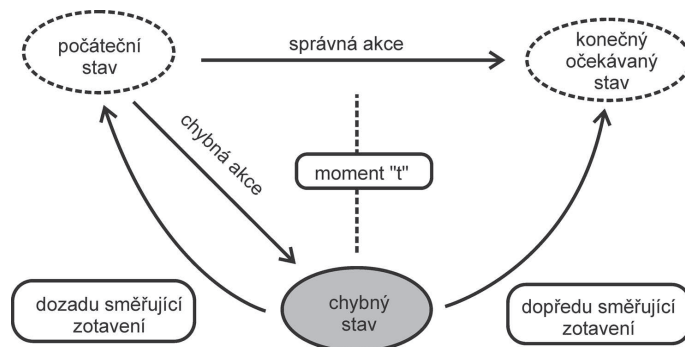
Obrázek 121: Reasonův bariérový model (Reason, 1990).

Zotavení po lidské chybě

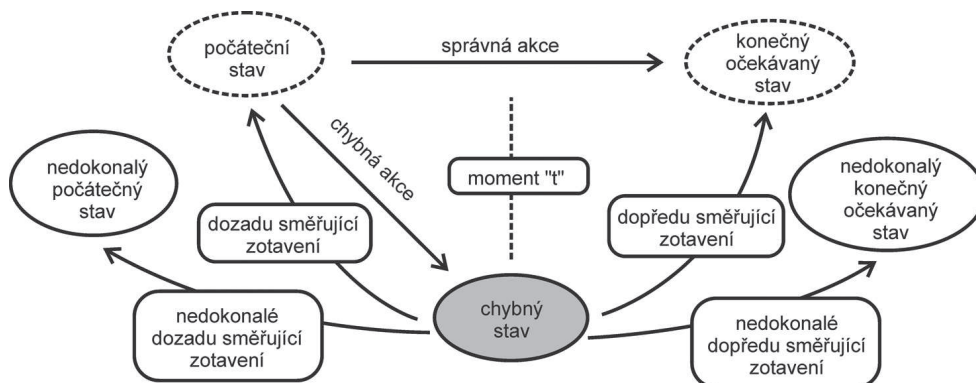
Lidské chybě může být zabráněno, než vznikne, tedy preventivními opatřeními, které by měly být zařazeny do samotného designu technologie, která bude využívána člověkem. Samozřejmě takto nelze úplně zabránit výskytu chyb, kde přichází na řadu represivní opatření, tedy zotavení po lidské chybě. Existuje několik různých druhů taxonomie zotavení po lidské chybě. Zde je popsána taxonomie podle Francise Jambona (Jambon, 1998). Předpokladem pro úspěšné zotavení je zaznamenání chyby. V některých případech dochází automaticky k zotavení funkcí systému, kterým je daná chyba zaznamenána a automaticky provedeny potřebné kroky k její nápravě. V případě, že tato funkce v systému pro danou chybu není zabudována, je třeba postupovat manuálně. Existují dva druhy zotavení, a to dopředu směřující a dozadu směřující. Proto, aby mohly být tyto pojmy vysvětleny, si je zapotřebí nejdříve definovat pojmy:

- Počáteční stav – stav systému před výskytem chyby.
- Konečný očekávaný stav – stav systému, který byl obsluhou očekáván na základě jejích akcí.
- Chybný stav – stav systému, který byl zapříčiněn lidskou chybou.

Dozadu směřující zotavení je tedy viděno jako pokus o obnovení systému do počátečního stavu poté, co byla zaznamenána lidská chyba. Oproti tomu všechny akce, kterými je dosažen konečný očekávaný stav, jsou považovány za dopředu směřující zotavení. V obou případech se jedná jak o jednoduché akce, tak o komplexní plánované akce (od výměny žárovky až po odstavení jaderné elektrárny). Na případě



Obrázek 122: Schéma zotavení systému (Jambon, 1998).



Obrázek 123: Reálné schéma zotavení systému (Jambon, 1998).

Lze poukázat na rozdíl mezi dopředu směřujícím a dozadu směřujícím zotavením. V případě výbuchu reaktoru jaderné elektrárny Černobyl bylo při stavbě sarkofágu provedeno dopředu směřující zotavení, jelikož nebylo možné systém uvést do počátečního stavu. Pokud dojde k prasknutí žárovky, tak je její výměna řazena mezi dozadu směřující zotavení, jelikož je v systému dosaženo počátečního stavu. Klíčovou roli v zotavení hraje čas. Pokud zotavení přijde příliš pozdě a dojde k nenapravitelné změně systému, jedná se o dopředu směřující zotavení. Je tak možno stanovit moment „t“. Než je tohoto momentu dosaženo, tak se jedná o dozadu směřující zotavení a po jeho překročení může být dosaženo pouze dopředu směřující zotavení (Trpiš, 2009). Model zotavení systému je znázorněn na obrázku 122.

V reálném světě však nemusí být dosaženo ideálního zotavení. V případě, že je rozbit talíř, tak slepením jeho stěpů je dosaženo pouze nedokonalého zotavení. Tento fakt je obsažen na obrázku 123.

Přístup na problematiku zotavení, který je zde popsán, je inženýrským pohledem. Nejsou zde zakomponovány žádné předpoklady z oblasti kognitivní psychologie. Dále je u tohoto přístupu počítáno, že člověk bude mít vždy za cíl, aby byl systém zotaven. Tento pohled je nicméně velice cenným nástrojem pro designéry, aby více porozuměli pohledu ze strany obsluhy systémů, které navrhují.

5.3.4 Příčiny selhání lidského činitele

Lidské selhání vzniká tehdy, když nastane situace, že požadavky na řešení úkolu jsou vyšší, než aktuální výkonnostní kapacity člověka (ať již mentální, tak i fyzické či duševní). Je odhadováno, že okolo 80 % úmrtí souvisejících s haváriemi je výsledek spíše vnitřních než vnějších příčin (Ferry, 1988). Proto téměř s každou nehodou je spojeno lidské pochybení v nejrůznějších podobách. Může se jednat o chyby managementu, špatně prováděné kontroly, nedostatečný výcvik a školení, anebo o individuální selhání pracovníků vzešlé z lajdáctví, podcenění situace nebo neschopnosti řešit danou situaci. Řadu těchto selhání lze ale odstranit nebo alespoň eliminovat.

Nejisté jednání

Jakmile se pracovník dopustí nejistého jednání, které vede až k nehodě, jedná se o lidské selhání. Ovšem, pokud budeme detailněji hodnotit příčiny této události, zjistíme, že se jedná jen o jednu z částí. Vždy je nutné se ptát, proč se lidé chovají nejistě?

Neznalost, paměť a motivace

Často slyšíme „já nevím“ nebo „nikdo mi nic neřekl“. Ovšem ne vždy platí, že tomu tak ve skutečnosti je. Přírozenou vlastností člověka je, že hledá nejjednodušší způsoby řešení, a to i tehdy, když si není jistý správností tohoto rozhodnutí. Pakliže lidé přistupují k tomuto způsobu řešení, lze jako příčiny hledat tyto: nedostatek znalostí plynoucí ze špatného výcviku, školení, nebo úrovně dokumentace a částečně také z dovedností (schopností) nebo způsobů jak práci dělat. Tyto nedostatky by ale měla odhalit dobře prováděná kontrola (Ferry, 1988).

Někteří lidé se dopouštějí nejistého jednání kvůli svým postojům. Negativně mohou postoje ovlivňovat tyto aspekty:

- Špatné pracovní návyky.
- Lhostejnost.
- Troufalost až opovážlivost.
- Lenost.

- Ukvapenost.
- Rozpoložení, nálada.
- Špatný příklad.
- Perfekcionismus.
- Nuda.
- Vědomé hazardování či záměrné poškozování.
- Nadřazené zájmy.
- Méněcennost, pocit podřízenosti.
- Paranoia.

S ohledem na situace, které mohou vést k nehodě, jsou lidé v pozici, že mohou mnohem snáze vykonat chybnou operaci, než stroj, který pracuje podle předepsaných podmínek. Když pak provede chybnou operaci stroj, výsledkem je často katastrofa. Ovšem konstatování, že stroj nepracuje tak, jak má, nebývá vždy na místě. Má-li stroj různé varianty řešení, nikdy se nerozhoduje svévolně, ale vždy podle zadání, které mu bylo uloženo člověkem – ať již konstruktéra, programátora nebo jeho obsluhy.

Při provádění většiny pracovních úkolů jsou lidé efektivnější při přerušované práci než stroje v přibližně 85 % efektivitu (výkonu). Některé typy chyb, které jsou příčinami nehod nebo se na nich podílejí, lze vyjádřit veličinou uváděnou pod zkratkou „BER“ (Basic Error Rates), což je počet lidských chyb na jeden milion provedených operací (Ferry, 1988). Hodnoty BER a HEP (Human Error Probability) pro vybrané chyby lidského činitele jsou uvedeny v tabulce 46.

Spolehlivost člověka je ovlivňována tolika hledisky, že je potřeba vědeckého studia vztahů mezi člověkem a jeho pracovním prostředím, aby bylo možné identifikovat

Tabulka 46: Vybrané typy lidských chyb vyskytujících se v procesním průmyslu a k nim příslušné hodnoty BER a HEP (Ferry, 1988).

Typ chyby	BER	HEP
Špatně přečtené instrukce	64500	$6,45 \cdot 10^{-2}$
Nesprávná montáž O-kroužků	66700	$6,67 \cdot 10^{-2}$
Špatné nastavení mechanického spojení	16700	$1,67 \cdot 10^{-2}$
Nedostatečně utažené ventily na potrubí	104	$1,04 \cdot 10^{-4}$
Špatně dotažené matice a šrouby	500	$5 \cdot 10^{-4}$
Špatně vyrobené ventily a klapky (např. nesprávné rozměry apod.)	2083	$2,083 \cdot 10^{-3}$
Opomenuté součástky ve spojení	1000	$1 \cdot 10^{-3}$

hlavní aspekty, které by mohly být důležité při vyšetřování nehod a odhalování jejich příčin. Hodnotit spolehlivost člověka kupříkladu z kvalifikačního hlediska je extrémně nesnadný a možná i nepraktický úkol. Chceme-li hodnotit spolehlivost člověka, pak je potřeba identifikovat vztahy mezi lidskými výkonovými charakteristikami a vnějšími faktory, které mohou spolehlivost člověka snižovat. Hlavní účel diskuze o spolehlivosti lidského činitele je demonstrovat, jak může být chybování člověka minimalizováno při daných podmínkách a designu. Pouze tento přístup umožní identifikovat slabá místa v systému již ve stadiu primárního vyšetřování nehod. Literatura uvádí, že spolehlivost člověka při výkonu jednoduchých činností se pohybuje v rozsahu 0,99995–0,99999 (tj. $HEP = 5 \cdot 10^{-5}$ až $1 \cdot 10^{-5}$) a pro náročné činnosti zahrnující zpracovávání množství vstupů, včetně jejich sběhu a komunikací s dalším operátorem, se pak tato hodnota snižuje na 0,97 až 0,99 (tj. $HEP = 3 \cdot 10^{-2}$ až 10^{-2}). Tyto hodnoty však úzce souvisejí se složitostí daného úkolu a také s pracovním prostředím, takže uváděná pravděpodobnost vzniku chyby je spíše orientační a v různých pracovních systémech se může řádově lišit. Spolehlivost lidského činitele může být snižována negativními vlivy pracovního prostředí, mezi které patří:

- Nedostatečný čas potřebný pro vykonání úkolu.
- Nevhodné mikroklimatické podmínky.
- Otřesy, nárazy, vibrace.
- Hluk.
- Nedostatečné nebo nevhodné osvětlení.
- Předepsaný oděv (často vede ke zhoršeným pocitům mikroklimatických podmínek).
- Nekompatibilní rozhraní a design zařízení.
- Náhlost změny vnějších podmínek (ať již mikroklimatických, tak i v tempu a režimu práce).
- Stres plynoucí z osamocení, izolací či vyloučení z kolektivu, anebo pramenícího z nedostatku spánku.
- Emocionální stres ze strachu, úzkosti či nudy.

5.3.5 Identifikace příčin selhání

Identifikace příčin selhání je jednou z nejobtížnějších partií posouzení vlivu lidského činitele na objekt nebo zařízení. Jedná se totiž o krok, ve kterém nejenže predikujeme něco, co se ještě nestalo (chyba), ale hledáme i faktory, jejichž působení k této chybě vedly (lépe řečeno mohou vést). V tomto pojetí hovoříme tedy o možných příčinách selhání lidského činitele, které se snažíme odhalit.

Většina literatury o lidských chybách bohužel neobjasňuje, že lidé činí chyby z různých důvodů a že činnost, kterou je třeba provést pro prevenci nebo redukci jednoho druhu chyb, nemusí být nejlepší způsob, jakým je třeba vypořádat se s jinými druhy chyb. Nejvýznamnější druhy lidských chyb a jejich obecných příčin lze podle Kletze shrnout následovně (Kletz, 1991):

- Chyby, kterým lze předejít lepším školením nebo pokyny – osoba, která se chyby dopustila, nevěděla, co má dělat. Tyto chyby se často nazývají chyby v důsledku špatného úmyslu (záměru).
- Chyby, kterým šlo předejít lepší motivací – osoba, která se chyby dopustila, věděla, co má dělat, ale neudělala to, protože se rozhodla to neudělat. Tyto chyby se občas nazývají přestupky, neboť osoba, která se přestupku dopustila, skutečně věděla, že porušení předpisů nebo obvyklé praxe není omluvitelné.
- Chyby způsobené nedostatkem fyzických nebo duševních schopností.
- Chyby způsobené snížením nebo krátkodobou ztrátou pozornosti. Úmysl (záměr) byl správný, ale nebyl proveden.

Obvykle se na vzniku výsledné chyby podílí více než jeden z těchto faktorů. Podrobnou analýzou lze jako nejčastější příčiny chybování proto odhalit zejména:

- Špatnou reflexi rizik u pracovníků obsluhy.
- Nedostatečnou kvalifikaci, trénovanost, osobnostní a zdravotní předpoklady personálu.
- Nevybavenost obsluhy zařízení a velínů jasnými a jednoznačnými instrukcemi pro výkon pracovních činností.
- Špatné systémy a výkon kontroly a řízení personálu.
- Nedostatečnou nebo nesprávnou informovanost obsluh.
- Nevhodné a nepříznivé pracovní podmínky a pracovní prostředí.
- Nesprávně, nebezpečně nebo neuspokojivě stanovené technologické, bezpečnostní a havarijní postupy.
- Nesoulad a spory mezi bezpečnostní a ekonomickou složkou provozovatele atd.

Je potřeba si uvědomit, že tento hrubý výčet je jen ilustrativní, nikoliv vyčerpávající a úplný. Identifikaci chyb a jejich analýzu provádí tým zkušených analytiků, kteří přiměřeným způsobem zohlední všechny možné relevantní vlivy, které mohou na příslušného pracovníka působit (před vznikem jeho selhání).

5.3.6 Základní rámec posouzení vlivu lidského činitele

Vliv lidského činitele se určuje na události a procesy, které mohou vést ke vzniku a rozvoji závažné havárie. Jedná se o možné iniciační události, přechodové jevy a řízené procesy, do kterých může lidský činitel přímo nebo nepřímo vstupovat, a to prostřednictvím výkonu kontroly nebo řízení objektu nebo zařízení, na kterých může ke vzniku uvažované závažné havárie dojít. Posouzení vlivu lidského činitele na systém (tj. na objekt nebo zařízení včetně příslušných rizik) by proto mělo zahrnovat:

- Analýzu vlivu lidského činitele na systém, včetně popisu činností provozní obsluhy, před vznikem potenciální iniciační události.
- Analýzu systému, včetně popisu činností provozní obsluhy, v případě vzniku iniciační události.
- Opatření pro eliminaci nebo omezení selhání (chybování) lidského činitele s možným následkem vzniku závažné havárie u identifikovaných kritických profesí při výkonu příslušných prací.

Posouzení vlivu lidského činitele na objekt nebo zařízení je komplexním materiálem, který přehledným způsobem zahrnuje posouzení spolehlivosti lidského činitele a chybování lidského činitele. Výše uvedený rámec pro vypracování posouzení vlivu lidského činitele na objekt nebo zařízení lze splnit prostřednictvím kvantitativní nebo kvalitativní analýzy. Současný přístup aplikovaný v České republice neklade takový důraz na kvantitativní hodnocení, jak je tomu v některých jiných členských státech EU, ale pokud bude kvantitativní hodnocení aplikováno, lze to jen přivítat. Za dané situace v ČR je upřednostňován především kvalitativní charakter posouzení vlivu lidského činitele, avšak s ohledem na vývoj v oblasti prevence závažných havárií dnes již nelze považovat za postačující pouze hrubý povrchní popis bez použití alespoň některé z uznávaných analytických metod. Pro praktickou potřebu jsou dále uvedeny možné metodické postupy vycházející z přístupů a postupů běžně využívaných například na pracovištích jaderných elektráren, řízení letového provozu nebo obdobných náročných činnostech operátorského charakteru (například Metodický pokyn odboru environmentálních rizik Ministerstva životního prostředí k rozsahu a způsobu zpracování dokumentu „Posouzení vlivu lidského činitele na objekt nebo zařízení v souvislosti s relevantními zdroji rizik“).

5.4 Funkční bezpečnost

Všechny výrobní procesy mohou obsahovat dílčí činnosti technologických uzlů, které je možné označit jako kritické s ohledem na nezanedbatelné riziko, které při provozu může vzniknout. Za současného stupně poznání mají technika a technologické postupy svá omezení, které významně ovlivňuje také člověk.

Přístupy k posilování bezpečnosti se průběžně zdokonalují. V prvních fázích vystačila modernější technika, ale postupně začaly být využívány moderní řídicí procesy a mikroprocesory. Výsledky praxe však ukázaly, že technika nevyřeší vše sama. Právě u běžných programovacích řídicích jednotek mohou vnitřní poruchy jednotek vést k nežádoucím projevům v celém systému. Především neurčitost chování komplexních systémů (včetně uživatelského software), obtížnost kontroly a nepřipravenost obsluhy vedly k požadavku na vytvoření verifikaci definovaných parametrů a praktického provozu (Prášek, 2009). Díky tomuto přirozenému technickému vývoji se zrodil nový podobor bezpečnostního inženýrství – **funkční bezpečnost**.

Zásadní obrat v přístupu ke koncepčnímu řešení bezpečnosti procesů přinesla norma IEC 61508 (transponovaná do normy EN 61508, resp. normy ČSN EN 61508), která řeší požadavky zabývat se bezpečností procesu od analýzy rizik již při návrhu systému, péči o něj v průběhu celého jeho životního cyklu až po ukončení provozu a demontáž. Tato norma, na kterou navazuje další významná norma EN 61511 (viz níže), nabízí model jednotlivých stupňů řízení bezpečnosti během doby života systému. Základem tohoto konceptu je pojetí funkční bezpečnosti jako nezávislé na spolehlivosti systému. Formulování samostatných požadavků na bezpečnost ji umožňuje posoudit nezávisle na funkčních schopnostech a tak poskytuje větší důvěru v bezpečnost za normálního i poruchového stavu zařízení nebo jeho řídicího systému. Paradoxem ovšem je, že bezpečnostní aktivity nelze vytrhnout z celkového kontextu, ale je třeba je posuzovat v souvislosti s ostatními částmi technologického zařízení, a to v celém jeho životním cyklu (Prášek, 2009).

5.4.1 Požadavky na funkční bezpečnost

Funkční bezpečnost představuje část celkové bezpečnosti týkající se pracovního procesu a základního řídicího systému procesů (BPCS), která závisí na správném fungování tzv. **bezpečnostního přístrojového systému** (SIS) a ostatních vrstev ochrany (ČSN EN 61511). Jak již bylo uvedeno výše, standardem, který zavádí prvky funkční bezpečnosti do praxe, je norma IEC 61511 – zejména pak v západní Evropě. Česká republika by však, coby členský stát Evropského společenství, rozhodně neměla zůstatvat pozadu. Za hlavní překážku lze u nás považovat skutečnost, že norma není právně závazná, neboť na ni neodkazuje žádný legislativní dokument, a proto je její implementace v průmyslu pomalá, ne-li žádná.

Norma samotná vychází ze starších norem řady DIN 19250 a příruček VDI Guideline 2180 a Namur Recommendation 31, které se zejména v Německu poměrně osvědčily. Jelikož tyto aplikace prokázaly vhodnost navržených přístupů, je standard IEC 61511 užitečným materiálem, který v sobě zahrnuje i problematiku spolehlivosti lidského činitele v rámci systému člověk–stroj.

Zmíněná norma používá jako základ model celkové bezpečnosti po celou dobu životnosti (pracovního) systému. Tento model obsahuje všechny činnosti, potřebné

pro zajištění toho, že bude dosažena požadovaná úroveň bezpečnosti pro zvažované systémy se vztahem k bezpečnosti. V rámci této normy je obsaženo poznání, že selhání systémů může být způsobeno buď selháním zařízení, nebo selháním člověka (Sadhra a Rampal, 1999).

Norma byla implementována do systému evropských norem a u nás jí odpovídá norma ČSN EN 61511, která má tři části:

- ČSN EN 61511-1: Požadavky na systémy hardwaru a softwaru, struktura, definice.
- ČSN EN 61511-2: Metodický pokyn pro používání ČSN EN 61511-1 (IEC 61511).
- ČSN EN 61511-3: Pokyn pro stanovení požadované úrovně integrity bezpečnosti.

V souvislosti se zaváděním prvků funkční bezpečnosti, bývají v praxi obvykle uplatňovány dva systémové přístupy, které lze s výhodou použít také pro hodnocení přístupu podniku k problematice lidského činitele. Jedná se o:

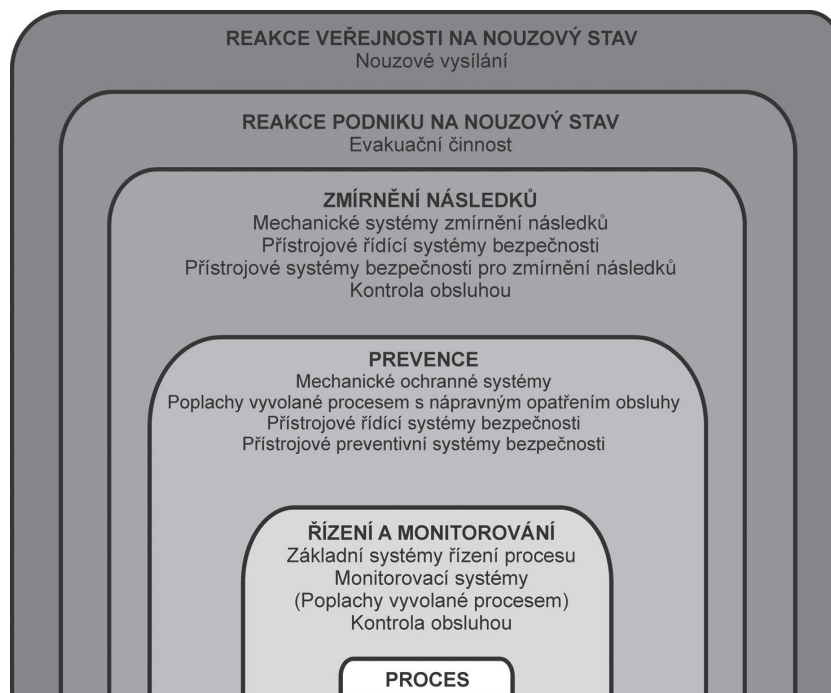
- přístup ochranné vrstvy a zohlednění úrovně automatizace (bezpečnostního systému) a
- zohlednění životního cyklu bezpečnostních systémů.

Na oba přístupy norma odkazuje a doporučuje jejich zavedení v systémové praxi. Přístup ochranné vrstvy rozlišuje stromy vrstev s různou bezpečnostně významnou funkcí operátorů a stručně se dá charakterizovat pomocí obrázku 124.

5.4.2 Ochranné vrstvy a bariéry

Systémy navrhované pro bezpečnostní účely nejsou žádnou novinkou. Již dlouho se používají jako součást bezpečnostních systémů v podmínkách průmyslové výroby tam, kde existuje nebezpečí újmy na zdraví či životech lidí nebo poškození životního prostředí. Tyto systémy a zařízení související s bezpečností, jsou nezávislé na běžném řídicím systému a v případě jeho nesprávné činnosti udržují technologický provoz v bezpečném stavu (Kosmowski, 2003). Hlavní součástí těchto systémů jsou ochranné vrstvy, které představují organizační, technická a systémová opatření (viz obrázek 124) a bariéry, které lze chápat jako dílčí prvky jednotlivých ochranných vrstev vytvořených pro potřebu maximální účinnosti funkce dané ochranné vrstvy.

Ochranná vrstva tedy představuje jakýkoli nezávislý mechanismus snižující riziko řízením, prevencí nebo zmírněním následků. Může zahrnovat různé bariéry v podobě výrobně-technologických opatření, jako například dostatečné velikosti nádob obsahujících nebezpečné chemické látky, konstrukční opatření, jako např. přetlakové



Obrázek 124: Schéma přístupu ochranné vrstvy (ČSN EN 61511).

ventily, bezpečnostní přístrojový systém nebo administrativní postup, jako je např. provozní řád či bezpečný pracovní postup, který slouží k zajištění bezpečné činnosti a snižuje tak riziko nežádoucího stavu (Drahten a Hermann, 2007). Reakce směřující ke snížení nebezpečí mohou být automatizované nebo spouštěné lidským zásahem.

Jelikož má člověk (operátor) v systému řízení bezpečnosti podniku aktivní funkci, je rozsah technické podpory závislý na vyhodnocení, nakolik reaguje operátor správně a jak vhodné je interface systému člověk–stroj, které jak kvalitu, tak především rychlost reakcí člověka za mimořádných stavů determinuje. Kromě toho se v tomto směru výrazně uplatňují také osobní dispozice operátora, tj. kvalita jeho fyzických a psychických vlastností. Proto je potřeba profesní úspěšnost operátora podrobit důkladné analýze a teprve po té je možno přistoupit k návrhu rozsahu a charakteru potřebných ochranných vrstev.

Podle IEC 61511 rozlišujeme tři vrstvy s různými bezpečnostně významnými funkcemi operátorů:

- Kontrolní a monitorovací systém (první – vnitřní – úroveň) – kontrola a monitoring zajišťují optimální podmínky procesu. Žádné selhání této vrstvy nepůsobí závažnou havárii. Jak se ukazuje, operátoři mají v rámci této vnitřní vrstvy dvě funkce:

- Řízení procesů – operátor může reagovat na základě svých dovedností anebo na základě informací získaných z výstrah kontrolního nebo monitorovacího systému, který zajišťuje optimalizaci procesu. Žádná taková chyba opět nemůže vést k závažné havárii.
- Dozor – operátor provádí za využití svých znalostí dohled nad procesem, to znamená, že upravuje za nestandardního stavu provozní podmínky za využití pouze drobných (anebo žádných) nástrojů či vybavení.
- Systém prevence (střední úroveň) – ČSN EN 61511 uvažuje málo automatizované a vysoce automatizované bezpečnostní systémy, v nichž je role operátora různá:
 - Operátor je součástí bezpečnostní funkce – tato situace nastává tehdy, jestliže je bezpečnostní systém podniku málo automatizovaný, tj. systém obsahuje pouze jednoduchý senzorový výstražný systém, takže přidruženou funkcí operátora je přenášet informaci získanou ze sdělovačů a zároveň ji vyhodnocovat a řešit.
 - Bezpečnostní systém je úplně automatizovaný – tato situace nastává tehdy, jestliže veškeré možné mimořádné provozní události jsou předem známy a předdefinovány do komplexních automatizovaných systémů včetně kompletního výstražného havarijního systému. V takovém případě vykonává operátor pouze funkci provozního dohledu.
- Systém zmírňování důsledků (třetí úroveň) – zde představuje operátor funkci supervizora, který zmírňuje nežádoucí následky procesu, bez jakýchkoli akčních nároků a potřeb, kromě případného zastavení provozu, jestliže k tomu nedojde automaticky.

5.4.3 Funkce lidského operátora

Lidský operátor je obecný pojem zahrnující vše, co se ve vztahu k řídicímu systému týká člověka. Pokrývá ergonomické aspekty systému, obsluhu systému a někdy i vedení (management). Říká se, že většina nehod je zaviněna alespoň z části člověkem. Proto je účelné brát při určování a při analýze rizika lidský činitel v úvahu. To se mnohdy neděje, a to ze dvou důvodů: za prvé se analýzy rizika tradičně zaměřují jen na poruchy zařízení a za druhé nejsou projektanti dostatečně obeznámeni se způsoby hodnocení spolehlivosti lidského činitele, resp. člověkem vykonávaných činností.

Ačkoliv se ČSN EN 61508 zmiňuje o lidském operátoru a doporučuje brát ho v úvahu, nenabízí žádný návod k tomu, co, jak nebo kdy v tomto směru udělat. Ve světle moderního pojetí spolehlivosti lidského činitele nemůže uspět argument, že nehody způsobené člověkem jsou zcela nepředvídatelné. Přesto jsme velmi často svědky, že v závěrech z vyšetřování nehod se otázka opomenutí na straně člověka, tedy selhání lidského faktoru, objevuje příliš často (Heinze, 2001). To norma ČSN

EN 61511 vyžaduje zaprvé změnu pohledu s ohledem na význam integrálního systémového přístupu, který rozšiřuje bezpečnostní požadavky pro jednotlivá zařízení (prostředky), tak i pro komplexní soubory zařízení (technologie, aparatury). Tyto požadavky jsou úzce vztaženy k vnějším podmínkám. Jedná se o tzv. model ochranných vrstev a model životního cyklu zařízení, jak již bylo zmíněno výše. Funkce interface mezi člověkem a strojem je úzce závislá na dokonalých znalostech lidských vlastností, co by senzorů, procesorů a činitelů, nikoli tedy pouze vlastností stroje jakožto hlavního akčního členu. Analýza nebezpečí a definice hrozby jsou v navrženém schématu postaveny v centru bezpečnostní pozornosti (výstrahy). Jiná norma, a to IEC 61508-1, požaduje, aby spolehlivost lidského činitele byla blíže hodnocena zvláště tehdy, jsou-li relevantní nebezpečí a nebezpečné situace určeny a hodnoceny v analýze rizik. V kontextu na přístup E/E/PE (elektrický/elektronický/programovatelný elektronický systém) představuje pojem bezpečnost systém zahrnující tři oblasti relevantních lidských chyb:

- Nežádoucí lidské činnosti anebo chyby při činnostech, které spouštějí funkci E/E/PE.
- Lidské chyby, jež aktivují výstražné systémy.
- Lidské chyby při testování nebo údržbě zařízení, které mohou redukovat efektivní funkci ochranného systému.

Důležitou okolností je, že tato norma vyžaduje kvantitativní vyjádření zbytkového rizika na základě výpočtu pravděpodobnosti chyby. Toto lze považovat za významný předěl v hodnocení spolehlivosti lidského činitele v systému člověk–stroj, které doposud bylo prováděno výlučně kvalitativními, kategorizačními technikami. Zmíněné hodnocení, které se provádí podle úrovně semikvantitativního prvku nazývaného **integrita bezpečnosti** (SIL), slouží jako důkaz efektivnosti provedených opatření.

Všeobecně se spolehlivost lidského činitele odhaduje na základě střední hodnoty pravděpodobnosti vzniku chyby (Human Error Probability – HEP). Literatura uvádí odhady této pravděpodobnosti ve výši 10^{-2} až 10^{-4} . Je nutno zdůraznit, že tyto hodnoty nejsou závislé na metodách hodnocení znalostí, úrovně a efektivitě výcviku, zvláštností podniku (či technologií) i operací pro provádění úkolů. Zmíněné hodnocení pochopitelně není absolutní a představuje pouze určitou aproximaci získanou na základě dosavadních zkušeností z provozní praxe. Absolutní vyjádření míry spolehlivosti, resp. nespolehlivosti lidského činitele, nemůže být nikdy přesně určeno (spočteno), na rozdíl od technických zařízení, u nichž lze posoudit objektivní prvky, jako např. materiálové vlastnosti konstrukcí, provozní podmínky apod., protože úroveň míry jeho spolehlivosti ovlivňuje řada faktorů, často nepostižitelných matematickými zákonitostmi (zejména jde-li o vlivy psychologické).

5.4.4 Počítačové systémy

Moderní chemický provoz se stává čím dál tím více složitější. Nové technologie umožňují jemnější řízení, a tudíž mnohem účinnější průběh procesů; také tyto nové technologie skýtají nové možnosti monitorování, určené pro zvýšení bezpečnosti. Důležitým faktorem těchto změn je zvýšené využití počítačů, jak pro řízení provozu, tak pro zajišťování bezpečnosti provozu. Počítač může monitorovat ohromné množství dat a tím dovoluje projektantům provozu realizovat postupy, které by pomocí konvenčních prostředků nebyly v praxi možné.

V chemickém provozu se počítače používají již po mnoho let a pomáhají operátorům řídit provoz tím, že jim podávají informace snadno pochopitelným způsobem. V některých případech se počítače používají pro automatické řízení procesů a bezpečně odpojí zařízení v případě havárie. V mnoha případech počítačové systémy mohou umožnit soustavnější kontrolu a řízení, než to bylo možné konvenčními metodami. To platí obzvláště pro chemickou výrobu po dávkách, kdy počítačové řízení umožňuje vyrábět mnohem konzistentnější výrobky a s menší pravděpodobností chyby operátora. V ostatních případech, jako je systém řízení hořáku, programovatelný elektronický systém (programmable electronic system – PES), obsahuje dodatečné funkce křížové kontroly, které by bylo obtížné zajistit konvenčními metodami.

Systémy se stávají složitější s hlavním řídicím systémem podporovaným v pozadí systémy pro optimalizaci, měřícími ústřednami se záznamem měřených údajů atd., které mohou navzájem propojovat velké množství separátních systémů a zařízení. Navíc, moderní komunikační systémy umožňují na dálku měnit řídicí proměnné či dokonce prvky programu, dokonce i z jiné země či kontinentu. Operátor se stává závislý na řídicím systému, může postrádat jakýkoli „cit“ pro řízení provozu v případě selhání počítačů.

Tato složitost jak provozu, tak i počítačových systémů přináší problémy, stejně jako i přínosy. Čím je provoz složitější, tím těžší je ujištění, že v systému nejsou žádné skryté konstrukční a projekční chyby, které se mohou za provozu projevit selháním a nehodou. Tento problém je zvláště akutní u počítačových programů, které mohou být nespolehlivé, jestliže programátor nepochopí zcela všechny aspekty řízeného procesu nebo jestliže chyba nastane při psaní programu. Některé softwarové chyby jsou zanedbatelné a je relativně snadné je odhalit. Ale i malé chyby mají potenciál způsobit vážné následky, a čím je software složitější, tím je větší pravděpodobnost chyb a je i obtížnější tyto chyby odhalit.

V jaderném průmyslu moderní softwarová praxe obsahuje formální matematické techniky, které někdy umožňují přísné prověření, že program se bude chovat podle zadání. Toto zadání musí však být samotné ve tvaru formálního matematického dokumentu a je zde vždy možnost, že toto zadání nepodchytí odpovídajícím způsobem všechna technická opatření pro bezpečnost provozu celého podniku. V současné době se tyto techniky v ostatních průmyslových odvětvích používají jen omezeně.

Obecně není prakticky možné odzkoušet počítačový program vyčerpávajícím způsobem na všechny možné různé vstupní signály, protože počet možných kombinací dosahuje obvykle astronomických hodnot. Docela slušnou úroveň spolehlivosti softwaru lze prokázat použitím vzorku těch vstupů, které jsou statisticky významné pro provozní použití, ale nedosahuje se tím úrovně, která je běžně dosahovaná u konvenčně technicky navržených systémů hardwaru, které jsou relativně jednodušší. Ze všech těchto důvodů je důležité stanovit meze, kam až je možné se u funkcí kritických pro bezpečnost spoléhat na počítačové programy. Mělo by se však zdůraznit, že tyto meze nevylučují použití počítačů pro bezpečnostní účely. V případě ochranného systému (např. primární počítačový systém se střední úrovní spolehlivosti – integrity bezpečnosti) lze zálohovat jednodušším, konvenčně navrženým (hardwired) sekundárním systémem, který zajistí potřebnou důvěru, že v případě potřeby nastane odpojení ohrožených provozů, zařízení.

Při analýze funkční bezpečnosti je dobré také zvážit možnost použití různých systémů pro snížení pravděpodobnosti společné příčiny selhání. Toho lze dosáhnout použitím různého hardwaru, různých operačních systémů a různých programovacích jazyků. Použití hardwired ochranných systémů (systémů na mechanickém principu) může maximalizovat diverzitu a v mnoha případech tyto systémy představují ekonomicky nejvýhodnější řešení. Potíž však může nastat, když se vyskytne byť drobná nekompatibilita použitých operačních systémů (ať již v rovině softwaru, tak i numerické – např. používání různých jednotek při výpočtech apod.). U kritických aplikací se doporučuje použít pro hodnocení spolehlivosti hardwaru analýzu pomocí stromu chyb. Tato analýza neodpoví na všechny otázky týkající se celkové spolehlivosti počítačového systému, ale může to často odhalit velmi důležité dílčí poznatky (Sadhra a Rampal, 1999).

5.4.5 Spolehlivost systému člověk–stroj

Hodnocení spolehlivosti systému člověk–stroj má za účel určit míru přijatelnosti rizika (například pomocí matice rizik), určit pravděpodobnost selhání ovládaného zařízení, definovat požadavky pro snížení rizika na přijatelnou úroveň a určit požadavky pro snížení rizika E/E/PE systému a ostatních technických zařízení nebo technologických částí, včetně rizik externích (Salvendy, 2006). Vyjádřit lze pochopitelně i pravděpodobnost vzniku lidské chyby, avšak tento přístup je velmi složitý a náročný, zejména pak z důvodu nedostatku generických dat.

Systémový pohled na lidskou činnost při řízení systémů odhalil, že lidské chyby mohou pramenit ze dvou hlavních důvodů: (1) z člověka samotného a povahy jeho psychických procesů a (2) podmínek, za kterých je činnost prováděna. Chybné akce vyplývající z povahy lidské psychiky pramení z vnitřních tendencí k provádění chyb. Člověk je svou povahou chybující tvor a tendence chybovat je jeho přirozenou vlastností. James Reason svým systémem GEMS (Generic Error Modelling System) naznačil obecnou povahu chyb, které se v podobě kiksů (slip), opomenutí (lapse)

a omylů (mistake) projevují v činnostech, založených na dovednostech, pravidlech a znalostech (skill-, rule-, knowledge-based).

Podmínky, za nichž je činnost vykonávána, mohou buď usnadňovat nebo naopak znesnadňovat činnost a tím přispívat k nižší nebo vyšší pravděpodobnosti projevu chybných úkonů. Jde o vnější okolnosti, za nichž je činnost prováděna. Tyto „podmínky“ bývají označovány jako faktory ovlivňující bezpečnost (PIFs – Performance Influencing Factors, resp. v jaderné energetice používané PSFs – Performance Shaping Factors).

5.4.6 Úroveň integrity bezpečnosti

Aby mohla být posouzena závažnost funkce operátora, co by jednoho z hlavních prvků systému člověk–stroj, je užitečné využít nějakou klasifikační škálu pro zhodnocení podmínek při interakci člověk–stroj. Toto hodnocení je důležité pro pochopení závislostí a nároků na operátora a pro následné definování potřeb pro snížení rizika vzniku chyby. Tento přístup je zvláště vhodný zejména pro aproximaci těchto aspektů vyskytujících se za extrémních podmínek, které nejsme schopni obvykle zcela věrohodně namodelovat nebo nacvičit. Zmíněné hodnocení je možné provést za pomoci určení prvku nazývaného **úroveň integrity bezpečnosti** (Safety Integrity Level – SIL). Ta se obecně definuje jako diskrétní úroveň (1 až 4) určená pro stanovení požadavků na integritu bezpečnosti bezpečnostních přístrojových funkcí, které mají být přiděleny do bezpečnostních přístrojových systémů (ČSN EN 61511).

Určení SIL je možno provést pomocí různých metod, které budou uvedeny dále. Účel, proč je nutné určovat úroveň integrity bezpečnosti je ten, že pomocí níže uvedené kategorizace lze určit cílovou střední hodnotu pravděpodobnosti poruchy na vyžádání⁵⁰ při obsluze daného zařízení/řídícího systému a četnost nebezpečných poruch při průběžném provozu⁵¹. Navržené hodnoty vycházejí ze zkušeností získaných z německého automobilového průmyslu. Nejvyšší úrovní integrity bezpečnosti je 4, nejnižší 1. Cílem je dosáhnout co nejvyšší úrovně SIL a tedy snížit pravděpodobnost vzniku poruchy na vyžádání, resp. četnost vzniku poruch bezpečnostní přístrojové funkce zařízení za normálního provozu.

Úroveň integrity bezpečnosti je číselně definována proto, aby mohlo být v praxi prováděno objektivní srovnání alternativních návrhů (při fázi návrhu zařízení) a řešení (při fázi provozu zařízení). Samozřejmě, že tento přístup neumožňuje posuzovat a vzájemně srovnávat všechna bezpečnostní zařízení/systémy. Je totiž známo, že při

⁵⁰ Porucha na vyžádání je taková porucha, která vzniká při provozním režimu „na vyžádání“, tj. tehdy, je-li zařízení trvale připraveno k činnosti, ale jehož aktivace/spuštění je provedeno pouze tehdy, je-li to nutné/vyžadují-li to okolnosti (provozní nebo havarijní stav). Tato aktivace může být provedena jak lidským zásahem, tak i automaticky při dosažení určitých kritických provozních parametrů.

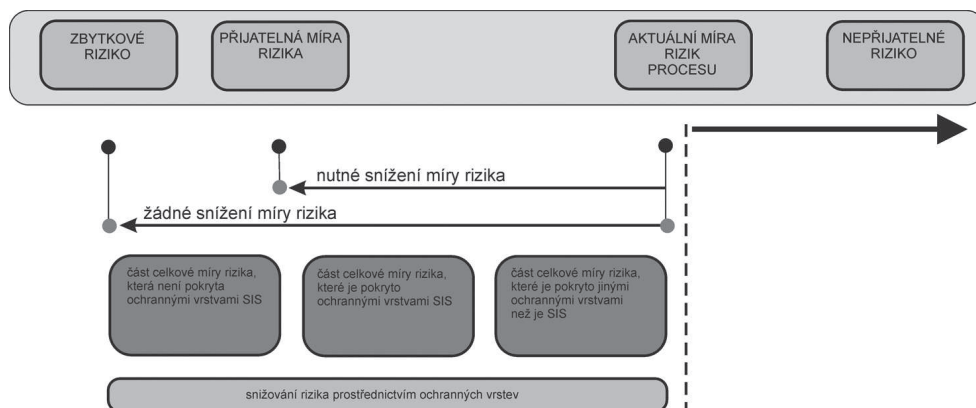
⁵¹ Nebezpečná porucha při průběžném režimu provozu je taková porucha při běžném provozu zařízení, která představuje potenciální nebezpečí pro systém jako celek, pakliže není provedena akce, která dalšímu rozvoji nežádoucí události zabrání.

daném běžném stavu znalostí se mohou systematické poruchy v mnoha případech posuzovat pouze kvalitativně.

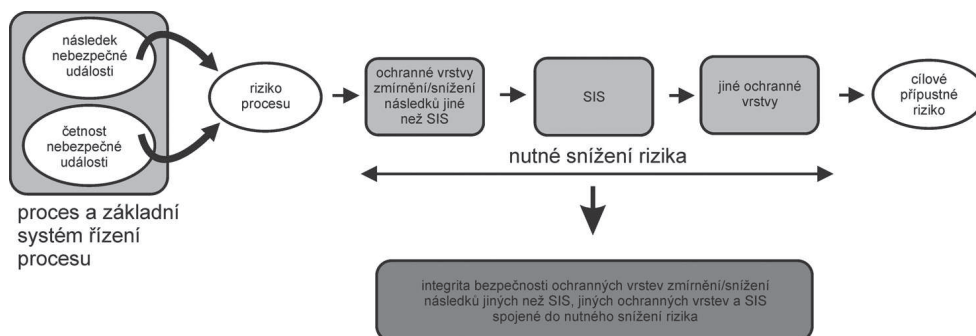
Požadovaná četnost nebezpečných poruch za hodinu bezpečnostní přístrojové funkce pro průběžný režim se určuje s uvážením rizika (v nebezpečném měřítku) způsobeného poruchou bezpečnostní přístrojové funkce působící v průběžném režimu spolu s četností poruch ostatních zařízení, které vede ke stejnému riziku, přičemž se uvažují příspěvky z ostatních ochranných vrstev. Ve složitějších případech je možné použít několik bezpečnostních systémů/funkcí s nižšími úrovněmi integrity bezpečnosti, aby se vyhovělo potřebě vyšší vrstvy funkce. Toho lze dosáhnout tak, že jsou použity systémy o SIL 2 a SIL 1, které jsou řazeny za sebou. To v praxi znamená, že požadovanou provozní funkci je možno vykonat pouze tehdy, jsou-li splněny požadavky nejprve prvního bezpečnostního systému a následně pak i požadavky druhého bezpečnostního systému. Splněním těchto požadavků jsou v podstatě splněny požadavky kladené na jeden bezpečnostní systém o SIL 3, protože výsledná pravděpodobnost vzniku poruchy při použití těchto dvou systémů je dána součinem pravděpodobností obou systémů a tedy odpovídá hodnotě pro SIL 3. Této možnosti je občas výhodné používat nejen z provozních, ale také z ekonomických důvodů. Aplikace, které vyžadují použití jedné samotné bezpečnostní přístrojové funkce s úrovní integrity bezpečnosti 4, se totiž v průmyslových technologiích vyskytují zřídka. Je důvodně praktické se takovým aplikacím vyhnout, protože je těžké a finančně nákladné dosáhnout a udržovat tak vysoké vrstvy funkčnosti během celého životního cyklu zařízení, technologie nebo výrobního procesu. Kromě jiného takto náročné systémy vyžadují značné nároky na znalosti obsluhy. S ohledem na svou komplikovanost tak mohou paradoxně samy o sobě implikovat vznik poruchy, protože obsluha nebo údržba jej nebude umět dokonale ovládat.

Jediná bezpečnostní přístrojová funkce o SIL 4 se připouští jen při splnění níže uvedeného kritéria a) anebo současném splnění kritérií b) a c).

- a) Kombinací vhodných analytických metod a zkouškami bylo jasně prokázáno, že se dosáhlo cílové frekvence poruch integrity bezpečnosti.
- b) Se součástkami, použitými jako část bezpečnostní přístrojové funkce byla učiněna rozsáhlá provozní zkušenost (taková zkušenost se získá v podobném prostředí a součástky se musely používat v systému nejméně se srovnatelnou vrstvou složitosti).
- c) Existuje dostatek údajů o poruchách hardwaru získaných ze součástek, užívaných jako část bezpečnostní přístrojové funkce, což dovolí dostatečnou důvěru k cílové míře poruch integrity bezpečnosti hardwaru, jaké je třeba (tyto údaje by měly být významné pro navržené prostředí, vrstvy aplikace a složitosti).



Obrázek 125: Model snižování rizika (Foord a kol., online).



Obrázek 126: Koncepce rizika a integrity bezpečnosti.

Celý výše nastíněný proces, který se snaží prostřednictvím zavádění ochranných vrstev redukovat stávající riziko (k čemuž je využíván právě výpočet hodnoty SIL), je s vyznačením vzájemných vazeb demonstrován na obrázku 125, resp. 126.

Cílové přijatelné riziko pak představuje takovou míru rizika, která je v kontextu na přijatá měřítko hodnot společensky a ekonomicky přijatelná. Integritu bezpečnosti, která slouží k jejímu dosažení, je proto nutno vnímat jako míru pravděpodobnosti, že ochranné vrstvy dosáhnou stanovených bezpečnostních funkcí (ČSN EN 61511) a tedy i očekávané (snížené) míry rizika.

5.4.7 Základní přístup při určování hodnoty SIL

Jak již bylo řečeno výše, bezpečnostní integrita představuje v podstatě „pravděpodobnost úspěchu“ a hodnota SIL pak definuje její čtyři diskrétní kvalitativní úrovně, přičemž úroveň 4 představuje nejvyšší bezpečnostní integritu. V takovém případě má

daný bezpečnostní systém v sobě zakomponováno již tolik bezpečnostních prvků, že bezpečnost jeho provozu je zajištěna. Ačkoli se zmiňované IEC normy soustředí na technickou bezpečnost systémů (zařízení i vlastních systémů řízení, např. velínů) a SIL, tyto principy jsou v podstatě obecné a lze je tedy aplikovat i na snižování environmentálních a finančních rizik, takže analogicky k SIL pak mohou být definovány indexy EIL a FIL. Ty mohou být aplikovány v kontextu se SIL jako prvky pro hodnocení ochranných funkcí v rámci ochrany životního prostředí nebo minimalizace finančních ztrát.

Jelikož je SIL definován jako míra zabezpečení daného zařízení nebo procesu, dá se říci, že v případě kontinuálně pracujícího zařízení vyjadřuje SIL frekvenci vzniku chyb (např. v jednotkách počet selhání za hodinu). Jelikož však faktické vysvětlení pojmu SIL nebylo jednoznačné a vznikaly zmatky, bylo na symposiu Safety-Critical Systems Symposium v únoru 2004 dohodnuto, že například v případě automobilu SIL představuje například tyto bezpečnostní funkce: ABS a airbagy. Oba tyto prvky mohou pracovat nezávisle na volbě řidiče, tj. aktivují se v případě potřeby, nicméně řidič má možnost inaktivovat je před započítím jízdy, rozhodne-li se tak. Čili nejedná se například o ruční brzdu, která je sice také bezpečnostním prvkem vozu, neboť zabráňuje samovolnému rozjezdu automobilu, nicméně její funkčnost není závislá na rozhodnutí řidiče. Přesto však můžeme i u tohoto bezpečnostního prvku očekávat selhání. Buď se jedná o technickou poruchu, nebo o špatné či žádné použití. Takže nezajistí-li řidič vůz ruční brzdou po zaparkování a dojde k jeho rozjetí, pak došlo k selhání prvku SIL vinou špatné obsluhy. Funkčnost tohoto zařízení dotčena nebyla, avšak prvek nezafungoval, když měl. V kontextu na bezpečnost stroje (v tomto případě automobilu) tedy došlo ke vzniku nežádoucí události. Stane-li se podobných incidentů více, může tato skutečnost vést až ke změně celkového indexu SIL, neboť četnost selhání stroje oproti původnímu očekávání se zvýšila. Nicméně v takovém případě je potřeba odhalovat příčiny tohoto stavu. Ověřili-li se, že technický stav vozu se výrazně nezměnil, pak je nutno hledat příčiny v chybné obsluze.

Základní otázkou však je, jak často bude selhání jednotlivých bezpečnostních funkcí vést až ke vzniku nežádoucí události. Obecně platí, že u funkcí s nízkými nároky (např. na rychlost nebo pozornost atd.) se nehodovost (frekvence selhání) považuje za kombinaci dvou parametrů: četnosti podnětů, jež mohou vést k těmto selháním a **pravděpodobnosti poruchy na vyžádání** (Probability the function Fails on Demand – *PF_D*). Z těchto hodnot lze vycházet při určení SIL, přičemž i v tomto případě se postupuje podle filozofie užívané pro hodnocení míry rizik.

Pro funkce, které mají vysoké požadavky (např. na rychlost či pozornost atd.), nebo se jedná o kontinuální operace, odpovídá nehodovost četnosti vzniku chyb λ (tj. počtu chyb za daný čas), a to při použití bezpečnostních opatření. Pojem alternativní opatření pak odpovídá **střední době bezporuchového provozu** (*MTTF*) dané funkce. Bylo zjištěno, že výsledná míra selhání má exponenciální distribuci. Tyto výkonové

míry jsou samozřejmě ve vzájemném vztahu. Obecně platí vzájemné vztahy popsané rovnicí 5-14:

$$PFD = \frac{\lambda T}{2} = \frac{T}{2MTTF} = \frac{1}{RRF} \quad (5-14)$$

kde T je tzv. interval odolnosti, tj. doba mezi jednotlivými selháními (rok), PFD je pravděpodobnost poruchy na vyžádání, λ je rychlostní funkce (rok^{-1}) a RRF je míra zbytkového rizika (Risk Reducting Factor).

$MTTF$ obvykle představuje pravděpodobnost, že stroj, zařízení nebo celý systém selže. Úroveň tohoto ukazatele je vyjádřena jako střední časový úsek (perioda), za který k tomuto selhání dochází. Tato hodnota je téměř vždy odhadována. Bohužel, tento přístup však často vede k mnohdy nereálným hodnotám. Lépe je $MTTF$ počítat na základě skutečně proběhlých selhání (Mahn a kol., 1995). Z výše uvedených vztahů plyne, že chceme-li významněji snížit nehodovost, pak by poměr $1/T$ měl být přinejmenším dvakrát, raději však více než pětkrát vyšší než požadovaná četnost.

U funkcí s nízkými nároky na rychlost SIL odpovídá PFD . U funkcí s vysokými nároky SIL představuje de facto četnost vzniku chyb. Za hranici mezi funkcí s nízkými nároky a vysokými nároky lze považovat takovou funkci, při které vzniká jedna chyba za rok. To se shoduje s prováděnými zkouškami pro odolnostní intervaly od 3 do 6 měsíců, což je v mnoha případech nejkratší možný proveditelný interval.

Uvažujme zařízení, které je vybaveno nějakým bezpečnostním prvkem konajícím příslušnou funkci (bezpečnostní přístrojovou funkci), která chrání před dvěma různými nebezpečnými situacemi. Jedna z těchto nebezpečných situací nastává v průměru jednou za dva týdny, tj. 25 krát ročně (jedná se tedy o funkci s vysokými nároky) a druhá v průměru jednou za deset let (jedná se o funkci s nízkými nároky). Jestliže je hodnota $MTTF$ dané přístrojové funkce 50 let (střední doba bezporuchového provozu daného bezpečnostního prvku), znamenalo by to, že bezpečnostní integrita daného zařízení dosahuje míry SIL = 1, protože pro jednotlivé funkce je hodnota PFD rovna:

$$PFD = \frac{0,04}{2 \times 50} = 4 \cdot 10^{-4} = \text{SIL } 3 \quad (\text{pro bezpečnostní funkci s vysokými nároky}),$$

resp.

$$PFD = \frac{10}{2 \times 50} = 10^{-1} = \text{SIL } 1 \quad (\text{pro bezpečnostní funkci s nízkými nároky}).$$

Při procesu určování SIL je nutné vykonat několik analytických kroků, které definoval Kosmowski (Kosmowski, 2003). Podle něj je nutné postupovat v tomto pořadí:

1. Určit četnost chyb systému, který není vybaven žádnou ochrannou vrstvou.
2. Určit následky možného selhání systému, který není vybaven žádnou ochrannou vrstvou.
3. Určit přijatelnost rizika (např. použitím matice rizik).
4. Určit kategorii SIL.

Bod 4 je klíčový, ale bez splnění bodu 1 a 2 jej není možné objektivně provést. Je potřeba si uvědomit, že jediný účinek **bezpečnostního přístrojového systému** (SIS) je redukovat četnost vzniku nebezpečných situací nebo pravděpodobnost jejich výskytu, to ale nelze provést, pakliže o těchto situacích (selháních, vzniku chyb) nemáme dokonalé informace.

Všechny metody pro určování SIL jsou založeny na podobných principech, které zahrnují provedení těchto kroků:

1. Identifikace nebezpečného procesu.
2. Určení přijatelného rizika pro daný proces.
3. Jestliže je při nebezpečném procesu překračováno přijatelné riziko, pak je nutno spočítat, jak moc je nutné míru rizika snížit a zda ochranné vrstvy budou správně fungovat i při kontinuálním provozu daného zařízení.
4. Určení faktorů vedoucích ke snížení rizika při použití jiných ochranných vrstev.
5. Výpočet faktoru RRF, což je v podstatě zbytkové riziko, kterého je nutno dosáhnout.

Vzájemný vztah jednotlivých faktorů a jejich ekvivalentní číselné hodnoty shrnuje tabulka 47. Určení přijatelnosti rizika je prováděno de facto souběžně s určením SIL. Jestliže je totiž hodnocením zjištěna hodnota SIL 1, pak je nutné navrhnout opatření ke snížení rizika, neboť se jedná ve většině případů o riziko nepřijatelné. Naopak v případě SIL 4 se jedná o riziko přijatelné. Kategorie SIL 3 a SIL 2 pak vyžadují podrobnější analýzu. V případě SIL 2 se většinou neobejdeme bez aplikace principu ALARP (blíže viz kapitola 5.5.6).

Určením kategorie SIL však nemusí hodnocení systému končit. Heinze (Heinze, 2001) využil obecně přijímaný přístup a rozšířil jej o tzv. „safety failure fraction“, což lze volně přeložit jako míru bezpečnosti subsystému. Jedná se o pravděpodobnostní veličinu vyjadřující, nakolik je daný systém odolný proti vzniku nežádoucích chybových stavů – tedy zda je stroj vybaven redundancí nebo jiným bezpečnostním systémem, který je schopen automaticky řešit odchylky od normálního stavu aniž by musel zasáhnout člověk či nikoli. V rámci hodnocení se používá semikvantitativní kategorizace spolehlivosti stroje a to pomocí tří stupňové škály, kde vyšší hodnota

Tabulka 47: Úrovně integrity bezpečnosti versus pravděpodobnost poruchy na vyžádání resp. četnost nebezpečných poruch bezpečnostní přístrojové funkce.

Úroveň integrity bezpečnosti <i>SIL</i>	REŽIM PROVOZU NA VYŽÁDÁNÍ Cílová střední pravděpodobnost poruchy na vyžádání <i>PF_D</i>	<i>RRF</i>	PRŮBĚŽNÝ REŽIM PROVOZU Cílová četnost nebezpečných poruch bezpečnostní přístrojové funkce zařízení λ	<i>MTTF</i> (rok ⁻¹)
SIL 4	10^{-5} – 10^{-4}	10^5 – 10^4	10^{-9} – 10^{-8} /hod	10^5 – 10^4
SIL 3	10^{-4} – 10^{-3}	10^4 – 10^3	10^{-8} – 10^{-7} /hod	10^4 – 10^3
SIL 2	10^{-3} – 10^{-2}	10^3 – 10^2	10^{-7} – 10^{-6} /hod	10^3 – 10^2
SIL 1	10^{-2} – 10^{-1}	10^2 – 10^1	10^{-6} – 10^{-5} /hod	10^2 – 10^1

Tabulka 48: Vzájemný vztah jednotlivých úrovní *SIL* a spolehlivosti stroje (Heinze, 2001).

Míra bezpečnosti subsystému (MBZ)	Spolehlivost stroje (odolnost proti vzniku chybové operace)		
	0	1	2
< 60 %	Není povoleno	SIL 1	SIL 2
60 % až 90 %	SIL 1	SIL 2	SIL 3
90 % až 99 %	SIL 2	SIL 3	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4

znamená vyšší spolehlivost. Pro finální hodnocení navrhl Heinze níže uvedenou tabulku 48, kde tzv. **míra bezpečnosti subsystému** (MBS) je definována jako poměr

$$MBZ = \frac{(\sum \lambda_S + \sum \lambda_{DD})}{(\sum \lambda_S + \sum \lambda_D)}, \quad (5-15)$$

kde λ_S je četnost chyb všech chyb (tj. včetně chyb bez následků), λ_D je četnost chyb s následky a λ_{DD} je četnost chyb s následky, které byly detekovány interní diagnostikou.

Tento přístup lze využít pro srozumitelné vyjádření míry spolehlivosti, resp. bezpečnosti, hodnoceného subsystému.

5.4.8 Posouzení nebezpečí a rizika

Mezi hlavní cíle posouzení nebezpečí a rizika patří popis a zhodnocení:

- Nebezpečí a nebezpečných jevů uvnitř procesu a při používání potřebných zařízení.
- Četnosti jevů vedoucích k jevu nebezpečnému.
- Rizik procesu spojených s nebezpečnými jevy.
- Všech požadavků na snížení rizika.
- Bezpečnostních funkcí požadovaných pro dosažení nutného snížení rizika.
- Zda některé z bezpečnostních funkcí nejsou bezpečnostními přístrojovými funkcemi.

Norma v souvislosti s tímto stanoví požadavek, že proces musí být již od počátku navrhován jako bezpečný. Mohou se však vyskytnout případy, kdy takový návrh není prakticky dosažitelný, anebo dostatečně ekonomicky zdůvodnitelný. V takových případech lze uplatnit již ve fázi návrhu takové přístupy, které povedou ke snížení předem známého rizika. Může se tedy jednat například o mechanické ochranné systémy či bezpečnostní přístrojové systémy. Tyto systémy mohou pracovat samostatně, nebo ve vzájemné kombinaci, avšak musí být splněn základní požadavek a to, přijatelná míra celkového rizika.

Vlastní posouzení nebezpečí a rizika musí být provedeno na procesu a s ním spojeném zařízení. Jeho výsledkem musí být:

- Popis každého nalezeného nebezpečného jevu a činitelů, které k němu přispěly (včetně lidských chyb).
- Popis důsledků a pravděpodobnosti takových jevů.
- Uvážení podmínek, jako jsou normální podmínky provozu, podmínky při spouštění, přerušení, údržbě, narušení procesu a nouzovém vypnutí.
- Určení požadavků na snížení rizika nezbytných k dosažení požadované bezpečnosti.
- Popis nebo odkazy na informace, týkající se uplatněných měřítek k snížení nebezpečí a rizika.
- Podrobný popis předpokladů uvažovaných v analýze rizik včetně možné frekvence vyžádaných zásahů a četnosti poruch zařízení a důvěry kladené na provozní omezení nebo na lidský zásah.

- Přiřazení bezpečnostních funkcí do vrstvy ochrany včetně potenciálního snížení efektivní ochrany před poruchou se společnou příčinou, mezi bezpečnostními vrstvami a základním řídicím systémem procesu (BPCS).
- Identifikace takových bezpečnostních funkcí, které jsou aplikovány jako bezpečnostní přístrojové funkce.

Příklady metod užívaných pro dosažení požadované SIL bezpečnostních přístrojových funkcí jsou zobrazeny v IEC 61511-3. Norma stanoví, že bezpečná míra pravděpodobnosti vzniku poruch BPCS, která vytváří vyžádání na ochrannou vrstvu, nesmí překročit hodnotu 10^{-5} za hodinu.

5.5 Management bezpečnosti a management rizik

5.5.1 Systémová bezpečnost

Během 80. let 20. století se v procesním průmyslu stalo několik závažných havárií, které vedly ke zvýšení důrazu na rozvoj a udržování účinných systémů řízení bezpečnosti. Byla zpracována řada návodů založených na technickém posouzení pro definování potřebných prvků systému řízení bezpečnosti. Příklady zahrnují API RP750: Process Safety Management (Řízení bezpečnosti v procesním průmyslu), CCPS Guidelines on Technical Management of Process Safety (Návody CCPS pro technické řízení procesní bezpečnosti) a DNV International Safety Rating System (DNV Mezinárodní systém hodnocení bezpečnosti).

Formální vyšetřování závažných průmyslových havárií ukázalo na širokou řadu faktorů, které mohou způsobit, nebo které mohou přispět ke vzniku havárie. Takovéto příčiny se často popisují jako iniciační bezprostřední nebo podstatné. Tímto se dělá rozdíl mezi takovými chybami, jako je otevření nesprávného ventilu a mezi iniciační příčinou havárie, jako je špatný projekt zařízení. Iniciační příčina činí bezprostřední příčinu vysoce pravděpodobnou. Jak již bylo probíráno v kapitole 5.3, lidská chyba hraje ve vzniku havárie hlavní roli.

Zde je důležité ocenit rozlišování mezi lidskou chybou buď jako bezprostřední příčinou selhání, nebo lidskou chybou, jako příčinou základní. Obecně přiřazení chyby jednotlivce jako příčiny havárie se už delší dobu nepřijímá jako úplné a odpovídající vysvětlení celé řady příčin, ani se už „lidská chyba“ nepovažuje za nevyhnutelnou. Spíše než hlavní příčina havárie je často lidský operátor brán jako dědic situace vytvořené špatným projektem, nesprávnou instalací, neodpovídajícími postupy nebo špatnými rozhodnutími managementu. Tento vývoj vedl k širokému přijetí konceptu, že způsob řízení bezpečnosti na pracovišti přímo ovlivňuje výkon bezpečnosti na pracovišti.

Správné porozumění určité problémové oblasti vyžaduje pochopení její historie, vědeckého základu, kulturního a sociálního prostředí, ve kterém byla vyvinuta a ve kterém se využívá. Systémová bezpečnost má své kořeny v inženýrství průmyslové bezpečnosti, která se datuje už od 19. století. Relativně nová disciplína systémové bezpečnosti je odpovědí na podmínky, které vznikly po 2. světové válce, když se vyvinuly její “rodičovské” disciplíny: systémové inženýrství a systémová analýza na řešení nových a komplexních inženýrských problémů. Vědecká báze všech těchto nových proudů inženýrství spočívá v teorii systémů, jejíž vývoj začal v 30. letech minulého století.

První studií, která se zabývala bezpečností jako samostatným předmětem, byla práce H. W. Heinricha, z r. 1929, ve které autor zpracoval 50 000 průmyslových havárií. Konstatuje se v ní, že na každý těžký pracovní úraz připadlo 29 menších zranění a 300 poruch bez ohlášených zranění a také, že těžkému zranění předcházelo tisíce skoronehod, tj. událostí, které měly nehodový průběh, ale skončily bez následku. Tato hypotéza se stala známou jako Heinrichova pyramida, která je statistickým základem pro eliminování nebezpečí ještě před tím, než dojde k těžkému úrazu.

Jiná studie pocházející ze stejného období se zabývala tehdy široce převládajícím přesvědčením, že bezpečnější zařízení s bezpečnostními ochranami jsou neefektivní a méně produktivní. Byla to velmi rozsáhlá studie, na jejímž vypracování se podílely velké inženýrské společnosti, zaměstnanci dvaceti průmyslových odvětví a šedesáti výrobních skupin. Závěrečná zpráva potvrdila hypotézu, že produktivita roste se zvyšující se bezpečností, což je poučení, které má význam. Studie vysvětluje historický úkaz nárůstu počtu havárií i přes úsilí průmyslové bezpečnosti, které je věnováno jejich snižování. Zjistilo se, že zvyšování počtu havárií souvisí s velkým nárůstem rychlosti zavádění mechanizace. Mechanizace ovlivnila bezpečnost třemi způsoby:

- Odstranila používání ručního nářadí.
- Zvýšila expozici nebezpečí údržbářského personálu.
- Umožnila zrychlení provozu a dávkování vstupního materiálu.

Závěr studie shrnuje, že přestože se i v průmyslu zvýšila expozice člověka nebezpečí (vystavení člověka nebezpečným situacím po časový interval), produktivita vykazovaná na člověka a hodinu se natolik zvýšila, že nebezpečí v poměru k produktivitě se ve skutečnosti snížilo. V prvních fázích zájmu o bezpečnost se kladl důraz na nebezpečné fyzikální podmínky. Jejich náprava byla významným pokrokem na počátku 20. století. Když zlepšení už nebyla tak výrazná, hledala se další vysvětlení. Heinrich publikoval v roce 1931 knihu s názvem Prevence průmyslových havárií, ve které dokazuje, že havárie a nehody vůbec jsou výsledkem nebezpečných činností a nebezpečných podmínek a tvrdí, že lidé způsobují mnohem více havárií, než nebezpečné podmínky. Toto tvrzení se stalo základem pro mnohé budoucí argumenty (Paleček a kol., 2006).

Poválečné období dalo vyrůst novému přístupu k bezpečnosti založenému na principech systémového inženýrství. I přes snahu některých inženýrů posilovat ideu zabudování bezpečnosti přímo do výrobků a průmyslových procesů byla většina bezpečnostních programů založená na a posteriori filosofii, tj. po havárii se provede podrobné vyšetřování a stanoví se, jak předcházet podobným haváriím v budoucnosti. Většina průmyslové výroby má relativně malý rozsah, proto vývoj nových, bezpečnějších výrobků a procesů na základě učení se z předcházejících chyb byl značně pomalý. Nástupem narůstající složitosti a ceny nových výrobků a nebezpečí v důsledku zavádění nových technologií se přístup učení z chyb stal neekonomický, až nepřijatelný. Objevením a využíváním vysokoenergetických zdrojů, jakými jsou např. vysokotlaké systémy a jaderná štěpná reakce, se zvětšily potencionální dopady havárií. V případě některých průmyslových odvětví, např. v jaderném průmyslu, je už jen jedna havárie považovaná za nepřijatelnou. Prudký rozvoj technologií po 2. světové válce přinutil průmysl přemýšlet v terminologii teorie systémů.

Teorie systémů

Počátky teorie systémů se datují od 30. let minulého století a tato teorie je považována za reakci na určité limity vědy při zvládání složitosti. Dvěma hlavními představiteli tohoto přístupu byli Norbert Wiener za inženýrství řízení a komunikace v technice a Ludwig von Bertalanffy za biologii. Bertalanffy zdůrazňoval, že ideje z rozličných oblastí se dají zkombinovat do všeobecné teorie systémů, a je proto považován za zakladatele tohoto přístupu (Mill, 1943).

Teorie systémů je doplňkovým přístupem a reakcí na vědecký redukcionismus. Redukování, opakovatelnost a vyvratitelnost formují společně základ vědeckých metod. Princip analytické redukce ve vědeckém přístupu, který spočívá v rozdělení problému na samostatné části a jejich následné separátní zkoumání, je spojovaný s Descartem (Paleček a kol., 2006). Princip redukcionismu spočívá ve třech předpokladech:

- Rozdělení na části nesmí porušit jev/skutečnost, která má být studována.
- Složky (komponenty) celku musí být stejné, ať se zkoumají odděleně nebo v celku.
- Principy, kterými se řídí sestavení celku z jednotlivých komponent, jsou jasné a přímočaré.

Systémový přístup se zaměřuje na systém jako celek a ne na jeho samostatné části. Vychází z předpokladu, že některé vlastnosti systémů mohou být adekvátně zkoumané jako celek jen tehdy, když se vezmou v úvahu všechny vlastnosti a proměnné předmětného systému a souvislosti vzájemných sociálních a technických aspektů. Aspekty a proměnné systémů se odvodí ze vzájemných vztahů mezi částmi systémů z toho, jak vzájemně mezi sebou reagují a ladí. Systémový přístup se soustřeďuje na analýzu a design celku jako odlišnosti od komponentů a částí (Paleček a kol., 2006).

Teorie systémů vychází z několika axiomatických definicí (Paleček a kol., 2006):

- Systém je množinou prvků, které se společně projevují jako celek k dosažení určitých společných cílů/výsledků. Všechny prvky jsou vzájemně provázané a přímo nebo nepřímo spjaté jeden s druhým. Tato idea je založena na předpokladech, že systémové cíle se dají definovat, a že stavba systému je atomistická, tzn., že systém může být rozdělen na jednotlivé komponenty a mechanismus jejich vzájemných interakcí lze popsat.
- Stav systému je v kterémkoliv časovém okamžiku určený množinou relevantních vlastností, které popisují systém v daném čase. Okolí systému je množina komponentů a jejich vlastností, které nejsou částmi systému, ale jejichž chování může stav systému ovlivňovat.
- Hranice mezi systémem a okolím je definovaná jako vstup nebo výstup čehokoliv, co přes ni přechází.
- Hierarchie systémů představuje skutečnost, že každá množina prvků, kterou lze považovat za systém, je všeobecně minimální částí hierarchie systémů, tzn., že systém může obsahovat podsystémy a zároveň může být částí většího systému.

Je důležité připomenout, že systém je vždy pouze modelem, abstrakcí v mysli analytika. V jednom a tom samém systému může pozorovatel vidět jiné účely než jeho projektant (pokud jde o umělý, člověkem vytvořený systém). Proto je třeba, aby pozorovatel i projektant definoval:

- Hranice systému.
- Vstupy a výstupy, prvky/komponenty.
- Strukturu.
- Relevantní interakce mezi komponenty a mechanismem, kterým si systém zachovává integritu.
- Účel resp. cíl, pro který má smysl považovat danou množinu prvků za koherentní entitu.

Systémové inženýrství

Vznik teorie systémů s různými historickými faktory vyvolal růst nové inženýrské disciplíny pojmenované systémové inženýrství. Byla to reakce na požadavky budování mnohem složitějších technologických systémů s následujícími charakteristikami:

- Velkým množstvím částí, počtem replik identických částí, prováděných funkcí a nákladů.

- Složitostí v tom smyslu, že změna jedné proměnné ovlivňovala mnohé další proměnné, a to navíc nelineárním způsobem.
- Poloautomatizací, tj. s rozhraním člověk–stroj, kde člověk vykonává určité funkce a stroj vykonává jiné.
- Nepredikovatelností, tj. nahodilostí vstupů a jiných poruch okolí.

Systémové inženýrství bylo nejintenzivněji využíváno v letectví a ve zbrojním průmyslu při vývoji interkontinentálních balistických raket. Hlavní principy systémového inženýrství:

- Definování cílů a ladění činnosti systému pro jejich dosažení.
- Stanovení a používání kritérií pro proces rozhodování.
- Vyvíjení alternativ.
- Modelování systémů pro analýzy.
- Implementace managementu a kontroly.

Ty jsou dnes všeobecně považovány za správnou inženýrskou praxi. Pokud je většina inženýrství založená na technologii a vědě, systémové inženýrství považuje za ekvivalentní významnou složku svojí praxe i management inženýrských procesů. Cílem systémového inženýrství je optimalizace provozu systémů podle prioritních kritérií návrhu. Základem každého přístupu pro dosažení tohoto cíle je výchozí předpoklad systémového inženýrství, že optimalizace jednotlivých komponentů nebo podsystémů všeobecně nezaručuje vytvoření optimálního systému. Je to známý fakt, že zlepšení některého z podsystémů může ve skutečnosti zhoršit vlastnosti celého systému. Když si uvědomíme, že podle principu hierarchie je každý systém vlastně podsystémem nějakého většího systému, představuje tento princip prakticky neřešitelný problém (Paleček a kol., 2006).

Systémový přístup poskytuje logickou strukturu pro řešení tohoto problému. Jako první se musí specifikovat cíle, kterých má systém dosáhnout a kritéria, podle kterých mohou být vyhodnocované alternativy návrhů. Potom nastupuje fáze syntézy systému, jejímž výsledkem je množina alternativních návrhů. Každá z těchto alternativ je následně analyzována a vyhodnocována podle požadovaných cílů a stanovených kritérií a nakonec je nejvhodnější z nich vybrána k realizaci. V praxi to představuje vysoce interaktivní proces vzájemného měnění původních cílů a kritérií na základě pozdějších stádií tvorby a rozpracování návrhu.

Systémoví inženýři nemusí být experty na všechny aspekty systému, ale musí rozumět podsystémům a různým jevům v nich natolik, aby byli schopni popsat a modelovat jejich charakteristiky. Znamená to, že systémové inženýrství často vyžaduje týmovou práci pro specifikaci náležitosti systému, vypracování studie realizovatelnosti,

porovnávací studie, návrh, analýzu a vývoj architektury systému a analýzy rozhraní člověk–stroj (Paleček a kol., 2006).

Systémové analýzy

V průběhu 50. let minulého století vyvinula RAND Corporation paralelně s rozvíjením systémového inženýrství metodologii nazvanou systémová analýza pro racionální postup při vyhodnocování alternativ návrhů při procesu rozhodování. Ve stručnosti lze říci, že systémová analýza je metoda pro rozsáhlé ekonomické odhadování nákladů a dopadů různých způsobů dosažení určitého cíle. Systémová analýza je provázaná s operačním výzkumem, je však více ucelenější, méně kvantitativní a více orientovaná směrem k širším strategickým a politickým otázkám (Mill, 1943).

Ve většině případů nedokážeme eliminovat všechny složky neurčitosti při procesech rozhodování, protože se k tomu nedají získat všechny relevantní informace. Z toho vyplývá, že následky jednotlivých směrů postupu nemohou být kompletně determinovány. Systémová analýza poskytuje organizovaný proces pro získávání a zjišťování specifických informací souvisejících s daným rozhodnutím. Systémové inženýrství a systémová analýza jsou už dlouhé roky fakticky sloučené a využívané při tvorbě komplexních systémů člověk–stroj, kde systémová analýza zabezpečuje údaje pro proces rozhodování a organizuje postupy výběru nejlepší alternativy návrhu. Tyto dvě disciplíny tvoří spolu teoretický a metodologický základ systémové bezpečnosti (Paleček a kol., 2006).

Základy systémové bezpečnosti

Po 2. světové válce se vývoj systémové bezpečnosti prolínal s vývojem systémového inženýrství, ačkoliv samotné kořeny systémové bezpečnosti sahají dost daleko do minulosti. Péče o průmyslovou bezpečnost se datuje už na přelom 19. a 20. století. Mnohé z jejich základních pojmů, jako např. předvídání nebezpečí a havárií a zabudování bezpečnosti do projektu od jejího počátku, předcházejí období po 2. světové válce. Podobně jako při systémovém inženýrství, mnozí odborníci praktikovali přístupy a techniky systémové bezpečnosti dávno před tím, než byla zformulovaná jako samostatná disciplína.

Systémová bezpečnost vzešla z programu vývoje interkontinentálních balistických raket pro vojenské letectvo (Intercontinental ballistic missiles – ICBMs) v 50. letech 20. století. V prvních raketových projektech nebyla systémová bezpečnost identifikována a přidělována jako specifická zodpovědnost konkrétní osobě/orgánu. Naopak, jak bylo tehdy zvykem, byl za bezpečnost zodpovědný projektant, manažer a hlavní inženýr. Do těchto projektů však vstoupila vyspělá technologie a podstatně větší složitost než v projektech předcházejících, a nevýhody standardního přístupu k bezpečnosti se staly zjevnými, i když se na mnohé problémy interface podsystémů přicházelo už příliš pozdě (Paleček a kol., 2006).

Havárie raketových střel byly velmi drahé a výsledky vyšetřování jejich příčin ukázaly vážné nedostatky v bezpečnosti celého systému, které si žádaly široké změny a nápravy. Náklady, které by byly potřebné k vykonání nutných modifikací a úprav, se ukázaly být tak vysoké, že se rozhodlo celý tento zbrojní program odložit a urychlit nasazení raketovému systému Minuteman. Tak se stalo, že velký raketový zbrojní systém, původně navrhovaný na dobu použití nejméně 10 let, byl používán méně než dva roky pro nedostatky jeho bezpečnosti.

Vyšetřování prvních havárií kosmických zařízení jasně ukázala, že příčiny většinou vyplývají z nedostatků návrhu, provozu a managementu. Tehdejší přístup k bezpečnosti založený na postupnosti „let-náprava-let“ byl očividně nevyhovující. Podle tohoto přístupu bylo vyšetřování havárie zaměřené na rekonstrukci příčin, přijetí opatření, anebo minimalizování opětovného vzniku havárie ze zjištěných příčin a případné standardizování přijatých opatření. Ačkoliv je tento přístup efektivní pro snížení počtu havárií z odhalených příčin, je na první pohled zřejmé, že je velmi drahý a v případě např. jaderných zařízení neakceptovatelný. Toto poznání vede k potřebě využití přístupů systémové bezpečnosti pro zajištění bezpečnosti provozu ještě před tím, než se vyskytnou první závažné nehody a havárie (Paleček a kol., 2006).

Zásady pro aplikaci systémové bezpečnosti byly již v roce 1966 uvedeny ve standardech USA pod označením MIL-S-381 30A a MIL-STD-882C. V nich je požadavek, aby zhotovitel stanovil a udržoval efektivní program systémové bezpečnosti naplánovaný a integrovaný ze všech fází vývoje zařízení, výroby, provozu a případné likvidace. Program systémové bezpečnosti musí zabezpečovat přesně stanovený postup metodické kontroly bezpečnostních aspektů a hodnotit projekt zařízení ve smyslu identifikování nebezpečí a předepsání časově i nákladně efektivních nápravných zásahů. Cíle programu systémové bezpečnosti mají zajistit:

- Bezpečnost zařízení odpovídající jeho poslání a zabudování v něm.
- Identifikaci, vyhodnocení, eliminaci anebo kontrolu na akceptovatelné úrovni nebezpečí přidružených k systému, podsystému a jednotlivým částem.
- Kontrola nad nebezpečími, která nemohou být eliminována, je zajištěná tak, aby chránila personál, zařízení a majetek.
- Použití nových materiálů, anebo výrobků a testovacích technik musí být spojené jenom s minimálním rizikem.
- Nápravná opatření požadovaná pro zlepšení bezpečnosti jsou minimalizována dočasným včleněním bezpečnostních faktorů během vzniku systému.
- Historické údaje o bezpečnosti generované podobnými programy bezpečnosti jsou brány v úvahu a používány všude, kde je to vhodné.

Tento vojenský standard systémové bezpečnosti vytvořil prakticky základ pro mnohé budoucí požadavky a programy mnoha agentur a průmyslných odvětví, která si buď

adaptovala programy systémové bezpečnosti z vojenství anebo NASA, anebo samostatně vyvinula své vlastní programy podle zkušeností, které byly získány z výstavby elektráren, z výroby složitých nebezpečných a drahých zařízení. Čekání na výskyt havárií a následné eliminování příčin se stalo neekonomickým a někdy až neakceptovatelným způsobem úprav a zdokonalování systémů.

Budování mnohých dnešních komplexních systémů si vyžaduje integraci částí (pod-systémů a komponentů) zhotovených různými samostatnými dodavateli a organizacemi. I když každý z dodavatelů dodrží požadovanou kvalitu svých částí, kombinování podsystémů do systémů vnáší nové chyby a nebezpečí, které nejsou vidět, pokud se na tyto části díváme jako na oddělené. V mnohých průmyslových odvětvích se potvrdilo, že zabudování bezpečnosti do zařízení nebo výrobků může zredukovat celkové náklady na jejich životní cyklus, a že dosažení akceptovatelné úrovně bezpečnosti vyžaduje přístupy systémové bezpečnosti.

Systémová bezpečnost využívá teorii systémů a systémové inženýrství pro prevenci předpověditelných havárií a pro minimalizování následků nepředvídatelných havárií. Zajímá se všeobecně o ztráty a škody a ne jen o smrtelné úrazy anebo o zranění, např. o poškození majetku, nesplnění poslání (mise, účelu) anebo environmentální škody. Klíčovým bodem je považovat ztráty za dostatečně vážné na to, aby na jejich prevenci byl věnovaný dostatek času, úsilí a prostředků. Velikost investic věnovaných na předcházení haváriím nebo jejich následkům bude závislá na sociálních, politických a ekonomických faktorech (Paleček a kol., 2006).

Prvotním zájmem systémové bezpečnosti je management rizik, tedy identifikace nebezpečí stanovení a vyhodnocení rizik, eliminace nebo kontrola pomocí analýzy designu a manažerských postupů. V roce 1968 vzniká nová disciplína „inženýrství systémové bezpečnosti“ jako „organizované veřejné mínění“. Jedná se o plánovaný, osvojený a systematický přístup k identifikování, analyzování a kontrolování rizik během celého životního cyklu systému za účelem snížení pravděpodobnosti výskytu nehod a minimalizace jejich následků.

Aktivity související se systémovou bezpečností začínají v nejranějších stádiích vývoje koncepce systému a pokračují přes všechny projekční činnosti, výrobu, testování, provoz a odstavení. Podstatný aspekt, který odlišuje přístup systémové bezpečnosti od ostatních přístupů bezpečnosti je prvořadý důraz na včasnou identifikaci a klasifikaci nebezpečí tak, aby mohly být přijaty nápravy pro jejich eliminování, anebo minimalizování ještě před konečným projektovým rozhodnutím (Paleček a kol., 2006).

Navzdory tomu, že je systémová bezpečnost relativně novou a ještě stále se vyvíjející disciplínou, má své základní ideje, které jsou zachovány ve všech jejích projevech a odlišují ji od ostatních přístupů bezpečnosti a managementu rizika. Systémová bezpečnost:

- Zdůrazňuje budování bezpečnosti a ne její přidávání do vytvářeného systému.
- Zaobírá se systémem jako celkem a ne jen s podsystémy a komponentami.
- Pojímá nebezpečí poněkud širě než jen jako chyby.
- Klade důraz na předcházející analýzu, než později na získanou zkušenost a dodatečně vytvořené standardy.
- Upřednostňuje kvalitativní přístupy před kvantitativními.
- Rozpoznává důležitost změn a konfliktů cílů v projektu systému a je více než jen systémové inženýrství.

Nejdůležitějším aspektem systémové bezpečnosti jsou postupy managementu bezpečnosti, který spočívá v (Paleček a kol., 2006):

- Stanovení politiky v definování cílů bezpečnosti.
- Definování odpovědností a kompetencí.
- Dokumentování a průběžné sledování nebezpečí včetně kontrol.
- Udržování bezpečnostního informačního systému včetně zpětné vazby a form hlášení poruch/havárií apod.

Spolehlivost a bezpečnost systému

Systémová bezpečnost a spolehlivost spolu úzce souvisí. Přitom platí, že bezpečné zařízení nebo bezpečný systém musí být spolehlivý, avšak spolehlivý ještě neznamená být bezpečný. Spolehlivostní inženýrství se přednostně zabývá chybami a redukováním četnosti jejich výskytu. Spolehlivost je definovaná jako charakteristika daného objektu vyjádřená pomocí pravděpodobnosti, že tento bude vykonávat specifikovaným způsobem funkce, které jsou na něm požadovány během stanoveného časového intervalu a za stanovených resp. předpokládaných podmínek.

Reprezentativními technikami spolehlivostního inženýrství spolehlivosti zaměřeného na minimalizaci chyb komponentů a tím i chyb komplexních systémů, které byly zapříčiněny chybami komponentů, jsou:

- Paralelní redundance.
- Zálohování zařízení.
- Koeficient a rezerva bezpečnosti.
- Snižování počtu přetížení.
- Limitování doby použití.

Tyto techniky jsou prokazatelně efektivní pro zvýšení spolehlivosti, ale bezpečnost nevyhnutelně nezvyšují, ba dokonce za jistých okolností ji mohou redukovat. Analýzy rizik při systémové bezpečnosti se dívají na interakce a nezaměřují se jen na chyby anebo jistoty inženýrského řešení. Spolehlivostní inženýři často považují spolehlivost a bezpečnost za synonyma. To je pravda jen v některých speciálních případech. Všeobecně má bezpečnost o něco širší význam než chyba a chyby ještě nemusí snižovat bezpečnost. Běžně mají spolehlivost a bezpečnost mnoho společných vlastností. Mnohé havárie však nastanou bez toho, že by selhala nějaká komponenta. Právě naopak, častokrát všechny komponenty při nich fungovaly podle očekávání a bezchybně. Taktéž se může stát, že komponenty mohou selhat (mít poruchu) bez toho, aby došlo k havárii (Paleček a kol., 2006).

Havárie a nehody mohou být zapříčiněny provozem zařízení mimo povolené rozsahy hodnot parametrů a časových limitů, ze kterých vycházely analýzy spolehlivosti. To nám říká, že systém může mít vysokou spolehlivost a přece může vést k mimořádné události typu závažné havárie. Navíc generalizované pravděpodobnosti a analýzy spolehlivosti se nemohou přímo aplikovat na specifické nebo lokální podmínky. Nejdůležitější je, že havárie a nehody mnohdy nejsou výsledkem jednoduchých kombinací chyb/selhání komponentů (Paleček a kol., 2006).

Bezpečnost vystupuje na úrovni systému, když jsou komponenty provozovány společně. Události vedoucí k havárii mohou být složitou kombinací chyby zařízení, nesprávné údržby, problémů informačního a řídicího systému, zásahů člověka a konstrukčních chyb. Analýzy spolehlivosti se zabývají jen pravděpodobnostmi vzniku havárií a nehod souvisejících s chybami; nevyšetřují potenciální škody, které může způsobit správná činnost (provoz) jednotlivých komponentů. Není možné, aby spolehlivostní inženýrství nahradilo systémovou bezpečnost, může ji ale doplnit. Musí to však být provedeno s jasným vědomím, že konečným cílem je zvýšení odolnosti systému vůči nebezpečí náhodných chyb. Je to vždy lepší, když se zařízení/systém navrhuje tak, že individuální náhodné chyby nemohou způsobit havárii i kdyby se vyskytly, ačkoliv to není vždy možné (Paleček a kol., 2006).

Velmi opatrní musíme být při aplikování technik odhadování spolehlivosti pro posuzování bezpečnosti. Nakolik nejsou havárie nevyhnutelně zapříčiněné událostmi, které se dají vyjádřit pravděpodobnostmi, nemůžeme pro ně všeobecně používat míry pravděpodobnosti rizika. Odhady pravděpodobnosti měří pravděpodobnost náhodných chyb a ne rizik a nehod anebo havárií. Když se při analýzách systémové bezpečnosti najde projektová chyba, bude daleko účinnější, když se odstraní, než když budeme někoho přesvědčovat pomocí vypočítaných pravděpodobností, že tato chyba nikdy nepůsobí havárii. Vysoké hodnoty pravděpodobnosti nezaručují bezpečnost a bezpečnost nevyžaduje ultra vysokou spolehlivost. Hlavním nedostatkem pravděpodobnostních modelů nejčastěji není to, co zahrnují, ale to, co nezahrnují. Příklad zní: „Uvažujme ohraničený systém, uvnitř kterého se mohou vyskytnout poruchové události s pravděpodobností řádově 10^{-3} a výše. Rozšířme teď jeho hranice tak, že do nového systému zahrneme i události, u kterých pravděpodobnost výskytu

byla řekněme řádově 10^{-4} nebo vyšší. Pokud bychom pro náš původní systém navrhli dvojnásobnou redundanci, mohli bychom zredukovat pravděpodobnost výskytu událostí v něm na hodnotu 10^{-6} . Dominantními událostmi v novém systému se však stanou události s pravděpodobností 10^{-4} , zatím co návrháři systému budou v zajetí iluze, že systém bude o dva řády bezpečnější, resp. spolehlivější, než ve skutečnosti je. Pokud se v podobných případech neuvažuje správně, může se lehkou dospět i k takovým absurdním hodnotám pravděpodobností jako 10^{-16} nebo 10^{-18} . Nízké hodnoty pravděpodobnosti jednoduše hovoří o tom, že systém neselže uvažovaným způsobem, ale naopak, selže s daleko vyšší pravděpodobností způsobem, o kterém jsme neuvažovali“. Odlišování rizika nehody od chyb je podstatné pro to, abychom porozuměli rozdílu mezi bezpečností a spolehlivostí (Paleček a kol., 2006).

Cena a efektivita systémové bezpečnosti

Z praktických důvodů musí být přístupy systémové bezpečnosti efektivně a cenově dostupné. Návratnosti nákladů na program systémové bezpečnosti se dosáhne tehdy, když se zabrání haváriím. Efektivnost programu systémové bezpečnosti se prokazuje velmi těžko, protože měřit něco, co se nestalo, je těžké. Jeden z nepřímých způsobů měření efektivnosti programu systémové bezpečnosti, byť i ne celkem uspokojivý pro nedostatek porovnávaných faktorů, je porovnávání systémů, které měly program systémové bezpečnosti s těmi, které ho neměly. Dobrým příkladem pro tento způsob prokazování efektivnosti programu systémové bezpečnosti je případ vývoje vojenských stíhaček F-4 a F-14 pro námořnictvo USA. Obě dvě tato letadla měla přibližně stejné bojové poslání, přičemž stíhačka F-4 neměla formální program systémové bezpečnosti a stíhačka F-14 takovýto program měla. Kumulativně měly materiálové poruchy při F-4 početnost 9,52/100 000 hod., přičemž při F-14 byla tato početnost 5,77/100 000 hod. Tento rozdíl početnosti se ještě zvětšil, když začaly skupinové lety. Částečně tyto rozdíly početnosti vysvětlovaly některé jedinečné vlastnosti jednotlivých typů stíhaček, avšak porovnávací údaje jednoznačně podporují efektivitu zavedení programu systémové bezpečnosti. Jinou cestou zjišťování efektivnosti programu systémové bezpečnosti je vykazování nebezpečí, které bylo personálem systémové bezpečnosti korigováno ještě předtím, než došlo k havárii, anebo bylo jinak zjištěno. Třetí cestou odhadování efektivnosti programů systémové bezpečnosti je zkoumání případů, při kterých nebylo respektované doporučení systémové bezpečnosti a došlo k haváriím (Paleček a kol., 2006).

Zvýšený tlak na efektivnost a ekonomičnost podnikání se promítá i do systémů managementu BOZP. Z ekonomického pohledu má oblast BOZP následující omezení:

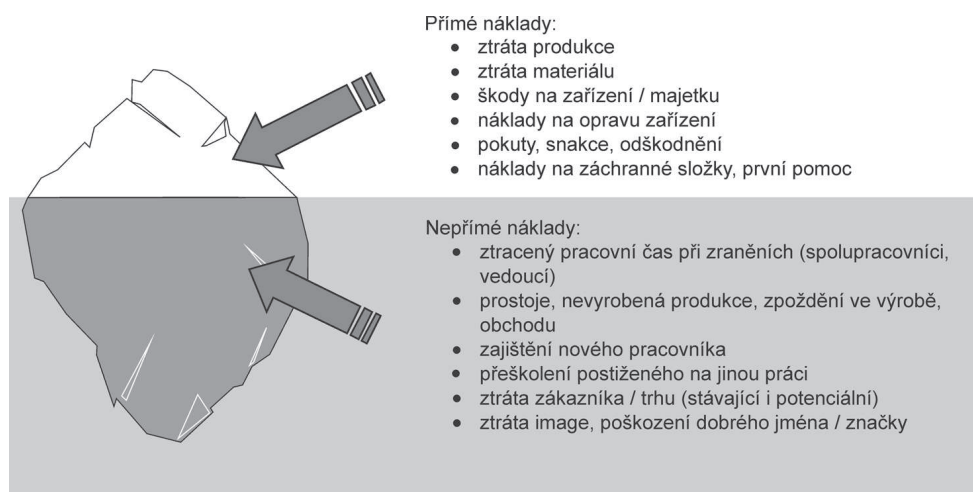
- Náklady na BOZP nejsou zcela exaktně vyjádřitelné a jsou většinou integrovány do rutinních řídicích operací.
- Motivační a stimulační systémy nebývají dobře nastaveny a vyúsťují spíše do podpory chování vedoucího k přesunu nákladů než k jejich snížení.

- Ekonomické stimuly nebývají zaměřeny na vztahy mezi BOZP a ostatními personálními aspekty zejména v oblasti rizikových pracovních míst a činností.
- Ekonomické náklady na pracovní úrazovost a nemocnost jsou jen obtížně a nepřesně vyčíslitelné.

V současné době proto vyvstává řada otázek typu:

- Jak může zdraví zaměstnanců ovlivnit konkurenceschopnost podniku?
- Jak peněžně vyjádřit hodnotu lidského života?
- Jak porovnat finanční úspory v důsledku lepších pracovních podmínek s vynaloženými náklady?

Tyto přístupy se značně odlišují od těch, které byly u nás prosazovány ještě před patnácti lety, kdy u BOZP nebyly brány v úvahu žádné ekonomické aspekty, ať se to již týkalo ztrát nebo nákladů. Do určité míry k tomu přispěla i skutečnost, že výkaznictví i celkový „účetní“ systém je v této oblasti málo propracován a je zaměřen převážně na sledování a vyjádření přímých ztrát a nákladů. Méně zahrnuje náklady a ztráty nepřímé, i když ty, podle odhadů, jsou čtyři až pětkrát vyšší. Náklady přímé a nepřímé ilustruje obrázek 127. Tento fakt se negativně projeví v rozhodování managementu, kdy dochází k rozdílnosti názorů a přístupů pracovníků ekonomických útvarů, pracujících s tvrdými daty a pracovníků pracujících např. v oblasti řízení lidských zdrojů, kteří mají na starosti bezpečnost a ochranu zdraví při práci. Tato rozdílnost pohledů se zvláště výrazně projevuje, pokud se podnik (společnost) po-



Obrázek 127: Příklady přímých a nepřímých nákladů spojených s pracovními úrazy (Řízení BOZP v podniku, 2009).

hybuje na globálních trzích. Logicky pochází celý problém z faktu, že práce není zbožím. Stroj může být vlastněn, pronajat, prodán. Zdokonalení, zhodnocení nebo znehodnocení je kapitalizováno v jejich tržní hodnotě. Ne tak práce, ta může být pronajata, nikoliv prodána (Paleček a kol., 2006).

Finanční stimuly

Úrazové pojištění a s ním spojený princip Bonus/Malus je jedním z významných nástrojů motivace ke snižování rizik a ke zvyšování úrovně BOZP na úrovni podniku. Avšak i tady vznikají problémy. Zprvė náklady na pojištění bývají součástí režijních nákladů – jedná se tady o fixní náklady, které se v podstatě nemění v průběhu rozhodujícího období (obvykle nejméně jeden rok). To znamená, že změny nebývají při rozhodování uvažovány. Například je-li pojištění součástí režie pro danou jednotku, neexistuje indikace dokazující, že investice do bezpečnosti může vést ke snížení pojistného. Vedoucí pracovník z provozu si může být vědom vztahu mezi riziky a pojištěním, ale z účetního hlediska je to těžko zachytitelné a vyčíslitelné (Paleček a kol., 2006).

Za druhé, předpokládejme, že podnik má dvacet organizačních jednotek. Režie je počítána na celý podnik a vychází ze všech operací. Potom změna v jedné jednotce výrazně neovlivní souhrnný údaj vycházející ze zbývajících devatenácti jednotek. Vhodnějším způsobem by mohlo být ovlivňování chování podniku pomocí redukce plnění v případě úrazu nebo nehody.

- Úprava evidence nákladů/ztrát a účetnictví. Cílem je získání informací o alokaci finančních prostředků, výskytu pracovních podmínek a stavu BOZP vzhledem k pracovním úrazům, nemocnosti a z nich vyplývajícím ztrátám.
- Návrh vhodných motivačních stimulů. V praxi často dochází k situaci, kdy motivační stimuly podporující např. zvyšování výkonu nebo produktivity působí proti zvyšování úrovně BOZP. Důležité je proto vytvoření konzistentního motivačního systému s jasně stanovenými indikátory a ukazateli.
- Integrace politiky BOZP. BOZP nelze prosazovat a její úroveň zvyšovat izolovaně od ostatních oblastí řízení. Změny v řízení jedné oblasti se mohou dotýkat i BOZP a naopak. Proto BOZP musí být integrální součástí celopodnikového řízení.

Souhrnně lze vztah bezpečnost (rizika) versus ekonomika vidět ve třech rovinách:

- Podnikové náklady převyšují náklady na jejich snížení. Úkolem managementu je nalézt a podpořit prostředky směřující k jejich snížení.
- Snižování rizik je nákladné z hlediska výsledků cost-benefit analýzy, ale je vyžadováno okolím (veřejností). V tomto případě vliv veřejnosti může výrazně ovlivnit výši nákladů do bezpečnosti.

- Jedná se o čistě ekonomické náklady na zlepšení pracovních podmínek, ale ty jsou vyžadovány právními předpisy. V tomto případě je velmi obtížné nalézt ekonomické stimuly.

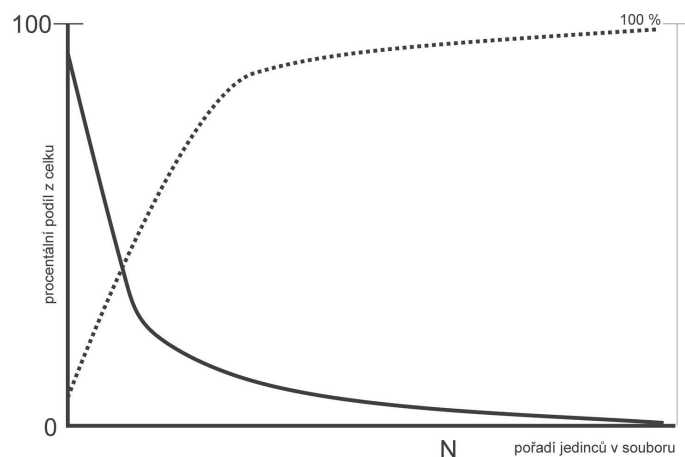
Paretův princip

Jistý americký multimilionář přišel s následující definicí, co je to být bohatý a co je to být chudý: „Být chudý znamená dostávat minimální výsledky s vynaložením maximálního úsilí“. „Být bohatý znamená dostávat maximální výsledky s vynakládáním minimálního úsilí.“ Nepracujte tvrději, pracujte chytřeji!

Jednou ze zásad, která nám umožní být efektivnější, je minimalizace všech činností, které nejsou užitečné, tj. těch, které přímo nepřispívají k dosahování našeho hlavního cíle. Při dodržování této zásady se můžeme řídit Paretovým principem, známým také jako pravidlo 80/20 (čti osmdesát na dvacet). Wilfredo Pareto, italský ekonom (žijící v 19. století), zjistil, že 20 % obyvatelstva vlastní 80 % všeho majetku v zemi. Toto pravidlo se později ukázalo jako obecně platné v mnoha dalších oblastech života:

- 20 % zákazníků nebo výrobků znamená 80 % obratu.
- 20 % zákazníků je autory 80 % stížností.
- 20 % pracovníků vykoná 80 % objemu práce.
- 20 % výrobních chyb způsobí 80 % zmetků.
- 20 % novin obsahuje 80 % informací.
- 20 % času stráveného na poradě ovlivní z 80 % obsah usnesení.
- 20 % mimořádných událostí způsobí 80 % všech následků z těchto mimořádných událostí.
- 20 % disponibilních zdrojů, sil a prostředků zvládne odstranit 80 % následků mimořádných událostí.
- 20 % iniciačních událostí je příčinou 80 % závažných průmyslových havárií atd.

Graficky tuto skutečnost popisuje obrázek 128. Z uvedených příkladů je zřejmé že, Paretovo pravidlo má vztah k obecné efektivitě činností, dějů a procesů v systémech. Kdo si toto pravidlo neuvědomuje, nerespektuje ho, nemůže dosahovat úspěchu. **Nejzávažnější aplikací je: 20 % jakéhokoli úsilí přináší 80 % celkového efektu (a to platí i pro krizové řízení).** Analýza podle pravidla 80/20 potom zkoumá vztah mezi dvěma řadami srovnatelných údajů. Jedna řada má charakter měřitelných prvotních veličin a druhá řada bývá vyjádřením procentuálního podílu členů řady na celkovém výsledku činnosti, která je sledována a měřena (Paleček a kol., 2006).



Obrázek 128: Grafické vyjádření Paretova principu.

Analýzou je tato činnost proto, že můžeme porovnávat dvě řady – jednu závislou a jednu nezávislou. Má kvantitativní naplnění, kvalitativní stránkou pravidla 80/20 je způsob myšlení. Ne všichni jsou zaměřeni na odborné analytické činnosti, ale i kvalitativní stránka pravidla je velmi cenná. Spočívá v tom, že myšlení podle tohoto pravidla je uplatnění jeho vlivu na naši (především rozhodovací) činnost. Stejně jako u analýzy podle pravidla 80/20 začínáme s hypotézou o možné nerovnováze mezi vstupy a výstupy, tak i při myšlení podle tohoto pravidla provádíme odhad důležitosti jednotlivých činností, které mají vliv jako celek na výsledek činnosti. To znamená, abychom si ze všech věcí byli schopni povšimnout těch důležitých, méně důležitých a nedůležitých stránek a zabývali se jenom těmi skutečně důležitými. Učíme se tak vidět les skrz stromy (Paleček a kol., 2006).

Nikdy se nám sice nepodaří bez měření objevit oněch 20 % důležitých skutečností, které jsou nejefektivnější, ale toto pravidlo nás učí rozlišovat a odhadovat to důležité v záplavě veškerých skutečností. Neustále nás nutí se ptát, co je opravdu důležité a co je nedůležité. Toto pravidlo nás učí rozhodovat se na základě vlastního odhadu důležitosti podmínek naší činnosti a činnosti ostatních. Kvalitativně se způsob myšlení podle tohoto pravidla projeví tak, že činnost takto uvažujícího člověka je úspěšnější než dříve (Paleček a kol., 2006).

K tomu lze použít tyto zásady:

- Dosahovat výjimečnou produktivitu (zlepšením myšlenkových činností) a nezvyšovat přitom fyzické úsilí činnosti.
- Hledat zkratku a neprocházet celou cestu – problematika zobecnování.
- Mít svůj život pod kontrolou při vynaložení nejmenšího úsilí.

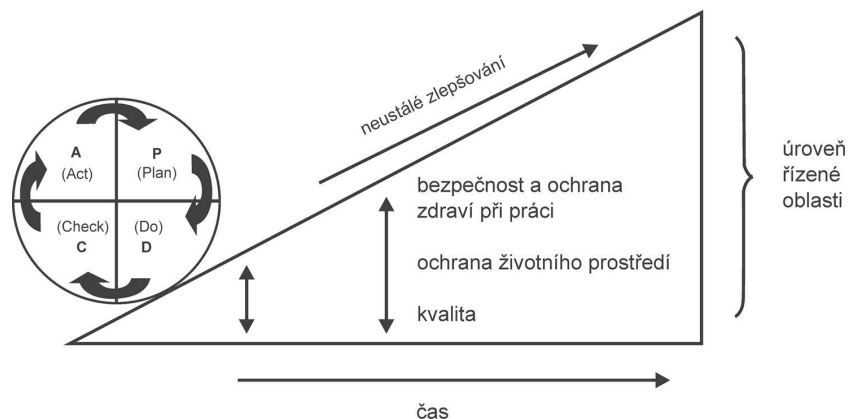
- Umět si vybírat a nesnažit se zvládnout vše (platí to i při přidělování dílčích kompetencí podřízeným).
- Snažit se o dokonalost v několika málo věcech a ne o výjimečný výkon ve všem (pro krizové řízení platí zvládnout průměrně všechno a výjimečně vlastní odbornost).
- Umět rozdělit pracovní úsilí odpovídajícím způsobem pro všechny.
- Mimořádně pečlivě vybírat svou pozici při řešení krizové situace (a to i pro pracoviště krizového řízení).
- Zaměřit se ve své práci na nejpodstatnější záležitosti, méně důležité delegovat ostatním.
- Odhadnout, které činnosti vedou k nejrychlejšímu a nejkvalitnějšímu výkonu práce.
- I při krizové situaci si najít místo svého psychického uvolnění a rozhodovat o důležitých věcech záchrany v co největším klidu („pohodě“), ostatní odsunout na pozdější dobu.
- Efektivně využívat ty chvíle života, kdy je nám štěstí nakloněno.
- Snažit se být nad věcí duševně i věcně a najít si svůj „balkón“ pro vidění věcí shora v případě, že mám mít o věcech přehled a mám je řídit.

Demingův princip trvalého zlepšování

Novou situaci a klima na světových trzích po 2. světové válce plně pochopili japonští stratégové, průmyslníci a manažeři, kteří jako první docenili teorie W. E. Deminga. S pomocí jeho metod komplexního chápání kvality předvedli „zázrak japonského managementu“ v podobě exploze vývozu kvalitní japonské produkce na světový trh. Tento tzv. Demingův princip je založen na čtyřech základních krocích, jejichž smyslem je dosažení trvalého zlepšování v řízené oblasti (původně pouze kvality) (Deming, 1986). Schematické znázornění tohoto principu ilustruje obrázek 129.

Obecný výklad Demingova principu:

- **Plan** – Plánuj: stanov cíle a procesy nezbytné k dosažení požadovaného výsledku.
- **Do** – Dělej: implementuj procesy (tj. proved', co jsi naplánoval).
- **Check** – Kontroluj: monitoruj a měř procesy ve vztahu k politice, cílům a stanoveným požadavkům, vypracuj zprávy o výsledcích (tj. kontroluj, co jsi provedl).
- **Act** – Jednej: prováděj opatření podle výsledků kontroly, uprav cíle a procesy směrem ke zvyšování výkonnosti a k trvalému zlepšování.



Obrázek 129: Schematické znázornění Demingova principu trvalého zlepšování (Horehledová, 2008).

Úspěch praktického pojetí Demingova principu u japonských podniků vedl k tomu, že i další průmyslové společnosti začaly v 80. letech 20. století obracet pozornost na kvalitu v širokém pojetí a zejména v Americe a Evropě začaly vznikat první modely jejího řízení založené na Demingově principu neustálého zlepšování a celých soustav nástrojů pro jeho uplatnění. Série norem ISO a norma OHSAS patří právě mezi takové vysoce úspěšné nástroje, které pomáhají zavést a udržovat různé systémy managementu, jež jsou v dnešní době pro organizace a jejich ekonomický růst klíčové. Tyto normy mají univerzální charakter, což znamená, že nezávisí ani na charakteru procesů, ani na povaze výrobků. Jsou tedy aplikovatelné jak ve výrobních organizacích, tak i ve službách, bez ohledu na velikost organizace (Dirner, 1997).

Obecně lze shrnout základní procesy systému managementu podle Demingova principu trvalého zlepšování následovně:

- Vymezení rozsahu systému.
- Vyhlášení politiky pro danou oblast.
- Plánování určení jednotlivých požadavků a způsobu jejich zavedení a udržování v praxi.
- Implementace jednotlivých požadavků do praxe a jejich řízení.
- Provádění a vyhodnocování kontrol.
- Provádění přezkoumání fungování systému managementu vedením.

Smyslem Demingova principu je dosažení trvalého zlepšování v dané oblasti (původně jen kvality). Princip zahrnuje plánování cílů a procesů nezbytných pro zajištění požadovaného výsledku, následné provedení naplánovaných akcí, jejich kontrolu prostřednictvím systematického monitorování a měření procesů ve vztahu k politice,

cílům a požadavkům. Posledním krokem procesu je jednání podle výsledků kontrol spočívající v upravení cílů a procesů směrem k trvalému zlepšování. Následuje opětovné plánování, provedení, kontrola a stále dokola.

5.5.2 Standardy pro systémy managementu bezpečnosti

Průmysl je v současné době jedním ze zásadních zdrojů negativních vlivů na lidské zdraví a životní prostředí. Rozmach civilizace a exploze znalostí se odráží v řadě lidských činnostech, přičemž mnohdy nevědomě dochází ke vzniku nežádoucích událostí s různě vážnými akutními i chronickými následky. K omezení těchto negativních důsledků se využívají vedle technologických opatření rovněž různá organizační opatření a ekonomické nástroje. Mezi tyto nástroje patří především systematická organizace a manažerské systémy, kdy je v obecném pojetí podstatou na základě předdefinovaných postupů a stanovených pravidel řídit a usměrňovat aktivity organizací tak, aby dosáhly předpokládaných efektů.

Dnes se manažerské techniky v organizacích aplikují prakticky na všechny oblasti řízení, jako je kvalita produktů, bezpečnost zaměstnanců a okolí podniku, bezpečnost informací, ovlivňování životního prostředí, rozhodování v oblasti financí, plánování, přerozdělování zdrojů atd. Systémy managementu kvality, ochrany životního prostředí nebo bezpečnosti informací se v organizacích implementují podle mezinárodních norem ISO, systém managementu bezpečnosti a ochrany zdraví při práci nejčastěji podle mezinárodní normy OHSAS 18001 (ČSN OHSAS 18001:2008, 2008), ale rovněž podle instrukcí Mezinárodní organizace práce ILO-OSH 2001 (ILO-OSH 2001, 2001) a podle různých národních programů a návodů (v ČR program Bezpečný podnik (Bezpečný podnik, 2008)). Systémy managementu podle uvedených standardů se implementují nejčastěji za účelem upevnit pozici organizace na trhu, posílit konkurenceschopnost svých produktů, zvyšovat prestiž a zisk, přičemž podstatou těchto systémů je zabezpečení řízení organizace na všech úrovních s cílem zajistit např. požadovanou úroveň bezpečnosti, kvality produktů nebo dosahovat snižování až eliminace dopadů činností organizace na životní prostředí. Podstatné však je, že implementace těchto systémů managementu je dobrovolná a prokazuje se certifikáty, které jsou organizacím udělovány akreditovanými organizacemi na základě úspěšného certifikačního auditu. Existují však i systémy managementu, které jsou u organizací implementovány na základě zákonné povinnosti (viz systém řízení bezpečnosti ve smyslu prevence závažných havárií popsáný v kapitole 5.5.3).

První systematický a moderní pokus o formulování systému k řízení aspektů BOZP vznikl ve Velké Británii, kde bylo v r. 1993 vydáno doporučení HSG65 (Successful health and safety management), které bylo v r. 1996 transformováno do normy BS 8800 (Occupational health and safety management system). HSG65 představuje návod na „Úspěšný systém managementu BOZP“, původně vydaný britským Úřadem pro zdraví a bezpečnost (HSE = Health and Safety Executive) v roce 1991 a následně revidovaný v roce 1997. Účelem tohoto „Úspěšného systému managementu BOZP“

je prokázat, že BOZP může a má být řízeno se stejným stupněm odbornosti a podle stejných standardů, jako ostatní klíčové podnikatelské činnosti tak, že rizika jsou účinně řízena a lidé jsou preventivně chráněni. V roce 1991 šlo o relativně nový přístup, třebaže dnes je široce přijímán v mnoha právních systémech. Druhé vydání HSG65 bylo značně novelizováno a v současnosti jsou značné tlaky na další revizi, ale není žádný pevný plán na tuto revizi. HSG65 je založen na neustálém zlepšování systému managementu o šesti prvcích na vysoké úrovni a obsahuje bohaté množství praktických návodů. Avšak není, pravděpodobně úmyslně, strukturován tak, aby mohl být snadno přeměněn na normu, podle které lze hodnotit a HSE nevydal žádné průvodní dokumenty porovnatelné s dokumenty vydanými ISO na podporu ISO 9001 a 14001. Proto je obtížné toto tvrzení jednoduše ověřit, ačkoliv mnoho organizací, zvláště těch působících ve Velké Británii, tvrdí, že mají svůj interní systém managementu BOZP založen na HSG65.

Norma BS 8800 znamenala důležitý posun v oblasti řízení BOZP, avšak neumožňovala certifikaci systému managementu. Hlavní text normy je podporován řadou příloh, které poskytují detailní praktické návody na implementaci systému managementu BOZP. Tyto přílohy pokrývají klíčové činnosti, jako je hodnocení rizik, šetření úrazů, měření výkonu a audit, čímž ukazují jejich propojení s celkovým systémem managementu BOZP. Mezi BS 8800 a HSG65 existuje mnoho vazeb a ve své kombinaci představují bohatý zdroj návodů na správnou praxi v oblasti BOZP, jak na vyšším stupni řízení, tak i na provozní úrovni. Stejně jako HSG65, tak i BS 8800 není specifikací systému managementu BOZP, podle kterých se dá hodnotit a certifikovat stávající systém managementu.

Při navrhování původní BS 8800 se lišily názory na to, zda by se mělo či nemělo podporovat nezávislé hodnocení a certifikace systému řízení BOZP v organizaci, jako je to u systémů managementu kvality a ochrany životního prostředí. Někteří považovali tyto certifikáty za užitečné, zvláště ve vztahu k účinnému managementu dodavatelského řetězce, ostatní byli přesvědčeni, že stávající certifikační postupy vyžadují nadměrné náklady, daly vzniknout nepoužívaným manuálům, mnoho dobrého nepřinesly, a proto by se mělo bránit novým certifikátům. Prokázalo se nemožné sladit tyto dva rozporné názory v rámci BS 8800, a tak byla tato norma strukturována a publikována jako norma, podle které se systém managementu necertifikuje.

To byl také jeden z důvodů, proč byla v roce 1999 vydána mezinárodně uznávaná specifikace OHSAS 18001 (OHSAS 18001:1999, 2004), která stanovila požadavky na systém managementu BOZP, podle nichž bylo možné zavedený systém posuzovat a certifikovat. Doprovodným dokumentem byl OHSAS 18002:2000 Systémy managementu bezpečnosti a ochrany zdraví při práci – směrnice pro zavádění OHSAS 18001 (OHSAS 18002:2000, 2004), která citovala specifické požadavky OHSAS 18001 a poskytovala potřebné návody k jejich implementaci do praxe.

OHSAS 18001:2007

V druhé polovině roku 2007 byla vydána norma BS OHSAS 18001:2007, která novelizuje specifikaci OHSAS 18001:1999. V březnu 2008 byl následně vydán český překlad této normy formou ČSN. V návaznosti na aktualizaci OHSAS 18001 proběhla i celková revize OHSAS 18002, která má rovněž status mezinárodní normy. Její český překlad byl vydán jako ČSN OHSAS 18002:2009.

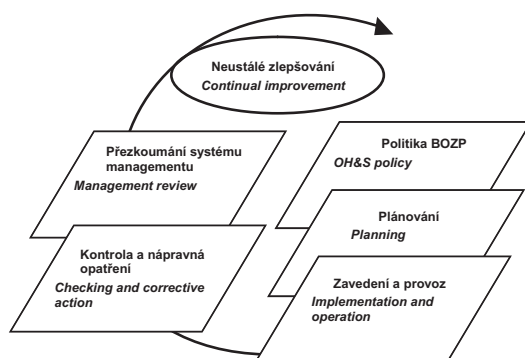
Jedním z hlavních cílů novelizace OHSAS 18001 bylo přiblížení struktury normy OHSAS struktuře norem ISO 14001 a ISO 9001, a tím zlepšení kompatibility systému managementu BOZP se systémy managementu kvality a ochrany životního prostředí. Součástí příloh normy OHSAS 18001 je proto srovnání obsahu těchto tří norem, z něhož je kompatibilita uvedených systémů managementu zřejmá. Vybrané prvky a procesy systému managementu BOZP odpovídají rovněž prvkům a procesům stanoveným dalšími normami, jako např. ISO 19011 (Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu) a ISO/IEC Guide 73:2002 (Management rizika – slovník). Důležitou součástí příloh normy OHSAS 18001 je také srovnání jednotlivých prvků systému managementu BOZP požadovaných normou OHSAS 18001 s prvky stanovenými Metodickými návody mezinárodní organizace práce pro systémy řízení BOZP – ILO-OSH 2001. Podle těchto návodů nejsou zavedené systémy managementu BOZP v organizacích ČR certifikovány. Uvedené srovnání popisuje vzájemné vztahy mezi jednotlivými prvky včetně konstatování, že systém managementu BOZP zavedený podle požadavků OHSAS 18001 bude kompatibilní rovněž s doporučeními těchto metodických návodů.

Veškeré požadavky normy OHSAS 18001 směřují k zajištění celé problematiky bezpečnosti na pracovišti a ochrany zdraví při práci na základě Demingova principu trvalého zlepšování, přičemž zásadní částí je proces identifikace nebezpečí a následného posouzení rizik. Norma stanoví základní podmínky, které musí být při tomto procesu brány v úvahu, a vyzdvihuje nezbytnost zaměření organizace především na podstatu celého procesu, kterou je stanovení adekvátního způsobu řízení daného rizika. Při určování způsobu řízení rizika pak musí organizace podle požadavků normy postupovat v souladu se stanovenou hierarchií (1. odstranění, 2. nahrazení, 3. technická opatření, 4. značení a organizační opatření, 5. osobní ochranné prostředky), což rovněž odpovídá požadavkům právních předpisů (zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů). Základní prvky systému managementu BOZP podle normy OHSAS 18001 jsou:

- Stanovení Politiky BOZP.
- Zavedení plánovacích mechanismů zahrnujících:
 - identifikaci nebezpečí, posuzování rizik a stanovení způsobu jejich řízení,

- identifikaci požadavků právních předpisů a jiných požadavků, které se na organizaci vztahují.
- Stanovení cílů a programů v oblasti BOZP.
- Implementace a provoz zahrnující:
 - stanovení odpovědností, povinností a pravomocí,
 - způsob plánování a přerozdělování zdrojů,
 - požadavky na školení, výcvik a odbornou způsobilost zaměstnanců,
 - požadavky na komunikaci, konzultace a spoluúčast zaměstnanců na řízení BOZP v organizaci,
 - požadavky na dokumentaci systému managementu,
 - podmínky řízení provozu,
 - požadavky na havarijní připravenost a reakci.
- Kontrola a nápravná opatření zahrnující:
 - požadavky na měření a monitorování výkonnosti organizace v oblasti bezpečnosti,
 - podmínky hodnocení souladu provozní činnosti s požadavky právních předpisů a s jinými požadavky,
 - podmínky vyšetřování incidentů,
 - podmínky přijímání nápravných a preventivních opatření,
 - požadavky na provádění interních auditů systému managementu BOZP,
 - přezkoumání systému managementu BOZP vedením společnosti.

Uvedené prvky systému managementu schematicky znázorňuje obrázek 130.



Obrázek 130: Model systému managementu BOZP podle požadavků normy OHSAS 18001 (ČSN OHSAS 18001, 2008).

ILO-OSH 2001

Jako výsledek spolupráce Mezinárodní organizace práce a Mezinárodní asociace hygieny práce byla vyvinuta instrukce ILO-OSH 2001, která je určena k řízení bezpečnosti a zdraví zaměstnanců v organizaci a jeho zlepšování. Není právně závazná ani nevyžaduje certifikaci. Tato instrukce poskytuje základní principy a strukturu systému řízení pracovního zdraví a bezpečnosti jak na národní, tak zejména na podnikové úrovni s cílem minimalizovat dopady práce na zdraví a životy zaměstnanců. Důležitý je požadavek trvalého zlepšování, který organizaci nutí neustále vyvíjet úsilí ke zvyšování úrovně BOZP včetně pracovních podmínek.

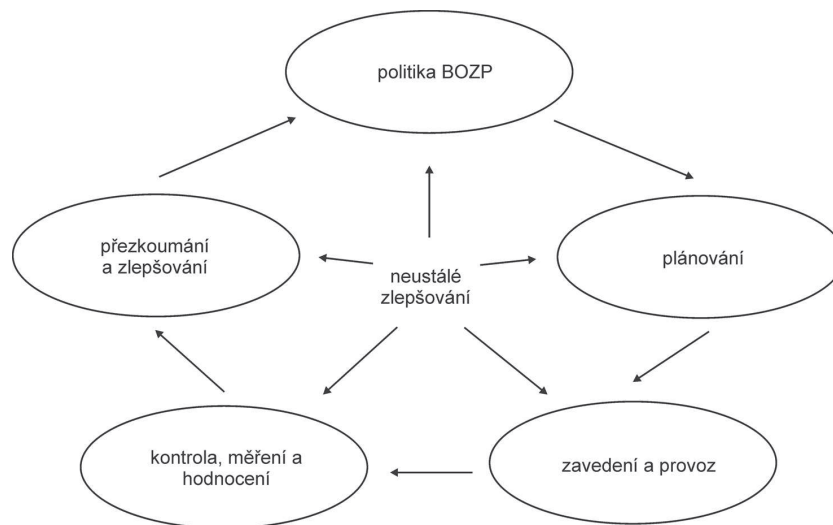
Instrukce ILO-OSH 2001 patří co do ucelenosti mezi nejpokročilejší používaná systémová řešení pro řízení BOZP v podniku. Zavedení takového pracovních-bezpečnostního systému do již existujících řídicích struktur organizace nebývá jednoduché a při zodpovědném přístupu k věci může trvat i několik let.

Postupy stanovené tímto metodickým návodem byly na české podmínky spolu s dalšími požadavky prosazovanými v rámci EU aplikovány prostřednictvím Národní příručky Systém řízení bezpečnosti a ochrany zdraví při práci.

Bezpečný podnik

Se snahou vnést řád do velkého množství předpisů, norem, instrukcí a návodů pro řízení bezpečnosti a ochrany zdraví při práci na podnikové úrovni v českém prostředí vytvořil Český úřad bezpečnosti práce ve spolupráci s Výzkumným ústavem bezpečnosti práce, v. v. i. program Bezpečný podnik. Záměrem tohoto programu je sloužit zejména velkým a středním podnikům jako podpůrný nástroj k plnění legislativních požadavků a zavedení systematického přístupu k zajišťování bezpečnosti. Jeho princip je v podstatě shodný s pravidly systémů managementu kvality a ochrany životního prostředí, jedná se tedy o zavedení, udržování a kontrolu s cílem trvalého zlepšování úrovně BOZP (viz obrázek 131).

Pravidla a postupy programu Bezpečný podnik umožňují podnikům a organizacím zavést funkční, transparentní, účinný a ekonomicky efektivní systém řízení bezpečnosti odpovídající požadavkům směrnic EU např. 96/82/EHS o prevenci závažných havárií nebo 96/61/EHS o integrované prevenci a kontrole znečištění a z nich vycházející legislativě České republiky. Podstatným rozdílem oproti jiným návodům pro systémy managementu bezpečnosti jsou požadavky kladené i na jiné oblasti řízení, jako např. požární ochrana, nakládání s nebezpečnými chemickými látkami, ochrana životního prostředí, nakupování služeb atd.



Obrázek 131: Princip trvalého zlepšování systému řízení BOZP podle programu Bezpečný podnik (Bezpečný podnik, 2008).

5.5.3 Požadavky na systém managementu bezpečnosti

Pro plnohodnotné a efektivní plnění povinností na úseku BOZP by si měl každý podnik vytvořit určitý předem definovaný systém řízení BOZP, jehož funkce by měla směřovat k minimalizaci pracovní úrazovosti, k prevenci rizik a k aktivní spolupráci se zaměstnanci (tj. napříč celým pracovním kolektivem v horizontálním i vertikálním směru), včetně součinnosti s odbory. Systém se musí opírat především o dokumentaci potřebného rozsahu, vyhledávání a odstraňování rizik, průběžnou kontrolu, operační řešení zjištěných nedostatků (zahrnující zainteresovanost managementu a jeho ochotu vynakládat potřebné finanční prostředky) a širokou systémovou spolupráci.

Systémová spolupráce představuje kooperaci a komunikaci mezi „jednotlivými hráči“, kterými jsou: osoba odborně způsobilá v prevenci rizik, zástupci provozních (správních) úseků, zástupci výrobních úseků, zástupci úseku personálních záležitostí, vrcholový management a odbory. V takto postaveném systému potom osoba odborně způsobilá zejména zpracovává a vede dokumentaci BOZP, provádí pravidelné kontroly stavu BOZP za účelem vyhledávání rizik na jednotlivých pracovištích, podává návrhy na odstranění zjištěných závad, provádí školení vedoucích zaměstnanců z BOZP, sepisuje protokoly o úrazech a je členem komise pro odškodňování pracovních úrazů. Personální úsek naproti tomu zajišťuje smluvního lékaře pracovně-lékařské péče a dohlíží nad prováděním pravidelných lékařských prohlídek, vyšetření a očkování zaměstnanců, poskytuje nově přijímaným zaměstnancům všeobecné informace o bezpečnosti práce v podniku (nejlépe ústně doplněné o písemně zpracované podklady), informuje dotčené osoby o změnách v personálním obsazení na jednotlivých pracovištích (např. o nově přijatých zaměstnancích, o zaměstnancích

převedených na jinou práci apod.), komunikuje a projednává jménem zaměstnavatele příslušné náležitosti s odbory a vysílá svého zástupce do komise pro odškodňování pracovních úrazů a do komise provádějící komplexní bezpečnostní prověrku. Provozní (správní) úsek pak zajišťuje technickou a materiální podporu, údržbu zařízení, úklid, nákup a vydávání OOPP zaměstnanců apod. a vysílá svého zástupce do komise pro odškodňování pracovních úrazů a do komise provádějící komplexní bezpečnostní prověrku. Dalším důležitým článkem jsou odbory, jejichž účast by měla být aktivní a měla by vést k pozitivní spolupráci se zaměstnavatelem, především s nejvyšším managementem. Účelem funkce odborů by mělo být nalézání shody s vrcholovým managementem, a to v takovém smyslu, aby byly odstraněny všechny prvky případné diskriminace či znevýhodňování jednotlivců nebo skupin, a ve všeobecné míře hájeny a rozvíjeny zájmy i potřeby zaměstnanců. Prioritami by tedy v žádném případě nemělo být vydírání zaměstnavatele, pořádání stávek či protestů a pouze předstíraný zájem o hájení práv zaměstnanců, jakožto zástěrka pro uplatňování svých vlastních zájmů. Ovšem také zaměstnavatelé, především vrcholový management, by měli brát odbory jako žádoucího partnera a nikoli jen jako partnera trpěného, považovaného za přežitek doby. Takový přístup vede totiž k polarizaci vztahů uvnitř podniku, což není ku prospěchu ani žádné ze zainteresovaných stran, ani společnosti jako celku (Skřehot, 2007).

V systému řízení BOZP se nesmí zapomínat také na vedoucí pracovníky napříč celou hierarchií řízení firmy. Podle zákoníku práce (viz § 101, odstavec 2) totiž péče o zajišťování BOZP tvoří nedílnou a rovnocennou součást pracovních povinností vedoucích zaměstnanců na všech stupních řízení v rozsahu jejich povinností. V tomto duchu tedy největší břímě odpovědnosti leží na statutárním zástupci firmy, obvykle jednatelem či ředitelem. Ovšem fyzicky by se prevence měli zúčastňovat především vedoucí na nižších stupních řízení, zejména vedoucí výrobních úseků, kde se vyskytuje obvykle nejvíce problémů a pracovních rizik. Jejich všímavost a průběžná komunikace s podřízenými zaměstnanci na straně jedné a předávání zjištěných skutečností osobě odborně způsobilé a zástupcům provozního úseku by měl tvořit jejich hlavní přínos do systému řízení bezpečnosti. Tito vedoucí by také měli provádět pravidelné školení svých podřízených o BOZP a o rizicích na jejich pracovištích, přezkušovat jejich znalosti a průběžně kontrolovat dodržování předpisů (včetně používání OOPP zaměstnanci).

Pro management BOZP platí následující zásady:

- Bezpečnost by měla být nedílnou součástí podnikatelských činností daného podniku. To zahrnuje rozvoj kultury bezpečnosti podniku, jakož i odpovídajících interních bezpečnostních přístupů a postupů včetně zajištění jejich používání zaměstnanci na všech úrovních podniku.
- Každodenní řízení bezpečnosti by mělo být odpovědností vedoucích pracovníků, aby zajistili bezpečný provoz každého zařízení.

- Vedoucí pracovníci přímého řízení by měli zajistit, aby byly pro každé zařízení vytvořeny provozní postupy a návody nezbytné pro jeho bezpečný provoz.
- Hlavní odpovědností vedoucích pracovníků by mělo být takové obsazování nebezpečných zařízení obsluhou, aby bylo zajištěno jeho bezpečné provozování v kteroukoli dobu. Vedoucí pracovníci by měli přijmout všechna reálná opatření pro zajištění toho, aby každý zaměstnanec na nebezpečném zařízení, včetně dočasných zaměstnanců (brigádníků) a smluvních subdodavatelů, dostal přiměřené informace jak o běžných provozních, tak i abnormálních podmínkách provozu daného zařízení.

Systém managementu BOZP vychází z poznatků zjištěných při úvodním přezkoumání a měl by obsahovat tyto hlavní prvky:

- Politika.
- Organizační zajištění.
- Plánování a realizace (tj. naplánování, zavedení a udržování v praxi).
- Vyhodnocování (na základě provádění kontrol a měření).
- Opatření ke zlepšení (na základě vyhodnocování a přezkoumání).

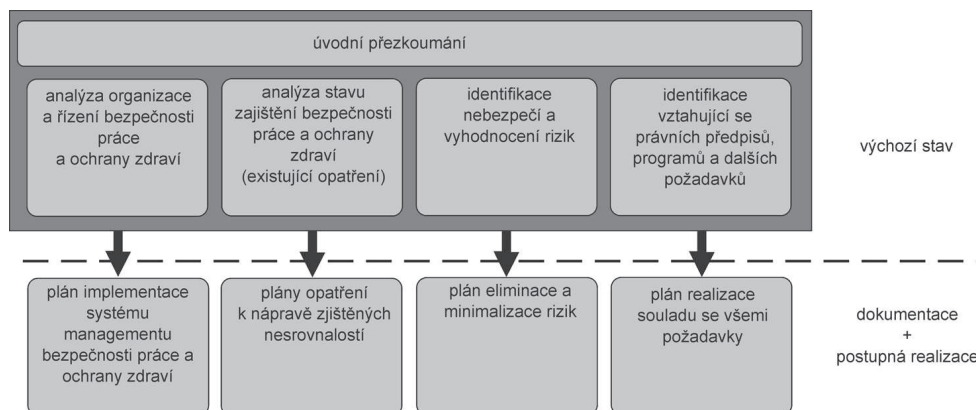
Takto vytvořený systém řízení BOZP by měl být integrován do celkového řízení organizace.

Úvodní přezkoumání

Při úvodním přezkoumání je hodnocen současný stav řízení a zajištění BOZP v podniku a existující opatření. V návaznosti na zjištěný „výchozí stav“ se plánují konkrétní činnosti vedoucí k vyšší efektivitě řízení a úrovni zajištění bezpečnosti a ochrany zdraví zaměstnanců. Schematicky úvodní přezkoumání popisuje obrázek 132.

Politika BOZP

V rámci stanovení systému řízení BOZP musí organizace definovat celkový přístup k řešení BOZP. Tento přístup nebo strategie v oblasti zajištění BOZP bývá označován jako politika BOZP. To zahrnuje prohlášení o celkových (strategických) cílech a zásadách v oblasti BOZP, popis opatření a organizační struktury, odpovědností a zdrojů potřebných k dosažení daných cílů. Definování této politiky není přímočarým úkolem. Vedoucí pracovníci jsou nuceni dávat do souvislosti zdroje potřebné k naplnění stanoveného přístupu k řešení bezpečnosti a finanční podmínky podniku.



Obrázek 132: Schematické znázornění úvodního přezkoumání.

Zaměstnavatel musí zformulovat politiku BOZP, která by měla být:

- Specifická pro danou organizaci a přiměřená její velikosti a charakteru činnosti a rizik.
- Stručná, srozumitelně formulovaná, opatřená datem, její platnost by měla být stvrzena podpisem nebo prohlášením zaměstnavatele.
- Uvedena ve známost všem zaměstnancům, kterým by měla být snadno přístupná na jejich pracovišti.
- Vyhodnocována z hlediska trvalé přiměřenosti.
- Dle potřeby přístupná všem externím zainteresovaným stranám.

V Politice BOZP by se měla organizace zavázat k dodržování minimálně těchto základních zásad a cílů:

- Bezpečnosti a ochrany zdraví všech příslušníků organizace předcházením vzniku pracovních úrazů, nemocí z povolání a nehod na pracovišti.
- Dodržování příslušných právních předpisů k zajištění BOZP, plnění dobrovolných programů, kolektivních smluv a dalších požadavků, ke kterým se organizace zavázala.
- Zajištění, aby zaměstnanci a jejich zástupci byli konzultováni a vyzýváni k aktivní spoluúčasti na všech prvcích systému managementu BOZP.
- Neustálé zvyšování úrovně bezpečnosti a systému managementu BOZP.

Plánování

Účelem plánování je pomocí postupných kroků a konkrétně stanovených cílů vytvoření systému managementu BOZP, který bude jako minimum podporovat dodržování platných právních předpisů, zahrnovat všechny základní prvky systému managementu BOZP a směřovat k neustálému zvyšování úrovně bezpečnosti.

Organizace musí přijmout opatření zajišťující vhodné a přiměřené plánování opatření a cílů v oblasti BOZP založené na výsledcích úvodního a dalších přezkoumání nebo na jiných dostupných údajích. Toto plánování by mělo přispívat ke zlepšování bezpečnosti a ochrany zdraví zaměstnanců a mělo by zahrnovat:

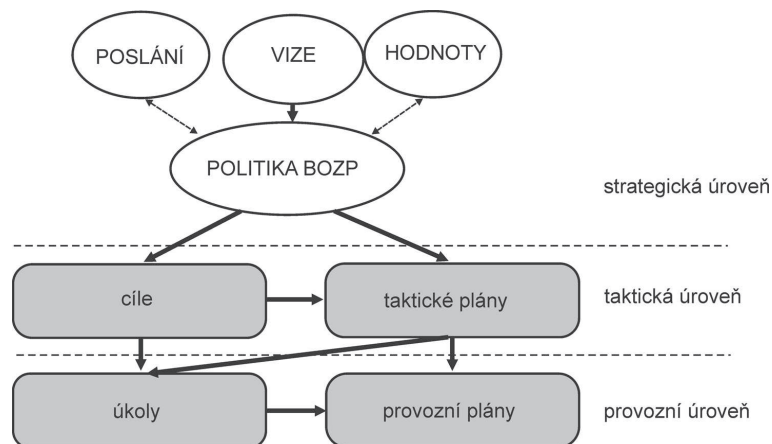
- Jasnou definici cílů BOZP organizace včetně stanovení priorit popř. kvantifikace.
- Vypracování plánu k dosažení každého cíle se stanovením odpovědností, termínů plnění a ukazatelů plnění stanoveného cíle, které jsou vždy hmatatelným důkazem toho, že cíl byl splněn.
- Výběr hodnotících kritérií, která mají prokázat splnění stanoveného cíle, obvykle se jedná o exaktní hodnotu, které má být splněním daného cíle dosaženo (např. počet pracovních úrazů za rok).
- Zabezpečení přiměřených zdrojů nezbytných pro splnění stanovených cílů – materiální, finanční, lidské.

Cíle BOZP

V souladu s politikou BOZP a na základě výchozího a dalších přezkoumání stanovuje zaměstnavatel cíle organizace v oblasti BOZP, které by měly být:

- Specifické pro danou organizaci a přiměřené její velikosti a charakteru prováděných činností a zejména existujícím rizikům.
- V souladu s platnými právními předpisy, jakož i s technickými a obchodními povinnostmi organizace souvisejícími s BOZP.
- Zaměřeny na neustálé zlepšování bezpečnosti a ochrany zdraví zaměstnanců.
- Měřitelné, reálné a dosažitelné.
- Dokumentovány a oznámeny všem příslušným funkcím a úrovním organizace.
- Pravidelně vyhodnocovány a aktualizovány.

Návaznost strategie, politiky, plánování a cílů BOZP ilustruje obrázek 133.



Obrázek 133: Schéma plánování v rámci systému managementu bezpečnosti.

Organizace

Organizaci lze rozdělit na čtyři základní kroky:

- Organizační zajištění.
- Odpovědnosti a pravomoci.
- Odbornou způsobilost, školení, výcvik.
- Komunikace.

K jednotlivým krokům blíže.

Organizační zajištění

Za zajištění bezpečnosti a ochrany zdraví při práci vrcholově odpovídá zaměstnavatel. Podle § 102, odstavce 1 zákona č. 262/2006 Sb., zákoník práce, je zaměstnavatel povinen vytvářet bezpečné a zdravé neohrožující pracovní prostředí a pracovní podmínky vhodnou organizací bezpečnosti a ochrany zdraví při práci, kterou může být například zavedení systému managementu BOZP podle požadavků národních a mezinárodních norem a programů a přijímáním opatření k předcházení rizikům.

Odpovědnosti a pravomoci

Vhodným prostředkem k uplatňování pravidel řízení BOZP je na úrovni nejvyššího vedení jmenování osoby s odpovědností, povinnostmi a pravomocí pro:

- Rozvoj, uplatňování, pravidelné přezkoumávání a vyhodnocování systému managementu BOZP.

- Pravidelné informování nejvyššího vedení o stavu systému managementu BOZP.
- Zajišťování spoluúčasti všech příslušníků organizace.

V rámci organizačního zajištění BOZP by měla organizace určit odpovědnosti, povinnosti a pravomoci pro vývoj a uplatňování systému managementu BOZP a dosahování stanovených cílů BOZP. Je tedy nezbytné stanovit základní struktury a postupy, které:

- Delegují odpovědnosti za BOZP a pravomoci na vedoucí pracovníky na všech úrovních řízení.
- Definují odpovědnosti, povinnosti a pravomoci vybraných osob pro provádění identifikace nebezpečí, vyhodnocování a kontrolu rizik.
- Zabezpečí účinný dozor nad zajištěním BOZP.
- Podpoří spolupráci a komunikaci mezi jednotlivými pracovníky na různých úrovních v podniku.
- Stanoví a budou uplatňovat jasnou politiku BOZP a měřitelné cíle.
- Vytvoří podmínky pro identifikaci nebezpečí a eliminaci nebo omezení rizik spojených s pracovními činnostmi.
- Budou realizovat programy prevence a podpory ochrany zdraví.
- Vytvoří vhodné podmínky pro účast zaměstnanců a jejich zástupců při naplňování politiky BOZP.
- Poskytnou přiměřené zdroje k zajištění stanovených úkolů v oblasti BOZP.

Důležitým prvkem systému managementu BOZP v organizaci je účast zaměstnanců. Podle § 108 zákona č. 262/2006 Sb., zákoník práce, mají zaměstnanci právo účastnit se na řešení otázek souvisejících s BOZP. Pokud v organizaci není k tomuto účelu zřízena odborová organizace nebo stanoven zástupce zaměstnanců, musí být dané otázky projednány přímo s každým zaměstnancem. Zaměstnavatel by měl zajistit, aby záležitosti týkající se BOZP byly konzultovány se zaměstnanci a jejich zástupci a všichni zaměstnanci byli školeni a dostatečně informováni o všech aspektech BOZP, které jsou spojeny s jejich prací. K tomu jim musí vytvořit vhodné podmínky (z hlediska času, potřebných zdrojů atd.).

Odborná způsobilost, školení, výcvik

V organizaci musí být přijata opatření zajišťující příslušnou odbornou způsobilost všech osob s ohledem na aspekty bezpečnosti a ochrany zdraví v rámci jejich úkolů a odpovědností. Zaměstnavatel musí být schopen odpovědně přistoupit k problematice identifikace nebezpečí a hodnocení rizik spojených s pracovními činnostmi a uplatňovat systém managementu BOZP. Za tímto účelem stanoví zá-

kon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci, podmínky způsobilosti a odborné způsobilosti k zajišťování a provádění úkolů v hodnocení a prevenci rizik možného ohrožení života nebo zdraví zaměstnanců.

Základní charakteristiky programů školení jsou následující:

- Zahrnutí všech příslušníků organizace.
- Řízení odborně způsobilými osobami.
- Zabezpečení účinného a včasného vstupního i periodického školení.
- Zahrnutí postupů pro vyhodnocování úplnosti a účinnosti školení.
- Pravidelné přezkoumávání k zajištění jejich aktuálnosti, přiměřenosti a účinnosti.
- Dokumentace s ohledem na velikost a charakter činnosti organizace.
- Poskytnutí bezplatného školení všem účastníkům, pokud možno v pracovní době.

Komunikace

Nezbytnou součástí řízení BOZP jsou základní pravidla pro komunikaci a informování o záležitostech týkajících se BOZP v rámci organizace i s externími subjekty a zainteresovanými stranami. Je tedy nezbytné zavést a dodržovat opatření a postupy pro:

- Přijímání i vydávání, dokumentování a včasné vyřizování interních a externích sdělení týkajících se BOZP.
- Zajištění interní komunikace v oblasti BOZP v rámci organizace, na různých úrovních řízení a mezi nimi navzájem.
- Zajištění, aby byly přijímány, projednávány a vyřizovány upozornění, podněty a připomínky týkající se BOZP předkládané zaměstnanci a jejich zástupci.

Jedná se např. o udržování systému porad na různých úrovních řízení, zavedení knihy stížností nebo schránky na anonymní podněty, připomínky a návrhy, pro externí komunikaci vytvoření komunikačního standardu upravujícího pravidla a podmínky BOZP, které musí být součástí smluv atd.

Dokumentace

V závislosti na velikosti a charakteru činností organizace je třeba zavést a udržovat dokumentaci systému managementu BOZP, která by měla zahrnovat:

- Politiku (strategii) a cíle BOZP organizace.

- Stanovené hlavní úlohy a odpovědnosti při uplatňování systému managementu BOZP.
- Významná rizika v oblasti BOZP spojená s činnostmi organizace a opatření pro jejich prevenci a omezení.
- Dohody, postupy, pokyny a další interní dokumenty použité v rámci systému managementu BOZP.

Dokumentace systému managementu BOZP by měla být jasně sestavena a prezentována způsobem srozumitelným všem osobám, které ji mají používat, musí být pravidelně přezkoumávána a v případě potřeby revidována.

Podle potřeb organizace by měly být lokálně vedeny a řízeny záznamy BOZP, jejichž základní typy jsou následující:

- Záznamy spojené s uplatňováním systému managementu BOZP.
- Záznamy o pracovních úrazech, nemocech z povolání a nehodách.
- Záznamy spojené se zákony nebo právními předpisy týkajícími se BOZP.
- Záznamy o expozici zaměstnanců a jejich zdravotním stavu.
- Výsledky monitorování.

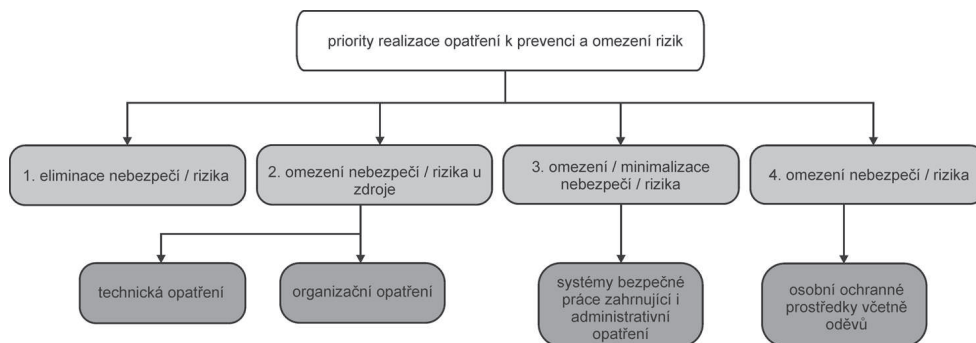
Zaměstnanci by měli mít právo přístupu k záznamům, které se týkají jejich pracovního prostředí a zdraví, při respektování jejich důvěrnosti. Dokumentace systému managementu BOZP by měla prokázat, že je v organizaci systém managementu BOZP zaveden. Záznamy by pak měly dokladovat, že je systém uplatňován, udržován a že je funkční.

Opatření k prevenci a omezení rizik

V rámci systému managementu BOZP je třeba průběžně identifikovat nebezpečí a hodnotit rizika, která mohou ohrozit bezpečnost a zdraví zaměstnanců. Na základě výsledků hodnocení rizik se pak stanovují další nutná opatření. Opatření k prevenci a omezení rizik by měla být uplatňována v určitém pořadí podle legislativně určených priorit, jak ilustruje obrázek 134.

Postupy prevence a omezení nebezpečí v rámci celkového managementu bezpečnosti by měly:

- Být přizpůsobeny nebezpečím a rizikům, které v organizaci existují.
- Být pravidelně přezkoumávány a upravovány.
- Být v souladu s platnými právními předpisy a odrážet správnou praxi.



Obrázek 134: Schematické znázornění priorit při realizaci opatření k prevenci a omezení rizik.

- Respektovat současný stav znalostí včetně informací nebo zpráv z organizací jako jsou např. inspektoráty práce.

Základní kroky těchto postupů stručně uvádí tabulka 49.

Při volbě bezpečnostních opatření by se mělo vycházet z následujících zásad:

- Je-li to možné, je třeba vyloučit nebezpečí přímo u zdroje, např. náhrada nebezpečné chemické látky méně nebezpečnou látkou.
- Nelze-li vyloučit nebezpečí, je třeba jej omezit, např. užitím nízkonapěťového napájení.
- Kde je to možné, přizpůsobit práci individuálním schopnostem pracovníků.
- Využít nové, moderní postupy pro zlepšení bezpečnosti.
- Preferovat kolektivní ochranné prostředky.
- Využívat kombinace technických a organizačních opatření.

Přitom bychom měli vzít v úvahu:

- Potřebu zavedení plánované údržby.
- Osobní ochranné prostředky a jejich posouzení z hlediska vhodnosti.
- Havarijní opatření, včetně havarijních a evakuačních plánů.
- Preventivní opatření a způsoby monitorování nebezpečných/rizikových situací.

Tabulka 49: Přehled postupů prevence a omezení nebezpečí v rámci celkového managementu bezpečnosti.

Stanovení rámce, kontextu	Tento krok znamená výběr posuzovaného systému (objektu) a stanovení rozsahu. To je vymezení objektu, systému, u kterého se budou rizika posuzovat (stroj, zařízení, pracoviště, činnost, materiál, látka aj.) a o formulaci kritérií, ke kterým budeme riziko vztahovat (systémové selhání, nehoda, úraz, či jiné poškození zdraví aj.). Při posuzování rizik spojených s pracovní činností je důležité uvažovat nejen běžný pracovní proces, ale i mimořádné situace a činnosti.
Identifikace nebezpečí	Jedná se o identifikování zdrojů možného ohrožení zdraví, majetku, životního prostředí apod. Důležitým zdrojem informací pro tento krok je evidence událostí, které v minulosti nastaly. U nich by měly být uvedeny i zdroje, které se na vzniku události a příslušných následcích podílely. V případě, že tyto informace nejsou k dispozici nebo jsou nedostatečné, je třeba použít některou z metod umožňujících zdroje nebezpečí identifikovat. Jedná se např. o kontrolní seznamy, Co – kdyby (What-if), strom chyb, strom poruch apod. Jedná se o identifikování toho, co, proč a jak může při pracovních činnostech nastat. Tyto údaje tvoří základní vstupní data pro další analýzu.
Analýza rizik	Tato část obnáší rozbor rizik z hlediska možných následků a reálné pravděpodobnosti jejich vzniku v kontextu s existujícími opatřeními. Analýza by měla zahrnovat celý rozsah potenciálních následků a pravděpodobností, s jakými tyto následky mohou nastat. Kombinací pravděpodobnosti a závažnosti potenciálního následku získáme úroveň (míru) příslušného rizika. Analýza rizik by měla zobrazovat především: • systematickou identifikaci možných selhání, nehod a poruch včetně vyjádření výsledků, • kvantitativní nebo alespoň semi-kvantitativní vyjádření míry rizika, • vyhodnocení možných řešení směřujících ke snížení rizika, • identifikaci faktorů, které se na iniciaci rizika podílejí a které k němu přispívají včetně systémových nedostatků a kritických míst. Výsledky analýzy rizik jsou pak podkladem pro rozhodování, zda je riziko možno přijmout / tolerovat, či zda jej musíme snížit. V tom případě výsledky analýzy využijeme pro výběr vhodných opatření ke snížení nebo eliminaci rizik.
Hodnocení rizik	Tento krok spočívá ve srovnání námi vypočtené (vyjádřené) hodnoty míry rizika s předem stanovenými kritérii. S ohledem na všechna existující opatření pak lze vyhodnotit, zda riziko je nebo není přijatelné. Jestliže výsledné riziko je nižší než stanovená hodnota přijatelného rizika, není obvykle třeba další snižování rizika, ale tato rizika stále sledujeme, aby zůstala pod hranicí přijatelnosti. V případě, že hodnota rizika je nad nebo na hranici přijatelnosti, je nezbytné přijmout taková opatření, která by vedla ke snížení rizika pod mez přijatelnosti. Na základě toho můžeme stanovit priority dalších aktivit a rozhodnout o přijetí adekvátních bezpečnostních opatření.

Řízení rizik	Systémová bezpečnost používá široce akceptované priority jak zvládnout nebezpečí: • eliminovat zdroje rizik (skutečná bezpečnost), • redukovat (omezit) nebezpečí/rizika, • zvládnout rizika, • lokalizovat a zmírňovat škody, • sledování přijatelných rizik, realizace vhodných opatření ke snížení nepřijatelných rizik. Jakmile je nebezpečí jednou identifikováno a jsou vyhodnocena rizika s ním spojená, musí být nejvyšší prioritou jejich eliminace nebo jejich spolehlivá kontrola.
Monitoring	Monitoring má za cíl dokumentovat: • způsob a četnost prováděného posuzování a hodnocení rizik, • výsledky auditů a ostatních nástrojů monitoringu, • přijatá opatření ke snížení rizik, způsob a výsledek jejich implementace. Je nezbytné průběžné a trvalé sledování rizik a změn, které mohou tato rizika ovlivnit.
Informování	Protože i po realizaci opatření k omezení rizika většinou určitá reziduální (zbytková) rizika zůstávají, je povinností zaměstnavatele o těchto rizicích informovat všechny dotčené osoby a subjekty. Informování dotčených osob o procesu řízení rizik a o rizicích, která nejsou akceptovatelná a o přijatých opatřeních na jejich snížení je důležitou součástí řízení rizik na všech úrovních.

Bezpečnostní opatření je třeba posuzovat z hlediska jejich účinnosti. K tomu mohou pomoci následující otázky:

- Bude revidovaný řídicí systém vést k dosažení přijatelné úrovně rizika?
- Jsou vytvářena nová nebezpečí?
- Bylo vybráno nejúčinnější řešení i z hlediska ekonomického?
- Co si lidé dotčení novými opatřeními o nich myslí?
- Budou opatření uplatněna a nikoliv ignorována např. v důsledku tlaku na pracovní výkon?

Řízení provozu

Proces řízení provozu představuje konkrétní způsob řízení jednotlivých potenciálních zdrojů rizik (tj. činností, zařízení, látek, materiálů a produktů atd.), resp. stanovení provozních nástrojů jejich řízení. Vycházíme tedy z identifikace nebezpečí a hodnocení rizik, při němž by mělo být zohledněno především následující:

- Běžné a mimořádné činnosti (normální provoz, různé druhy odstávek, údržba atd.).

- Činnosti všech osob, které mají na pracoviště přístup (včetně návštěv, externích pracovníků, pracovníků provádějících kontroly, inspekce nebo audity apod.).
- Všechna zařízení a stroje, infrastruktura, vybavení, materiály a produkty na pracovištích.
- Lidské chování a způsobilost.
- Identifikovaná nebezpečí vznikající mimo pracoviště, která mohou negativně ovlivnit bezpečnost a ochranu zdraví na pracovišti.

Pro konkrétní potenciální zdroje rizik by pak měl být stanoven způsob jejich řízení prostřednictvím tzv. bezpečných postupů., tj. postupů a pravidel pro bezpečné provádění stanovených činností s ohledem na potenciální rizika. Jedná se především o:

- Návodů k obsluze.
- Pracovní a technologické postupy.
- Pokyny pro bezpečnou manipulaci se zařízeními a stroji, pro jejich údržbu, četnost kontrol a revizí, pokyny pro případnou výměnu součástí atd.
- Místní provozní bezpečnostní předpisy.
- Provozní řády.
- Pracovní řády.
- Individuální pokyny a pravidla zaměstnavatele pro bezpečné provádění činností.
- Instrukce týkající se pracovních podmínek a pracovního prostředí.

Tyto postupy musí být zdokumentovány, musí být udržovány v aktuálním stavu a dostupné na příslušných pracovištích.

Řízení změn

Důležitým prvkem řízení BOZP je sledování a vyhodnocování dopadů změn na zajištění BOZP v organizaci a ještě před jejich vznikem přijmout vhodná preventivní opatření. Příklady změn, které mohou ovlivnit bezpečnost, uvádí tabulka 50.

Před jakoukoli úpravou nebo zavedením nových pracovních metod, materiálů, procesů nebo strojního zařízení je třeba provést identifikaci nebezpečí na pracovišti a hodnocení rizika. Toto hodnocení by mělo být provedeno v konzultaci a ve spolupráci s příslušnými zaměstnanci a jejich zástupci. Na základě provedení změny je třeba zajistit, aby byli řádně informováni a vyškoleni všichni příslušníci organizace, jichž se změna dotýká, a aby byla provedena aktualizace související dokumentace.

Tabulka 50: Příklady vnitřních a vnějších změn s možným vlivem na bezpečnost.

Příklady vnitřních změn	Příklady vnějších změn
Změny v personálním obsazení	Změny v legislativě
Změny v důsledku zavedení nových procesů nebo technologií	Fúze organizací
Změny pracovních postupů nebo organizace práce	Rozvoj poznatků o provozovaných činnostech a používaných technologiích
Změny organizační struktury nebo počtu zaměstnanců	Vývoj v přístupech k BOZP

Předcházení haváriím, havarijní připravenost a zásahy

Každá organizace musí být dostatečně připravena na možný vznik havárie, proto je v rámci systémového řízení bezpečnosti třeba zavést a dodržovat opatření pro předcházení haváriím a pro havarijní připravenost a zásahy. Tato opatření by měla zahrnovat:

- Identifikaci potenciálu vzniku nehod a havárií.
- Stanovení adekvátních preventivních opatření.
- Stanovení vhodných opatření a zajištění prostředků pro účinnou reakci na vzniklou havárii.

V rámci těchto opatření by mělo být zajištěno následující:

- Dostupnost informací, interní komunikace a koordinace na pracovištích v případě havárie.
- Způsob informování a komunikace s příslušnými orgány, okolními subjekty, tísňovými službami, atd.
- Způsob zajištění první pomoci, lékařské pomoci, likvidace požáru a evakuace všech osob na pracovišti.
- Informování a školení všech pracovníků organizace, včetně pravidelných cvičení postupů pro předcházení haváriím a havarijní připravenosti a zásahů.

Nákup zboží a služeb, vztahy s dodavateli

Při řízení BOZP v organizaci je třeba zavést a dodržovat postupy zajišťující, aby:

- Byla identifikována a vyhodnocována shoda s požadavky na zajištění BOZP kladenými na organizaci a plnění těchto požadavků se promítalo do podmínek nákupních a leasingových smluv.

- Před nákupem zboží a služeb byly identifikovány příslušné národní zákony a právní předpisy, jakož i vlastní požadavky organizace.
- Byly vytvořeny podmínky pro dosažení souladu s požadavky před použitím těchto zboží a služeb.

V souvislosti implementací systému managementu BOZP je nezbytné uzavřít a udržovat dohody, které zajistí dodržování stanovených požadavků v oblasti BOZP ze strany dodavatelů a jejich zaměstnanců. Dohody s dodavateli, kteří pracují v areálu organizace, by měly:

- Zahrnovat kritéria BOZP v postupech pro hodnocení a výběr dodavatelů.
- Před zahájením prací stanovit účinnou trvalou komunikaci a koordinaci mezi příslušnými rovinami organizace a dodavatele, včetně ustanovení týkajících se oznamování nebezpečí a opatření k jejich prevenci a omezení.
- Zahrnovat opatření pro hlášení pracovních úrazů, nemocí z povolání a nehod zaměstnanců dodavatele během provádění prací pro organizaci.
- Zajistit, aby dodavatelé a jejich zaměstnanci byli před zahájením prací a podle potřeby i v jejich průběhu informováni a školeni o nebezpečích a možných rizicích ohrožení bezpečnosti a zdraví na pracovišti.
- Zajistit pravidelné monitorování úrovně BOZP u činností dodavatele v lokalitě organizace.
- Zajistit, aby dodavatelé respektovali postupy a opatření BOZP v lokalitě organizace.

Monitorování a měření úrovně BOZP

Pro zajištění účinnosti a efektivity systémového řízení BOZP je třeba vyvinout a provádět monitorování, měření a zaznamenávání úrovně BOZP. Rovněž je třeba stanovit pro toto monitorování odpovědnosti, povinnosti a pravomoci. Cílem monitorování je zabezpečení:

- Zpětné vazby ohledně úrovně BOZP.
- Dostupnosti informací umožňujících stanovit, zda se každodenně účinně uplatňují opatření pro identifikaci, prevenci a omezení nebezpečí a rizika.
- Základu pro rozhodování v oblasti zlepšování procesů identifikace nebezpečí a omezování rizik a celkové rozhodování v rámci systému managementu BOZP.

Monitorování a měření úrovně BOZP by mělo:

- Sloužit jako prostředek ke stanovení rozsahu naplňování politiky a cílů BOZP a omezování rizik.
- Zahrnovat aktivní monitorování zahrnující prvky nezbytné pro uplatňování proaktivního řízení:
 - monitorování plnění specifických plánů, programů a stanovených kritérií úrovně a cílů BOZP,
 - systematické kontroly pracovních systémů, objektů, provozů a zařízení,
 - dozoru nad pracovním prostředím včetně organizace práce,
 - dozoru nad zdravotním stavem zaměstnanců, podle potřeby založený na vhodném lékařském sledování zaměstnanců, které umožňuje včasné odhalení známek a symptomů poškození zdraví, s cílem stanovit účinnost opatření k prevenci a omezení nebezpečí a rizik,
 - dodržování platných právních předpisů, plnění kolektivních smluv a dalších závazků týkajících se BOZP, které organizace přijala.
- Zahrnovat reaktivní monitorování zahrnující identifikaci, oznamování a vyšetřování:
 - pracovních úrazů, nemocí z povolání (včetně sledování záznamů o hromadné absenci z důvodu nemoci) a nehod,
 - ostatních ztrát, například škod na majetku,
 - nedostatků v zajišťování BOZP a selhání systému managementu BOZP,
 - programů rehabilitace a obnovy zdraví zaměstnanců.
- Být zaznamenáváno.

Monitorování musí být postaveno na kvalitativních i kvantitativních kritériích, která by měla vycházet z identifikovaných rizik a z politiky a cílů BOZP. Volba ukazatelů úrovně BOZP by se měla řídit jednak velikostí a charakterem provozovaných činností organizace a jednak cíli v oblasti zvyšování úrovně BOZP. Příkladem takových kritérií mohou být ukazatele efektivity BOZP uvedené v následující tabulce 51.

Tabulka 51: Ukazatelé efektivity BOZP.

Ukazatel	Četnost monitorování	Odpovídá
Nežádoucí události (nehody, úrazy, havárie)		Vedoucí výroby
Celkový počet	1 × měsíčně	
Počet evidovaných úrazů s rozdělením dle závažnosti následků	1 × měsíčně	
Počet havarijních situací	1 × měsíčně	
Zjištěné příčiny	2 × ročně	
Kalkulace nákladů a ztrát	2 × ročně	
Počet evidovaných nemocí z povolání	1 × ročně	Technický vedoucí
Počet dnů pracovní neschopnosti	1 × měsíčně	Vedoucí výroby
Počet dnů absence	1 × měsíčně	Vedoucí výroby
Hodnocení kontrol BOZP (jejich četnost, zjištěné nedostatky a jejich náprava)	2 × ročně	Technický vedoucí
Plnění cílů BOZP	2 × ročně	Technický vedoucí
Počet realizovaných opatření (technická / organizační / účinnost)	1 × ročně	Technický vedoucí
Úroveň rizikových faktorů – hluk, prach, chemické látky	1 × ročně	Technický vedoucí
Praktický nácvik havarijní připravenosti a reakce	1 × ročně	Technický vedoucí

Jednou z hlavních monitorovacích činností jsou kontroly:

- Pravidelná kontrola BOZP a PO – na všech pracovištích organizace by se měly pravidelně provádět následující kontroly:
 - vizuální kontrola pracoviště a používaných zařízení obsluhou dle provozní dokumentace, tj. obvykle vždy před začátkem a při ukončení směny,
 - průběžná denní namátková kontrola dodržování požadavků na BOZP a PO a povinností stanovených v rámci systému managementu BOZP vedoucími na všech stupních řízení.
- Preventivní prohlídka BOZP a PO – odborně způsobilá osoba v prevenci rizik provádí pravidelně (např. 1 × za čtvrtletí) preventivní prohlídku zajištění BOZP a PO; z hlediska BOZP se jedná o kontrolu úrovně zajištění BOZP, zejména stavu výrobních a pracovních prostředků, vybavení pracovišť, úrovně rizikových faktorů pracovních podmínek a související dokumentace. V oblasti PO se tato prohlídka provádí formou preventivní požární prohlídky objektů a pracovišť a prověřováním dokladů o plnění povinností stanovených

předpisy o PO. O těchto prohlídkách se vyhotovují záznamy do knih kontrol BOZP a Požárních knih.

- Prověrka BOZP – cílem prověrky BOZP je důsledné prověření stávajících rizik a způsobu jejich řízení a prověření shody s požadavky právních a ostatních předpisů k zajištění BOZP. Podrobněji viz dále.

Vyšetřování pracovních úrazů, nemocí z povolání a nehod

Vyšetřování původu a příčin pracovních úrazů, nemocí z povolání a nehod by mělo sloužit k identifikaci případných selhání systému managementu BOZP a zejména jako prevence jejich opakovaného vzniku. Tato povinnost vychází i z požadavků právních předpisů (§ 105 zákona č. 262/2006 Sb., zákoník práce). Vyšetřování by měly provádět kompetentní osoby za přiměřené účasti zaměstnanců a jejich zástupců, přičemž výsledky by měly být dokumentovány. Výsledky vyšetřování by měly být zahrnuty do přezkoumání systému řízení BOZP prováděného vedením organizace. Nedílnou součástí opatření stanovených na základě výsledků vyšetřování nehod a úrazů musí být rovněž úprava dokumentace, proškolení a výcvik dotčených pracovníků, revize hodnocení rizik, příp. návrhy cílů na další období atd.

Prověrka BOZP, hodnocení souladu

Specifickým prvkem systému managementu BOZP je prověrka BOZP, která je jako povinnost uložena zaměstnavateli zákoníkem práce. Z pohledu systému managementu BOZP implementovaného podle normy OHSAS 18001 prověrka BOZP odpovídá prvku zvanému hodnocení souladu.

Jedná se o prověření souladu řízení provozu s požadavky právních a ostatních předpisů k zajištění BOZP. Výstupem je vyhodnocení aktuálního stavu zajištění BOZP, plnění zákonných požadavků a způsobu řízení rizik v organizaci, popis zjištěných nedostatků a doporučení vhodných opatření k jejich odstranění, příp. dalších opatření ke zvýšení úrovně zajištění BOZP. Prověrka BOZP se obvykle provádí formou kontroly zajištění BOZP v provozu a přezkoumání dokumentace BOZP.

Ačkoli povinnost provádět prověrku BOZP není nová a byla zakotvena již v dřívějších právních úpravách zákoníku práce, přesto se ukazuje, že firmy, pokud nemají zaveden systém managementu BOZP, ji příliš neplní. Důvodů, proč tomu tak může být, se nabízí hned několik. Jedním z nich může být skutečnost, že se mnozí zaměstnavatelé mylně domnívají, že se na ně tato povinnost nevztahuje, neboť u nich nepůsobí ani odborová organizace ani není zvolen zástupce zaměstnanců pro oblast BOZP, v jejichž součinnosti či po dohodě s nimi, totiž podle § 108, odstavce 5 zákoníku práce musí být tyto prověrky prováděny.

Druhým důvodem může být skutečnost, že si zaměstnavatelé tento odstavec nesprávně vykládají a považují za prověrku BOZP každou běžnou, namátkovou nebo

i plánovanou kontrolu prováděnou osobou odborně způsobilou v prevenci rizik (tzv. bezpečnostním technikem). Ovšem tento druh kontrolní činnosti vychází z jiného ustanovení zákoníku práce, a to z § 102, odstavce 3, který pojednává o soustavném vyhledávání rizikových faktorů prostředí, zjišťování jejich příčin a o odstraňování identifikovaných zdrojů rizika. Tento bod tedy hovoří o prohlídkách prováděných za účelem prevence rizik a nikoli o komplexním zhodnocení stavu BOZP v podniku. Třetím a patrně nejčastějším důvodem se zdá být skutečnost, že zaměstnavatelé tuto povinnost prostě přehlížejí či cíleně ignorují. Dlužno podotknout, že v případě nedodržení této povinnosti jim totiž nehrozí bezprostředně žádný postih a je bezesporu pravdou, že oproti jiným prohřeškům na úseku bezpečnosti práce, na které se i kontroly inspekčních orgánů mnohem více zaměřují, patří tento mezi mnohem méně závažné. Ano, absence výstražného značení na rizikových místech, nedostatečné zajištění osobních ochranných pracovních prostředků či neprovádění pravidelného výcviku a školení, zaměstnance mnohem více a bezprostředněji ohrožuje na životě a zdraví, avšak neprovádění prověrek bezpečnosti práce může přinášet firmě v konečném důsledku mnohem větší problémy, než se na první pohled jeví (Skřehot, 2007).

Osnova bezpečnostní prověrky

Jelikož neexistuje legislativně stanovený obsah a metodický postup provádění prověrky BOZP, měl by si zaměstnavatel (zastoupený pro tento účel nejlépe pracovní komisí) nejprve stanovit určitou osnovu či harmonogram, podle kterého bude postupováno. Protože je, zvláště pak ve výrobních podnicích, oblast bezpečnosti značně rozsáhlá a komplikovaná (protože se prolíná např. s požární ochranou, hygienou, ergonomií, ochranou životního prostředí atd.), je vhodné si pro účely prověrky BOZP vyhradit určité klíčové oblasti, které budou pro daný rok prioritně kontrolovány (a s ohledem na tuto skutečnost pak do kontrolní skupiny přizvat i příslušné odborníky). V žádném případě ale nesmí být tímto krokem při kontrole opomenuty i ostatní oblasti bezpečnosti, protože by se tím vytratil smysl prověrky, která má být komplexní kontrolou.

Osnovu prověrky je nutno koncipovat jako etapový dokument, který by měl v ideálním případě zahrnovat (Skřehot, 2007):

- Kontrolu dokumentace.
- Fyzickou kontrolu na pracovištích.
- Hodnocení determinant kultury bezpečnosti.
- Analýzu pracovní úrazovosti.
- Závěrečné shrnutí.

1. Kontrola dokumentace

Kontrola dokumentace by měla být co nejširší, neboť v kvalitně zpracované a dobře vedené dokumentaci se odráží celková efektivnost zajištění bezpečnosti. Byť zákoník práce hovoří o povinnosti provádět prověrku na všech pracovištích zaměstnavatele, přesto by fyzická kontrola oproti kontrole dokumentace neměla být přeceňována a upřednostňována. Pracuje-li osoba odborně způsobilá dobře, zejména pak v součinnosti s příslušnými vedoucími jednotlivých úseků, měla by být fyzická kontrola prováděna v celé šíři a hloubce v pravidelných intervalech podle harmonogramu stanoveného interními předpisy organizace. Kontrola dostupnosti, stavu a provádění aktualizace dokumentace BOZP by se měla zaměřit například na dokumenty, jejichž následující výčet je pouze ilustrativní a nikoli úplný (Skřehot, 2007):

- Pracovní řád organizace.
- Dokumentace o evidenci pracovní doby zaměstnanců a jejím rozvržení.
- Dokumentace o provedeném školení vedoucích zaměstnanců z BOZP.
- Dokumentace o provedeném školení zaměstnanců z BOZP.
- Dokumentace o provedeném školení zaměstnanců provádějících vyhrazené nebo specifické práce (obsluha koteln, řidiči motorových vozíků, řidiči služebních vozidel, jeřábníci, svářeči atd.).
- Knihy úrazů a protokoly o vzniku pracovních úrazů (včetně protokolů o odškodňování prováděných komisí, lékařských zpráv atd.).
- Zařazení prací do kategorií podle vyhlášky č. 432/2003 Sb. (Kategorizace prací).
- Analýza a hodnocení rizik.
- Směrnice pro poskytování OOPP a vedení evidenčních karet.
- Návod k obsluze strojů a zařízení.
- Doklady o revizích a zkouškách vyhrazených technických zařízení a ručního elektrického nářadí.
- Doklady o prováděných prohlídkách prostředků pro práci ve výškách a nad volnou hloubkou (žebříků, lešení, plošiny, zábrany proti pádu do hloubky apod.).
- Doklady o posouzení zdravotní způsobilosti zaměstnanců vykonávajících vyhrazené práce (např. řidiči, jeřábníci apod.), včetně zdravotních průkazů zaměstnanců pracujících v závodním stravování.
- Provozní řády (sklady, dílny, garáže, koteln, strojovny výtahů atd.).
- Havarijní a evakuační plány a poplachové směrnice.

- Smlouva o zajištění závodní pracovnělékařské péče, včetně přehledu lhůt periodických preventivních lékařských prohlídek zaměstnanců.
- Kontrolní a provozní knihy (kniha pro provádění svařovacích prací, kniha kontrol BOZP, kniha dozorce výtahu, provozní deník kotelny, deník jízd služebních vozidel apod.).
- Směrnice BOZP (je-li zpracována).
- Protokoly o expozičních měření rizikových faktorů provedených autorizovanou osobou podle zákona č. 258/2000 Sb.
- Traumatologický plán podniku.
- Seznam prací zakázaných ženám a mladistvým.
- Doklady o stavu budov a dalších prostor, zejména doklady o kolaudaci budov, dílen, laboratoří atd., a také stavební plány objektů.

Pro kontrolu dokumentace, jejíž rozsah je vždy závislý na charakteru vykonávaných činností v organizaci, počtu zaměstnanců apod., lze s úspěchem využít nejrůznější kontrolní listy, které značně urychlují práci a usnadňují i následné přezkoumání stavu při další prověrce BOZP. Příkladem může být kontrolní list uvedený v tabulce 52.

Tabulka 52: Vzor kontrolního listu pro provádění kontroly dokumentace BOZP v rámci prověrky BOZP (Skřehot, 2007).

Název dokumentu	Číslo dokumentu	Byl dokument předložen ke kontrole?		Je dokument aktualizován?		Místo uložení dokumentu	Osoba odpovědná za vedení dokumentu (funkce)	Poznámka / opatření
Kniha úrazů pro výrobu OPZ	2007_15/ /OPZ	Ano	Ne	Ano	Ne	Kancelář vedoucího výroby OPZ	Ing. Josef Babka (vedoucí OPZ)	—
Provozní řád skladu hotových výrobků	2005_26/ /OPZ	Ano	Ne	Ano	Ne	Sklad č. 235	Ing. Antonín Mošt (směnový mistr OPZ)	Dokument nebyl aktualizován v souladu se změnou podmínek na pracovišti – dokument nutno aktualizovat do 31.8.2007

2. Fyzická kontrola stavu BOZP na pracovištích

Fyzická kontrola stavu BOZP na pracovištích nemusí vždy představovat komplexní kontrolu všech prostor firmy, nýbrž jen vybraných pracovišť, kde lze očekávat nezávažnější rizika (např. ty, na kterých se vyskytovalo nejvíce zranění a pracovních úrazů v daném roce), nebo vybrané provozy podle zaměření kontroly v daném roce. V takovém případě je nutné, aby byl stav BOZP na daném pracovišti posouzen komplexně, včetně rizik plynoucích z nedostatečného technického, materiálního nebo personálního zajištění, anebo liknavého a nezodpovědného přístupu odpovědných osob spolu se špatným organizačním zajištěním jednotlivých činností. V takovém případě je vždy potřeba zjišťovat pravé příčiny tohoto stavu. V rámci fyzické kontroly by měla komise svou pozornost zaměřit zejména na (Skřehot, 2007):

- Rozmístění, vybavenost a systém využívání nástěnných lékárníček.
- Stav a používání OOPP u zaměstnanců, jimž byly tyto vydány.
- Udržování pořádku na vybraných pracovištích.
- Rozmístění technických zařízení a nábytku na pracovištích z hlediska vhodných ergonomických a stavebně-technických dispozic.
- Dodržování hygienických standardů na vyhrazených místech (např. v závodní kuchyni, jídelně, sauně, sprchách, zdravotním středisku, rehabilitaci apod.).
- Zajištění bezpečnostních požadavků pro skladování nebezpečných látek a materiálů (množství, způsob uskladnění podle druhu a charakteru, dostupnost bezpečnostních listů apod.).
- Nakládání s odpady, tj. systém svozu a likvidace odpadu, třídění apod.
- Technický stav žebříků, lešení, zábran proti pádu do hloubky apod.
- Technický stav komunikací, tj. podlah, schodišť, chodníků, cest, nakládacích ramp, včetně jejich značení, provádění úklidu a údržby.
- Rozmístění (vhodných) bezpečnostních značek a používání bezpečnostních signálů.
- Stav sociálních zařízení s ohledem na udržování čistoty, dostupnost mycích prostředků, provádění úklidu, stavební řešení.
- Stav šaten s ohledem na technický stav lavic a skříněk, dostatečné výměny vzduchu, provádění úklidu.
- Kontrolu garáží s ohledem na množství skladovaných hořlavých kapalin, zajištění skladovaných materiálů (např. pneumatik) proti pádu, zajištění garážových vrat proti samovolnému uzavření, výměna vzduchu, pořádek apod.
- Kontrolu stavu skladovacích regálů, tj. jejich technický stav, skladovaný materiál, nadměrné přetěžování, označení nosností.

- Kontrolu stavu svítidel, osvětlovacích těles a nouzového osvětlení.
- Kontrolu kotelny.
- Kontrolu výtahů (může, ale i nemusí zahrnovat zkoušku vyprošťování uvízlých osob, tu provádí revizní technik).
- Kontrolu svařovacích souprav (stav hadic, jejich délky, barevné provedení a jejich zajištění kroužkovými svorkami, regulačních ventilů, spalovací trysky, pojezdového vozíku, zajištění lahví na vozíku) a uskladnění lahví se stlačenými plyny podle požadavků příslušné ČSN.
- Zhodnocení ergonomických faktorů podle požadavků nařízení vlády č. 361/2007 Sb., například:
 - dostatečného prostoru na jednoho zaměstnance,
 - velikosti pracovní desky a prostoru pro nohy,
 - opracování hran nábytku,
 - použitého materiálu nábytku,
 - vybavení potřebným nábytkem, zařízením a pomůckami a jejich rozmístění na pracovištích,
 - umístění a volby vhodné výpočetní techniky,
 - nastavení velikostí znaků na monitoru PC na minimálně 3 mm,
 - použití vhodného sedadla, tj. s nastavitelnou výškou sedací plochy a opěrek zad a s opěrkami rukou,
 - osvětlení pracovního místa, včetně zástěn proti oslňování,
 - tepelně vlhkostního mikroklima,
 - úrovně hluku,
 - výměny vzduchu, atd.
- Věcné prostředky požární ochrany (jejich množství, rozmístění, doklady o kontrolách a revizích, technický stav).

3. Analýza pracovní úrazovosti

Míra pracovní úrazovosti je odrazem nejen stavu zajištění BOZP na pracovištích ze strany podniku, ale také osobního přístupu jednotlivých zaměstnanců k vlastní bezpečnosti při výkonu pracovních povinností. Zcela logicky tedy bývá vnímána jako reflexe na vzájemnou vazbu zaměstnanec-pracoviště-podnik. Rozbor pracovní úrazovosti by tedy měl tvořit nedílnou součást prověrky BOZP, a to tak, aby byly vyhodnoceny příčiny vzniku úrazů a navržena systémová opatření (např. zlepšení systému výcviku, změna pracovních podmínek, zaměstnanecký motivační program,

technická vylepšení apod.), jejichž účinnost bude po jejich realizaci dále sledována (Skřehot, 2007).

4. Závěrečné shrnutí prověrky

Každá prověrka musí být završena závěrem, který srozumitelným způsobem shrne její průběh, charakter a rozsah sebraných dat, zjištěné nedostatky a navrhovaná opatření (technická i organizační). Nutné je také určit jejich přesná termínová plnění, osoby zodpovědné za jejich provedení a termín následné dohlídky. Ze zjištěného stavu by měla vyplynout také určitá strategie, kterou bude podnik aplikovat ve střednědobém časovém horizontu, za účelem neustálého zlepšování stavu bezpečnosti práce, ochrany zdraví zaměstnanců, pracovního prostředí a celkové kultury bezpečnosti. Tato strategie by se měla také promítnout do písemného prohlášení managementu firmy, tzv. politiky bezpečnosti, která tvoří určitou deklaraci závazků vedení firmy ve vztahu k zaměstnancům.

Audit

Klíčovým prvkem všech formálních systémů managementu je proces auditu. Při auditu zjišťuje kvalifikovaný auditor soulad procesů probíhajících v organizaci (prováděných činností) s požadavky stanovenými normou – v případě systému managementu BOZP např. normou OHSAS 18001. Účelem auditů je získání podkladů pro vyhodnocení, zda je účinně uplatňován systém managementu BOZP a jeho prvky v zájmu bezpečnosti a ochrany zdraví zaměstnanců a předcházení nehodám.

Pro odpovědnou realizaci auditů je třeba stanovit:

- Požadovanou kvalifikaci auditorů.
- Způsob a frekvenci jejich provádění.
- Rozsah.
- Jejich program.
- Metodiku vyhodnocování.
- Způsob prezentace výsledků.

Auditor musí být nezávislý na auditované organizaci, resp. činnosti. Pokud audit není nezávislým procesem, jde o monitorování vedením společnosti. Jsou však různé stupně nezávislosti a ve všech organizacích, s výjimkou těch nejmenších, by bylo možné implementovat systém, využívající auditory, zaměstnané sice v organizaci, ale v jiné části s odlišným vztahem podřízenosti než v auditované části. Toto je definováno jako audit první stranou (interní audit), na rozdíl od externích auditů definovaných jako audit třetí stranou (audit zákazníka u dodavatele je audit druhou stranou).

Audit zahrnuje hodnocení jednotlivých prvků systému managementu BOZP nebo jejich dílčích souborů, tj. jedná se o všechny prvky uvedené v předchozím textu.

Nástroje auditu

Mezi hlavní nástroje auditu BOZP patří:

- Vývojové diagramy podávají názornou formou přehled jednotlivých činností v rámci procesů včetně určení odpovědností za tyto činnosti a pomáhají určit, zda prováděné činnosti v procesu jsou správně zařazeny, nejsou zbytečně opakovány, vedou k požadovaným cílům apod.
- Kontrolní seznamy neboli tzv. check-listy jsou soubory auditních otázek, které slouží jednak jako vodítko auditora pro systematický sběr informací a pro přezkoumání všech souvislostí, a jednak také jako formuláře pro záznamy zjištění, doklady o auditu a nástroje pro vyhodnocení výsledků auditu.
- Záznamy o zjištěních tvoří auditor během a bezprostředně po auditu na základě zjištěných skutečností, a to obvykle ve formě předem stanovených formulářů.

Hlavní cíle auditu

Audit má za cíl:

- Zjistit, zda dokumentovaný systém managementu BOZP, jeho prvky a procesy, prováděné činnosti a pracovní podmínky odpovídají specifikovaným požadavkům normy.
- Ověřit soulad reálných procesů a dokumentovaného systému managementu BOZP.
- Ověřit, zda implementace systému managementu BOZP je účinná, tj. zda systém BOZP plní svůj účel.
- Stanovit účinnost a efektivnost zavedeného systému managementu BOZP s ohledem na plnění stanovených cílů.
- Poskytnout jasnou a přesnou formulaci zjištěných neshod doložených objektivními důkazy.
- Poskytnutí příležitosti prověřované organizace ke zlepšení v dosahované úrovni bezpečnosti (výsledky auditu by měly stimulovat další vývoj systému managementu BOZP).

Výstupy z auditu

Závěry z auditu by měly stanovit, zda systém managementu BOZP, jeho prvky a procesy:

- Jsou účinné pro naplňování politiky a cílů BOZP organizace.
- Jsou účinné z hlediska podpory plné spoluúčasti zaměstnanců.
- Odpovídají výsledkům hodnocení úrovně BOZP z předcházejících auditů.
- Jsou zavedeny v souladu s příslušnými právními předpisy.
- Naplňují cíle neustálého zlepšování a nejlepší praxe BOZP.

Základním výstupem z auditu je zpráva podávající přehled jednotlivých prvků systému řízení a jasný komentář k nim z hlediska aktuálního stavu v organizaci. Komentář se týká zejména silných stránek organizace, požadovaných aktivit pro zvýšení úrovně v auditované oblasti a také příležitostí pro celkové zlepšení systému řízení. Nedílnou součástí zprávy z auditu jsou následující informace:

- Přehled o zjištěných nedostatcích a nalezených neshodách.
- Doporučení ve vztahu ke konkrétním cílům.
- Doporučení ve vztahu k dalšímu rozvoji.
- Podrobnosti vyplývající z auditu ve vztahu k certifikaci.

Auditem se tedy zjistí nedostatky v prověřované oblasti, mezery v celkovém systému managementu a organizačním zajištění řízení a případné následky tzv. „provozní slepoty“. Mimoto mohou být výsledky auditu pro organizaci přínosem zejména z hlediska nalezení nových příležitostí pro:

- Snižování rizik.
- Snižování nemocnosti a úrazovosti.
- Zvýšení kultury bezpečnosti a pracovního prostředí.
- Zlepšení vnitřní komunikace a celkového rozvoje organizace.

Přezkoumání systému managementu BOZP vedením organizace

Základní cíle přezkoumání systému managementu vedením organizace jsou následující:

- Vyhodnocení celkové strategie systému managementu BOZP v souvislosti s naplňováním plánovaných cílů a dosažením požadované úrovně bezpečnosti.

- Vyhodnocení schopnosti systému managementu BOZP splňovat potřeby organizace, zainteresovaných osob a subjektů včetně jejich zaměstnanců.
- Vyhodnocení potřeby změn systému managementu BOZP včetně politiky a cílů BOZP.
- Identifikace potřeb zavedení opatření ke včasnému odstranění nedostatků.
- Poskytnutí zpětné vazby včetně stanovení priorit pro smysluplné plánování a neustálé zlepšování.
- Vyhodnocení pokroku v oblasti plnění cílů BOZP organizace a realizace a účinnosti stanovených nápravných opatření.

V rámci zavedení systému managementu BOZP je třeba stanovit jasná pravidla pro provádění jeho přezkoumání vedením společnosti, jako např.:

- Stanovit frekvenci a rozsah hodnocení prováděných zaměstnavatelem nebo nejvyšší odpovědnou osobou za systém managementu BOZP podle potřeb a podmínek podniku.
- Brát v úvahu výsledky vyšetřování pracovních úrazů, nemocí z povolání a nehod, monitorování a měření úrovně BOZP a auditů.
- Zahrnout do hodnocení doplňkové interní a externí podněty, provedené změny, které by mohly ovlivnit systém managementu BOZP.
- Oznamovat výsledky přezkoumání osobám odpovědným za příslušné prvky systému managementu BOZP, zaměstnancům a jejich zástupcům.

Preventivní a nápravná opatření

Na základě výsledků monitorování a měření účinnosti systému managementu BOZP, auditů a přezkoumání systému managementu BOZP vedením organizace musí být navrhována a realizována nápravná a preventivní opatření. Pro tento proces je třeba v organizaci vytvořit a udržovat podmínky, které by měly zahrnovat:

- Identifikaci a analýzu základních příčin jakékoli neshody s příslušnými předpisy pro BOZP a/nebo s opatřeními systému managementu BOZP.
- Iniciaci, plánování, uplatňování účinné kontroly a dokumentování nápravných a preventivních opatření včetně změn v samotném systému managementu BOZP.

Neustálé zlepšování

Smyslem implementace systému managementu BOZP je jeho neustálé zlepšování a tím zvyšování úrovně bezpečnosti v organizaci. Proto je potřeba průběžně realizovat opatření na základě informací z jednotlivých procesů systému managementu BOZP.

Fungování procesů systému managementu BOZP a úroveň bezpečnosti a ochrany zdraví v organizaci je vhodné porovnávat s výsledky hodnocení a úrovní bezpečnosti v jiných organizacích.

5.5.4 Systém řízení prevence závažných havárií

Systém řízení bezpečnosti ve smyslu PZH je v organizacích implementován na základě zákonné povinnosti. Tato povinnost je dána zákonem č. 59/2006 Sb., o prevenci závažných havárií a vztahuje se na organizace, které nakládají nebo v nichž je umístěna nebezpečná chemická látka v množství vyšším, než je zákonně určené limitní množství.

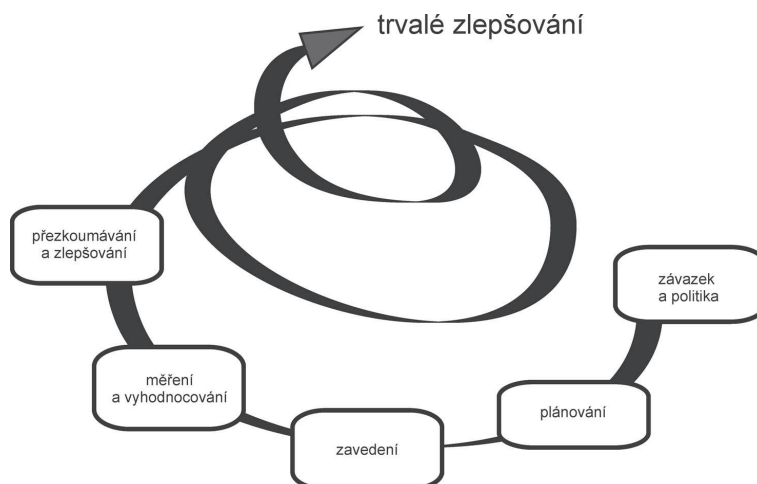
Zákon č. 59/2006 Sb., o prevenci závažných havárií stanoví povinnost zavést systém řízení bezpečnosti pro objekty a zařízení, v nichž je umístěna vybraná nebezpečná chemická látka nebo chemický přípravek, s cílem snížit pravděpodobnost vzniku a omezit následky závažných havárií na zdraví a životy lidí, hospodářská zvířata, životní prostředí, majetek v objektech a zařízeních a v jejich okolí. Základním prováděcím předpisem zákona o prevenci závažných havárií je vyhláška č. 256/2006 Sb., která stanoví podrobnosti systému prevence závažné havárie (PZH) a poskytuje podrobnější informace o zpracování bezpečnostní dokumentace, tj. určuje základní prvky systému řízení bezpečnosti.

Účelem systému řízení bezpečnosti (resp. systému řízení PZH) je postupné snižování množství používaných chemických látek v podniku, prevence vzniku nehod a havárií s účastí nebezpečných chemických látek a také zajištění připravenosti na řešení případných havárií a minimalizaci možných škod.

Systém řízení bezpečnosti je založen na základních procesech a prvcích klasického systémového řízení, se kterými se lze setkat v již zmíněných systémech managementu kvality nebo ochrany životního prostředí podle norem ISO. Jedná se tedy o cyklus několika základních procesů, které neustálým vývojem postupně vedou k trvalému zvyšování úrovně bezpečnosti (viz obrázek 135). Tyto procesy budou podrobněji popsány dále.

Bezpečnostní politika (politika PZH) a zásady PZH

Vedení podniku musí přijmout závazek, že podnik bude směřovat k postupnému zvyšování úrovně bezpečnosti z hlediska nakládání s nebezpečnými chemickými látkami. Tento **závazek** a základní **zásady PZH** musí vycházet z důkladného rozboru aktuálního stavu nakládání s nebezpečnými chemickými látkami a existujících podmínek řízení bezpečnosti. Politika prezentuje strategii společnosti v oblasti prevence havárií a bezpečnosti celkově a stanovuje jasný rámec pro aktivity managementu.



Obrázek 135: Základní prvky systému řízení bezpečnosti (Bernatík, 2006).

Organizace pak tento závazek a zásady PZH deklaruje ve veřejně vyhlášené bezpečnostní politice (resp. politice PZH), např. prostřednictvím intranetu, nástěnek a internetu.

Plánování

Podnik (resp. jeho vedení) musí naplánovat konkrétní **cíle**, kterých chce v oblasti nakládání s nebezpečnými chemickými látkami, zajištění bezpečnosti a prevence rizik dosáhnout, a to jak strategické dlouhodobé, tak i krátkodobé operativní cíle. Podle stanovených základních cílů se podle potřeby zpracovávají programy nebo **plány** PZH pro podnik celkově i pro jednotlivé organizační jednotky zvlášť. Cíle udávají, čeho se má dosáhnout, plány nebo programy pak zahrnují:

- Obsah a časový rámec nezbytný pro dosažení cílového stavu prostřednictvím dílčích konkrétních úkolů.
- Termíny plnění dílčích úkolů a celkových cílů.
- Odpovědnosti pro jednotlivé úkoly a cíle.
- Vyhodnotitelné ukazatele, parametry a kritéria pro hodnocení plnění stanovených úkolů, cílů a účinnosti realizovaných opatření.

Zásady a cíle v oblasti prevence závažných havárií musí vždy sledovat identifikované požadavky, tj. požadavky právních předpisů, očekávání veřejnosti nebo zákazníků apod.

Organizace

V rámci zavedení a realizace systému řízení bezpečnosti je nezbytné stanovit **způsob a organizaci řízení** nakládání s nebezpečnými chemickými látkami. Hlavními prvky tohoto procesu je uspořádání **organizační struktury**, tedy jednoznačné definování pravomocí, povinností a odpovědností v systému řízení bezpečnosti, a to na všech úrovních řízení a v rámci jednotlivých funkcí. To lze následně schematicky znázornit například pomocí tzv. matice odpovědností.

Nezbytnou součástí organizace je také plánování a **řízení potřebných zdrojů** pro realizaci systémového řízení a zavádění potřebných opatření. Jedná se jak o zdroje technické a finanční, tak i o zdroje lidské včetně stanovení způsobu jejich využívání (přerozdělování) a kontroly. Organizace systému řízení bezpečnosti zahrnuje také zabezpečení nezbytných **informačních a komunikačních toků**. Těmi musí být zajištěna dostatečná informovanost všech zaměstnanců o záležitostech, které se jich a jejich činnostech bezprostředně dotýkají z hlediska nakládání s nebezpečnými chemickými látkami, existujících rizik, důležitosti realizovaných opatření atd.

To vše velice úzce souvisí s nutností zajištění odpovídajícího **školení, vzdělávání a výcviku** zaměstnanců v této oblasti včetně jejich **motivace** k dodržování stanovených bezpečných postupů při nakládání s nebezpečnými chemickými látkami. Je tedy důležité stanovit veškerá pravidla týkající se tohoto procesu, např. kvalifikační požadavky pro jednotlivé pracovní pozice (zejm. ty, které mohou ovlivnit úroveň bezpečnosti nebo vznik nehody či havárie), druhy jednotlivých školení a výcviku pro jednotlivé pracovní pozice, četnost provádění školení a výcviku, druhy a způsob provádění praktických nácviků atd.

Jednotlivé prvky a procesy systému řízení bezpečnosti by měly být jasně stanoveny v rámci organizace a jejího celkového řízení, a toto by mělo být popsáno v rámci podnikových organizačně řídicích **dokumentů**. Je třeba si uvědomit, že by měly být popsány jednak bezpečné postupy, tedy způsoby, kterými by měly být činnosti prováděny, aniž by došlo k jakémukoliv ohrožení bezpečnosti zaměstnanců (příp. okolního obyvatelstva, životního prostředí nebo hmotných statků), a jednak také zakázané činnosti a jejich možné důsledky z hlediska bezpečnosti. Do systému dokumentace spadají i **záznamy**, které je nezbytné zpracovávat a udržovat pro jednotlivé prováděné činnosti a procesy v rámci systému řízení bezpečnosti. Jedná se o dokumenty, které prokazují, že stanovené činnosti jsou vykonávány tak, jak je stanoveno. Záznamy, veškerá interní dokumentace a bezpečnostní dokumentace jsou obvykle hlavním podkladem pro orgány státní správy pro objektivní vyhodnocení funkčnosti systému řízení bezpečnosti.

Identifikace nebezpečí, analýza a hodnocení rizik

Jedním ze základních procesů zavedení a realizace systematického řízení bezpečnosti je řízení rizik. Jedná se o sled jednotlivých dílčích kroků:

- identifikace nebezpečí (zdrojů rizik),
- analýza rizik,
- odhad rozsahu možných škod při vzniku nežádoucí události – na zdraví lidí, životním prostředí, majetku vlastním i okolních subjektů,
- výpočet pravděpodobnosti vzniku nežádoucí události,
- hodnocení přijatelnosti rizik,
- stanovení opatření,
- přehodnocení přijatelnosti rizik po realizaci opatření a vyhodnocení jeho účinnosti.

Podrobněji k této problematice viz kapitola 5.2.

Řízení provozu

Základem pro provádění činností při nakládání s nebezpečnými chemickými látkami je stanovení způsobu řízení rizikových provozních činností a potenciálních zdrojů s vlivem na bezpečnost, znečištění ovzduší, vod, půd a vznik odpadů na základě vyhodnocení rizik, což v praxi představují tzv. **bezpečné postupy**. Zaměstnanci musí být s těmito postupy seznámeni, měli by se podílet na jejich tvorbě a vylepšování a měli by je mít na příslušných pracovištích vždy k dispozici. Vedoucí pracovníci jsou povinni jejich dodržování pravidelně kontrolovat, stejně tak jako celkový stav pracovišť.

Nedílnou součástí bezpečného řízení provozu je pravidelné provádění **údržby** zařízení, pro které musí být rovněž stanoveny bezpečné postupy z hlediska možného vzniku havárie nebo jiné nežádoucí události. S prováděním údržby úzce souvisí také prověřování funkčnosti bezpečnostních, výstražných a signalizačních zařízení jak při běžné kontrole, údržbě nebo revizi, tak i v rámci nácviku reakce při vzniku nežádoucí události.

Řízení změn

Organizace musí plánovat veškeré změny a ještě před jejich realizací je posoudit z hlediska bezpečnosti a vyhodnotit možná rizika vzniku nežádoucí události. Podstatné je, aby se následkem realizace jakékoliv změny nezvýšilo riziko vzniku havárie, tudíž by měla být každá plánovaná změna posouzena kompetentními osobami. Jedná se o veškeré plánované změny, tj. změny v:

- technických řešeních,
- technologických procesech,
- SW vybavení,

- personálním obsazení,
- vnějších podmínkách.

Je nezbytné, aby v rámci systému řízení změn byla vždy stanovena odpovědná osoba za plánování a realizaci změny a také za kontrolu její správné realizace. Po provedení změny musí nezbytně následovat úprava dokumentace a proškolení a výcvik dotčených zaměstnanců.

Havarijní plánování

Dalším z procesů zavedení a realizace řízení bezpečnosti je zjišťování možných havarijních situací a stanovení postupů pro jejich zvládnutí. Tato organizace uvádějí ve svých havarijních plánech, které by měly popisovat všechny potenciální havarijní situace, jejich možný rozsah a následky a způsob jejich řešení včetně materiálního zajištění technickými prostředky a lidskými zdroji využitelnými pro omezení dopadů dané havarijní situace. Nedílnou součástí havarijních plánů by měly být nákresy bezpečnostních zón v provozech, únikových cest, evakuačních tras atd.

Havarijní plány by měly být v pravidelných intervalech prověřovány prostřednictvím praktických nácviků, aby bylo možné ověřit a posoudit, zda tyto plány a opatření pro ochranu a zásah k omezení dopadů havárie odpovídají zjištěným havarijním situacím.

Kontrola a audit

V návaznosti na vše dříve uvedené nezbytně nastupuje zásadní krok realizace systémového řízení – sledování plnění programu a **kontrola** dodržování stanovených cílů, úkolů a plánů. Tyto by měly být průběžně plněny, což by mělo být také pravidelně prověřováno. Za tímto účelem si musí organizace stanovit kritéria, podle nichž bude možné plnění vyhodnotit. Pro celý tento proces musí být stanoven postup včetně odpovědného zaměstnance, který za něj bude odpovídat. Tento krok se týká jednotlivých konkrétních úkolů a cílů.

Funkčnost a účinnost zavedeného systému řízení bezpečnosti se prověřuje prostřednictvím **auditu**. Nejedná se o kontrolu konkrétních požadavků, ale prověření existence a vzájemné provázanosti jednotlivých prvků a procesů systému řízení bezpečnosti. Audit je tedy nejen prostředek k nalézání nedostatků v systémovém přístupu, ale také hledání příležitostí ke zlepšení a realizaci nových systémových opatření.

Přezkoumání vedením a trvalé zlepšování

Finálním procesem systému řízení bezpečnosti je jeho přezkoumání vedením společnosti, které si tímto ověřuje, zda závazek, který na začátku učinilo, a politika jsou stanoveny vhodně. Vyhodnocuje reálnost naplnění stanovených závazků a vhodnost stanoveného způsobu jejich realizace. Vedení v rámci tohoto kroku porovnává dosa-

žený stav řízení se stanovenými cíli, zásadami a záměry, vyhodnocuje jej a stanovuje cíle na další období.

Systém trvalého sledování účinnosti opatření pro omezování rizik

Trvalým cílem každého provozovatele by měl být stav „bez havárií“. V bezpečnostní dokumentaci (viz kapitola 5.1.5) musí být uveden popis systému trvalého sledování účinnosti opatření pro omezování rizik. Musí být uvedeno, jak jsou sledována a vyhodnocována opatření pro omezování rizik. Cílovým indikátorem vyhodnocení může být, zda došlo ke snížení rizika (během nějakého časového období) – např. snížení počtu lidí v zóně rizika, snížení dopadů na životní prostředí, snížení pravděpodobnosti havárií, zmenšení zón ohrožení atd. (Ministerstvo životního prostředí, 2007).

Provozovatel by měl trvale zvyšovat bezpečnost procesů. Zejména v případě nových projektů a změn by měl usilovat o eliminaci nebezpečných látek a nebo o jejich náhradu méně nebezpečnými, o snížení množství nebezpečných látek jak v procesu, tak při skladování na nejnižší možnou míru, o výběr takových provozních podmínek nebo podmínek pro nakládání s látkami, které minimalizují riziko, o zavedení dalších ochranných a bezpečnostních bariér, např. konstrukce systému, který vydrží nejhorší možnou havárii bez ztráty své celistvosti, o další doplnění bezpečnostních systémů k zastavení nebezpečné události, o instalaci dalších zadržovacích bariér pro zachycení havarijních úniků, o užití adekvátních bezpečných vzdáleností od zařízení atd. Pomůckou mohou být dvě příručky OECD:

- Návod OECD pro indikátory výkonu prevence [Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response. OECD Environment, Health and Safety Publications Series on Chemical Accidents, No. 11, OECD 2003].
- Základní principy OECD pro prevenci chemických havárií, havarijní připravenost a zásahy [OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response. Guidance for Industry (including Management and Labour), Public Authorities, Communities and other Stakeholders, 2nd ed., OECD Environment, Health and Safety Publications, Series on Chemical Accidents, No. 10, OECD 2003].

5.5.5 Management rizik

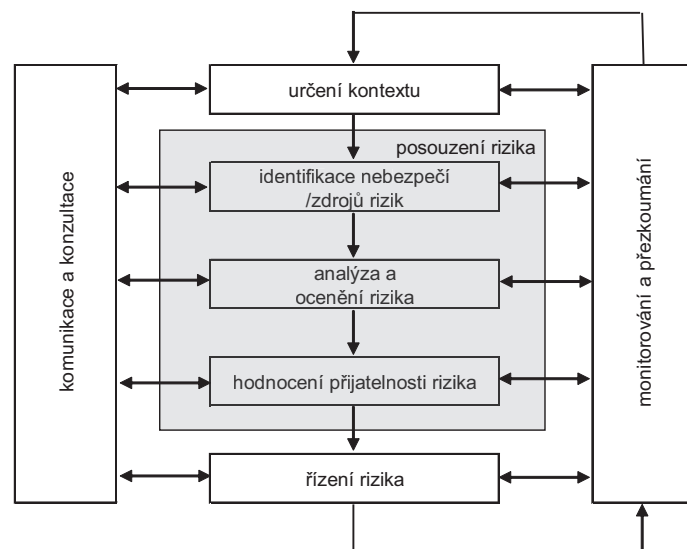
Klíčovou částí řízení bezpečnosti je management rizik. Jeho podstatou je identifikace nebezpečí a analýza a hodnocení rizik, které mohou být ohrožením pro životy a zdraví lidí, majetek nebo životní prostředí. Hlavním smyslem tohoto procesu je určení přijatelnosti rizik a systematická eliminace nebo snížení jednotlivých rizik na přijatelnou úroveň. Celkovým cílem systémů managementu bezpečnosti je postupné a trvalé zvyšování úrovně bezpečnosti.

Management rizik, zejména u velkých organizací, se stal nezbytnou součástí celkového řízení organizace. Důvodem je především skutečnost, že veškeré procesy, které v organizaci probíhají, jsou náhodného charakteru, a přes veškerou péči, kterou podnikatelský subjekt řízení průmyslového provozu věnuje, není schopen vyloučit řadu nežádoucích situací, které jeho podnikání ohrožují. Jedná se např. o:

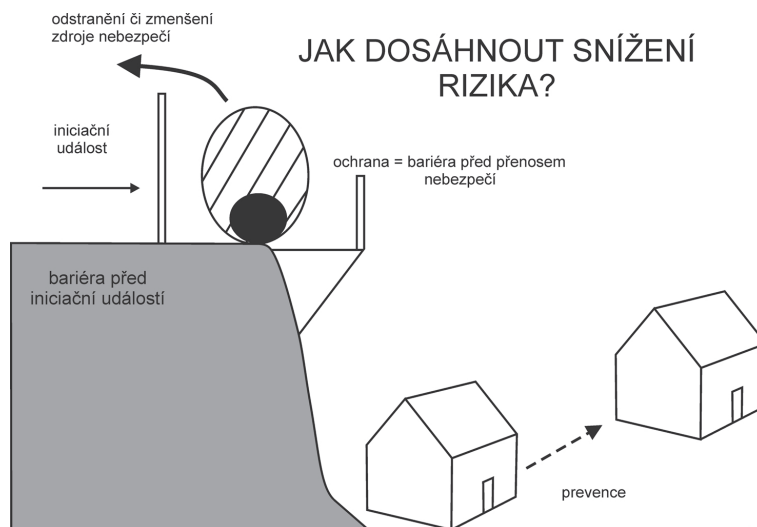
- Poruchy dodavatelsko-odběratelských vztahů.
- Nejistotu v oblasti pracovních sil (nevhodná kvalifikace, nedostatek pracovníků, nespolehlivost pracovníků – fluktuace, stávkové hnutí apod.).
- Neurčitost finančních zdrojů (nesolventnost obchodních partnerů, nejistota úvěru, problémy s pojištěním apod.).
- Nezabezpečení informačních technologií a systémů.
- Havárie a velké poruchy na provozovaném zařízení.
- Průmyslové havárie u jiných subjektů.
- Živelné události.
- Politickou nebo hospodářskou nestabilitu v regionu, kde je průmyslový provoz lokalizován, atd.

Pro tyto situace je charakteristická náhodnost jejich vzniku a nepříznivé následky pro podnikatelský subjekt. Proto je věnována pozornost studiu zákonitostí těchto náhodných událostí, jejich příčinám a následkům. Cílené snižování rizika je možné jen při respektování jeho ekonomických souvislostí a je vždy nutné provádět optimalizaci nákladů na řízení rizika.

Pro management rizika proto lze najít značné množství odborné literatury i mezinárodně uznávaných standardů. V současné době je na úrovni ISO zpracovávána nová norma komplexně řešící tuto problematiku, která bude publikována v roce 2010. Jedná se o normu ISO 31000 Management rizika – Principy a směrnice k jejich zavedení (Risk management – Principles and guidelines on implementation) (ISO/DIS 31000, 2008), která poskytne celkový rámec procesu managementu rizika a detailní principy pro jeho jednotlivé kroky. Záměrem tohoto standardu však není předepsat uniformní systém managementu rizika univerzálně pro všechny typy organizací. Návrh a implementace managementu rizika bude záležet na rozdílných potřebách a specifikách organizací, na jejich cílech, struktuře, produktech, procesech a specifických činnostech. Cílem je tedy spíše harmonizace procesů managementu rizik v rámci existujících systémů managementu. Proces managementu rizik podle normy ISO 31000 souhrnně znázorňuje následující obrázek 136.



Obrázek 136: Znáznornění procesu managementu rizika (podle ISO/DIS 31000, 2008).



Obrázek 137: Schematické znázornění základních principů managementu rizik.

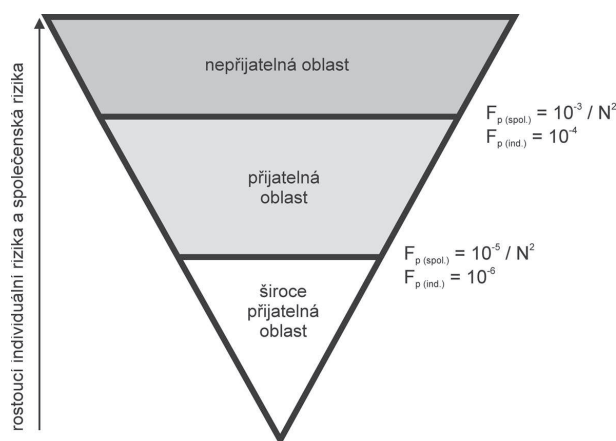
Vzhledem ke značně komplikované a v různých oborech jinak prakticky zažitě terminologii v této problematice uvádíme dva základní obecně přijaté termíny:

- **Management rizika** – jsou koordinované činnosti ke směřování a řízení organizace s ohledem na riziko. Management rizika všeobecně zahrnuje posouzení rizika, řešení rizika, přijetí rizika a komunikaci o riziku (ISO/IEC Guide 73:2002, 2002).
- **Řízení rizika** – jsou činnosti implementující rozhodnutí managementu rizika. Řízení rizika může zahrnovat monitorování a přehodnocení rozhodnutí a vyhovění těmto rozhodnutím (ISO/IEC Guide 73:2002, 2002).

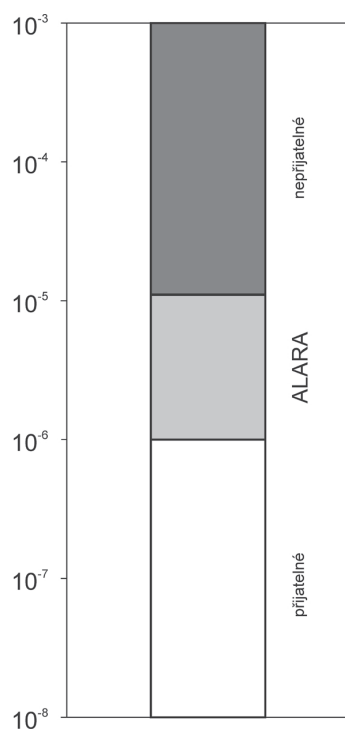
V kontextu různých oblastí bezpečnosti (BOZP, bezpečnost, informací, PZH) není tato terminologie vždy odpovídající. Nicméně podstata celého procesu je v každém případě analogická – podstatou je na základě objektivní analýzy a hodnocení snižovat míru rizika pomocí realizace vhodných opatření a kontroly jejich účinnosti. Obrázek 137 názorně ilustruje obecné principy managementu rizik.

5.5.6 Principy ALARP a ALARA

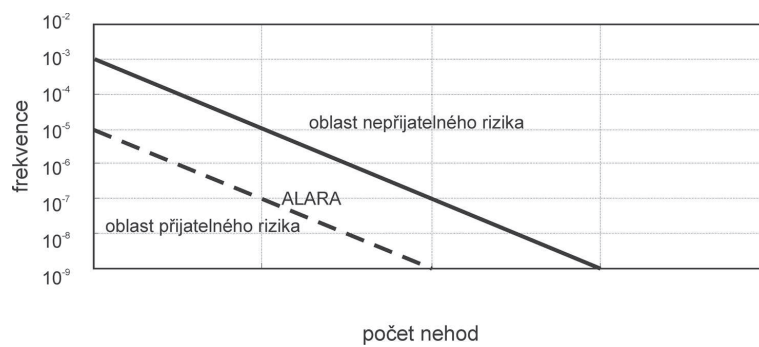
K systémovému snižování rizika lze přistoupit z hlediska již výše zmíněných principů ALARA a ALARP. ALARP (As Low As Reasonable Practicable) je princip snižování rizika na tak nízké, jak je to rozumně (racionálně) proveditelné (tj. náklady na další snížení rizika jsou již neúměrné vůči přínosu získaného realizací těchto opatření) (viz obrázek 138). ALARA (As Low As Reasonably Achievable) představuje princip snižování rizika na tak nízké, jak je to rozumně (racionálně) dosažitelné (viz obrázek 139 a obrázek 140).



Obrázek 138: Grafické znázornění principu ALARP a vyjádření kritérií přijatelnosti individuálního a společenského rizika.



Obrázek 139: Znáznornění principu ALARA a kritérií pro hodnocení individuálního rizika.



Obrázek 140: Grafické znázornění principu ALARA a kritérií pro hodnocení společenského rizika.

Oba principy rozlišují v přijatelnosti rizika tři úrovně:

- akceptovatelné riziko,
- tolerovatelné riziko a
- neakceptovatelné riziko.

Tyto principy jsou postaveny na obecné filozofii proaktivního managementu rizik a zahrnují v sobě také kritéria přijatelnosti individuálního a společenského rizika. Jejich smyslem je neustále vyhledávat a vyhodnocovat všechna rizika, přijímat vhodná nápravná opatření, která jsou ekonomicky a společensky zdůvodnitelná, provádět průběžnou kontrolu a audit a vyvozovat z nich příslušné důsledky. Jedná se tedy o praktickou aplikaci systému managementu bezpečnosti, jejíž nedílnou součástí je aktivní „zapojení zaměstnanců do problému“ tak, aby sami pochopili důležitost bezpečnosti jak pro sebe, tak pro podnik i okolní společnost. Dobře fungující management bezpečnosti tak vede nejen ke snižování rizik, zvyšování spolehlivosti výkonu a snižování zbytečných ztrát, ale také k zavedení kultury bezpečnosti jakožto nedílné součásti podnikové kultury (blíže viz kapitola 5.6).

Přijetí konceptu důležitosti dobrého systému managementu bezpečnosti – Safety Management System (SMS) – vedlo následně k rozvoji metod auditu, které lze použít pro hodnocení kvality řízení bezpečnosti. Audity systému managementu bezpečnosti by se neměly zaměřovat s běžným monitorováním, které management podniku používá denně pro řízení provozu na pracovišti. Ani by se neměly zaměřovat s technickými audity, resp. kontrolami, které jsou zaměřeny hlavně na problematiku „hardwaru“.

5.6 Kultura bezpečnosti

5.6.1 Firemní kultura a postoje k bezpečnosti v podniku

Pro organizace s vysokým potenciálem způsobit havárii by přístup k bezpečnosti měl být dominantním aspektem celkového chování a postojů – podnikové kultury. Bohužel mnoho lidí, kteří pracují v oblasti bezpečnosti, neví, co kultura bezpečnosti obnáší a jak ji posuzovat. Výzkum v oblasti firemní kultury resp. kultury bezpečnosti započal již na začátku 80. let 20. století, nicméně samotný pojem kultura bezpečnosti byla definována až Mezinárodní agenturou pro atomovou energii (IAEA) ve zprávě, která shrnovala příčiny a průběh havárie v Černobylu v roce 1986 (Kao a kol., 2008). Po této tragédii, která vznikla právě díky nízké úrovni kultury bezpečnosti při řízení elektrárny, vyplynula velká potřeba vytvořit samotnou koncepci kultury bezpečnosti, která by mohla být v praxi aplikována, a která by také umožňovala dozor ze strany inspekčních orgánů. Kulturu bezpečnosti bylo nutné ale nejprve definovat. Příslušná definice se však musela opírat o obecné atributy používané

pro popis jakékoli jiné kultury, která vždy představuje soubor takových postojů a charakteristik určité skupiny jedinců (národa, pracovníků určité organizace apod.) a také jednotlivců, který zajišťuje, že daným hodnotám (v tomto případě bezpečnosti) je věnována nejvyšší priorita daná jejím významem. Od té doby se pojem kultura bezpečnosti začal stále častěji používat zejména pak v souvislosti s bezpečností jaderných elektráren, ale i procesního průmyslu (Výzkumný ústav bezpečnosti práce, 2008).

Kultura bezpečnosti v praxi představuje určitý celek osvojených vzorů sociálního chování, umění, přesvědčení, myšlení dané komunity nebo populace. Je produktem individuálních a skupinových hodnot, postojů a pravomocí, a modelů chování, které určují závazek, styl a zběhlost organizace v plnění jejích programů pro zdraví a bezpečnost. Kultura ovlivňuje všechny aspekty činnosti organizace: poslání, strategii, používané prostředky, systémy měření, normy, systém odměňování, názor na povahu lidí i čas. Vše se v kultuře odráží. Je obtížné pochopit kulturu jako celek, ale je možné studovat jednotlivé normy a porozumět jim. Společenská norma je definována jako nevyřčené pravidlo chování, které – pokud se nedodrží – vede k sankcím. Příkladem pozitivní bezpečnostní normy může být podporování ohlašování bezpečnostních problémů zaměstnanci. Negativním příkladem bezpečnostní normy například je, když se jednotlivci přestanou obracet na odborníky na bezpečnost, protože je přestanou za odborníky považovat (Výzkumný ústav bezpečnosti práce, 2008).

Jelikož je kultura bezpečnosti součástí široce vymezené kultury podniku (organizační, podnikové, firemní kultury) a vstupují do ní prakticky všechny aspekty ostatních složek kultury, je jednou z nejvýznamnějších oblastí firemní kultury. Zcela jednoznačně hraje klíčovou roli v celkové úrovni bezpečnosti podniku. Úroveň firemní kultury se totiž odráží v kultuře bezpečnosti. Může být chápána jako podmnožina celkové kultury organizace popsaná jako sdílené hodnoty nebo smýšlení, kterými je charakterizované bezpečí v organizacích. Představuje setrvávající hodnotu a prioritu kladenou na pracovníky a na bezpečnost veřejnosti kýmoli v každé skupině a na každé úrovni podniku. Týká se míry, v níž jednotlivci a skupiny osob cítí svou osobní odpovědnost za bezpečnost, jednají tak, aby zachovávali, zvyšovali a sdělovali starost o bezpečnost, snaží se aktivně učit přizpůsobovat se a modifikovat (jak individuálně, tak podnikově) chování založené na poučení z chyb a být odměňováni způsoby, které jsou v souladu s těmito hodnotami. To, co je v určité firmě z hlediska bezpečnosti práce přijatelné, je nutné definovat a uplatňovat, má-li vzniknout firemní kultura, která si bezpečnosti váží. V ideálním případě by zaměstnanci měli znát všechna rizika spojená s jejich prací, měli by vědět, co je pro bezpečnost nezbytné a také přijmout vlastní odpovědnost. K tomu napomůže formulace norem, pomocí kterých budou zaměstnanci vědět o všech rizicích na svém pracovišti nebo budou po rizicích trvale vyhlížet (Výzkumný ústav bezpečnosti práce, 2008).

Základní charakteristiky kultury bezpečnosti

Za základní charakteristiky kultury bezpečnosti bývají považovány (Výzkumný ústav bezpečnosti práce, 2008):

- Povědomí důležitosti bezpečnosti u každého jednotlivce.
- Znalosti a kompetence získané výcvikem, školením a sebevzděláváním.
- Angažovanost za nejvyšší prioritu bezpečnosti jak vrcholového vedení, tak každého pracovníka.
- Motivace prostřednictvím vůdcovství, řízení pomocí cílů, systému odměn a postihů a prostřednictvím osobně přijímaných a vytvářených postojů.
- Dohled (supervize), včetně auditů a revizí s pohotovou reakcí na kritické postoje jednotlivců.
- Zodpovědnost nejen na základě formálního pověření, sestaveného popisu povinností a jejich pochopení jednotlivcem, ale i uvědomění pracovníka.

Na základě výsledků výzkumu, zkušeností a mezinárodní spolupráce expertů na bezpečnost byl vytvořen tříúrovňový model kultury bezpečnosti. Jednotlivé úrovně jsou definovány následovně (Výzkumný ústav bezpečnosti práce, 2008):

- **Úroveň základních předpokladů:**
Základní předpoklady jsou první, nejhlubší a tedy nejméně viditelnou úrovní kultury bezpečnosti. Jedná se o jakékoli zafixované představy o fungování reality, jež jsou jak společností, tak jednotlivci považovány za nezpochybnitelné či úplně samozřejmé a pravdivé. U člověka fungují zcela automaticky a nevědomě, a proto je také obtížné je identifikovat. Příkladem takového předpokladu je například tvrzení, že dané organizaci (osobě) lze věřit. Jsou východiskem myšlení a jednání lidí v organizaci. Zdrojem jejich vzniku je opakovaná zkušenost, či spíše funkčnost určitého způsobu řešení daného problému. Tento převzatý způsob jednání přijmou zaměstnanci za svůj a poté jej předávají i nově příchozím. Změna této úrovně podnikové kultury, zejména ve skupině, je velmi problematická.
- **Úroveň uznávaných hodnot:**
Uznávané hodnoty jsou často uváděné ve formálních dokumentech, jako jsou strategické plány, které mohou obsahovat prohlášení o poslání organizace a její vize. Jedná se o obecně uznávané hodnotové preference, zásady a pravidla pracovní morálky, loajality k firmě, vztahu k podnikovým partnerům, zákazníkům, akcionářům. Tato úroveň podnikové kultury je méně zřetelná a viditelná. Hodnoty a normy společnosti se totiž při první návštěvě obtížně poznávají, je třeba je dlouhodobě zkoumat. Bohužel, většina zaměstnavatelů se nezabývá podnikovou kulturou, natož aby je zajímaly hodnoty, které zastávají jejich zaměstnanci. A přitom jsou hodnoty jádrem firemní kultury

(pochopitelně jen tehdy, jsou-li skutečně sdíleny členy organizace). Chápeme je jako uznávané, chtěné a zavazující představy či ideje, které ovlivňují chování člověka. V podstatě rozlišujeme dvě kategorie hodnot – instrumentální a morální. Instrumentální hodnoty vedou k naplnění potřeby satisfakce (plat, materiální podmínky, realizace nápadu), morální hodnoty se projevují v pocitu hrlosti nebo ponížení (pomoc lidem, záchrana přírody). Sladění hodnot jednotlivců a firmy je klíčovým, ale také nejobtížnějším momentem budování strategicky potřebné kultury firmy. Normy chování jsou nepsaná pravidla pro chování v určitých situacích, které byly přijaty skupinou jako celkem. Ovlivňují způsob pracovní činnosti, komunikaci, styl oblékání. Jejich dodržování nebo porušování může být odměňováno či trestáno.

- **Úroveň artefaktů:**

Artefakty jsou vrchní, pro vnějšího pozorovatele nejviditelnější úrovní. Jsou označovány jako vnější projevy kultury a mohou být děleny na artefakty materiální a nemateriální povahy. Patří sem například kodex oblékání, architektura budov, úroveň formalit ve vztahu s autoritami, pracovní doba, schůze (jak často, jak jsou dlouhé, kdy se konají), jak se provádějí rozhodnutí, komunikace, rituály a ceremonie, řešení konfliktů, zvyky, logo, apod. Rozhodujícím nástrojem zprostředkování organizačních hodnot a norem je jazyk. Prostřednictvím vyprávění historek a příběhů z minulosti organizace se propojuje její historie a současnost a zároveň jsou v nich vyzvedávány pozitivní kvality. Artefakty jsou velmi snadno ovlivnitelné. Bohužel většina firem končí svou uniformitou právě na této úrovni.

5.6.2 Základní znaky dobré kultury bezpečnosti

Dobrá kultura bezpečnosti je odrazem hodnot, které jsou sdílené na všech úrovních organizace a které jsou založeny na přesvědčení, že bezpečnost je důležitá a každý v organizaci je za ni odpovědný. O kultuře bezpečnosti lze hovořit pouze tam, kde se nepodceňuje role, jakou sehraávají mezilidské vztahy a komunikace na pracovišti. Předpokládá to však nezbytnou změnu myšlení a přístupu ze strany vedoucích, to znamená nevidět věci pouze z hlediska vlastního postavení v hierarchii, ale respektovat především potřeby celku (Výzkumný ústav bezpečnosti práce, 2008).

Kvalita pracovního klimatu má značný význam pro bezpečnost práce i v tom, jaký je postoj a vztah k dodržování předpisů. Jejich odmítání či podceňování může být příčinou selhání a nezvládnutí situace, což může vést ke vzniku mimořádných událostí, průmyslových havárií nebo pracovních úrazů. Správná kultura bezpečnosti je taková, která neohrožuje nikoho uvnitř ani vně firmy. Je výsledkem pozitivních postojů k pracovišti a musí se týkat všech – od předsedy představenstva až po nováčka na nejnižším postu. Důležitý je i důraz na vzájemnou, významnou a měřitelnou bezpečnost a ochranu zdraví, na politiku a jednání, které slouží spíše jako vzor a nikoli nařízení. Rovněž ji charakterizuje osobní zdokonalování (vzdělávání) na všech úrovních organizace a také schopnost nést za své chování zodpovědnost. Základem

je tedy péče o celkovou pozitivní atmosféru, nepoškozující pracovní prostředí, bezpečné pracovní postupy, harmonické a přátelské vztahy mezi lidmi, dobré zdraví zaměstnanců, jejich bezpečnost a profesní rozvoj, stejně jako péče o zdravé životní prostředí a neškodlivé působení na celkovou ekologii krajiny. Většina těchto faktorů je současně prevencí stresu a násilí na pracovišti, proto je účelné spojit úsilí o bezpečnost práce se snahami o vytváření pozitivní kultury podniku, právě s prevencí pracovních podmínek stresu, tělesné zátěže v práci, apod. (Výzkumný ústav bezpečnosti práce, 2008).

K dosažení a udržení vysoké úrovně kultury bezpečnosti a tím i dostatečné bezpečnosti provozu je nezbytné, aby provoz s novými technologiemi zaměstnával potřebné množství vysoce kvalifikovaných pracovníků, kteří jsou si plně vědomi technických a administrativních požadavků na bezpečnost provozu. Tito pracovníci musí být vhodně motivováni, aby přijali za svůj pozitivní postoj ke všem bezpečnostním požadavkům. Kladný postoj je jedním ze základních prvků kultury bezpečnosti. K dosažení a udržení vysoké úrovně kompetencí je nutné, aby pracovníci byli podrobováni vzdělávacím a kvalifikačním programům, které musejí procházet neustálou kontrolou a revizemi, aby byla zajištěna jejich aktuálnost a správnost (Výzkumný ústav bezpečnosti práce, 2008).

Vedoucí pracovníci musejí povzbuzovat, oceňovat a hledat způsoby viditelné odměny za obzvlášť doporučeníhodné postoje k bezpečnosti. Je velmi důležité, aby systém odměňování zaměstnanců v podniku nepodporoval zvyšování výroby na úkor ohrožení bezpečnosti. V chybách zaměstnanců se má vidět především zdroj cenné zkušenosti a zaměstnanci mají být povzbuzováni ke zjišťování, hlášení a napravování nedokonalostí ve své vlastní práci i práci ostatních, aby tak pomohli sobě i druhým vyhnout se případným budoucím problémům. Při opakovaném výskytu nedostatků v práci anebo hrubého zanedbání povinností musejí vedoucí pracovníci uplatnit svou odpovědnost za disciplinární nápravné opatření, protože v opačném případě by mohla být ohrožena bezpečnost. Musejí to ovšem dělat velmi rozvážně, aby postihy nenapomáhaly k zatajování chyb. Výsledkem je celkově pozitivní postoj k bezpečnosti práce (Výzkumný ústav bezpečnosti práce, 2008).

Základní pravidla nastavení kvalitní kultury bezpečnosti

Na základě poznatků z praxe, psychologických analýz a řady teoretických prací bylo definováno dvacet základních pravidel pro utváření kvalitní kultury bezpečnosti (Výzkumný ústav bezpečnosti práce, 2008). Patří sem:

- **Chování manažerů:** vrcholoví manažeři podporují bezpečnost tím, že slouží jako model, vzor ostatním, prokazují svůj závazek svým chováním, postojem k bezpečnosti a umisťováním zdrojů, včetně času, stráveného na řešení otázek bezpečnosti a zvláště pak časem, stráveným úsilím zlepšovat bezpečnost, jejich chování v oblasti bezpečnosti musí být zřejmé jejich kolegům i ostatním zaměstnancům.

- **Sebehodnocení:** účelem sebehodnocení je podporovat zvýšený výkon v bezpečnosti pomocí přímého zapojení lidí do kritického přezkušování a zlepšování své vlastní práce a pracovních výsledků. Možné nedostatky lze zjistit a často i řešit dostatečně včas, než tyto nedostatky sníží rezervu bezpečného provozu. Silný závazek k procesu sebehodnocení může zaměstnance motivovat ke snaze o trvalé zlepšování bezpečnosti.
- **Postoj, že bezpečnost je vždy možné zlepšit:** organizace jsou neustále nespokojené s dosaženou bezpečností a stále se snaží o zlepšení. Tato uznávaná hodnota odráží fakt, že se v organizaci široce uplatňuje sebehodnocení.
- **Proaktivní a dlouhodobá perspektiva:** plány by měly obsahovat krátkodobé, střednědobé a dlouhodobé cíle, prokazující, že se organizace aktivně připravuje na budoucnost a také opatření, které tyto změny umožní.
- **Kvalita dokumentace a postupů:** dokumentace by měla být obsažná a snadno pochopitelná. Měla by být jasně stanovená odpovědnost za přípravu a prověřování dokumentace. Dokumentace by se měla používat jak pro práci, tak i pro školení. Je důležité, aby dokumentace byla přístupná zaměstnancům, a to ve formě vhodné pro pracovní použití.
- **Shoda s předpisy a postupy:** důležitost této charakteristiky pro bezpečnost je zřejmá. Postupy by také měly určovat, co se má dělat v případě neočekávané situace, která nemusí být pokryta stávajícími předpisy, nebo postupy. Porušování předpisů a postupů je jasným znamením slabé kultury bezpečnosti.
- **Jasně úlohy, pravomoci a odpovědnosti:** z hlediska bezpečnosti je důležité, aby nebyly nejasnosti o úlohách, nebo odpovědnostech v oblasti bezpečnosti. Popisy prací mají jasně tyto role a odpovědnosti definovat. Odpovědnost znamená, že jsou jasně stanovené cíle, pokrok v plnění je pravidelně hodnocen a jsou stanoveny následky za plnění i neplnění.
- **Motivace a spokojenost v práci:** chování zaměstnanců je silně ovlivňováno jejich motivací a spokojeností v práci. V tomto se odráží vůdcovství a pozornost věnovaná v organizaci náplni práce. Otázky motivace mohou být složité a může být při zpracování náplní práce vyžadována účast expertů.
- **Zapojení všech zaměstnanců:** zaměstnanci nebudou mít pocit, že bezpečnost je jejich věcí, pokud nebudou zapojeni do zjišťování a řešení problémů v bezpečnosti. Bezpečnost je oblast v organizaci, kde každý může přispět. Organizace má mít implementován proces pro zapojování zaměstnanců do problematiky bezpečnosti.
- **Dobré pracovní podmínky:** bezpečnost může být ohrožena, pokud jsou pracovníci pracovním přetížením. Jejich morálka a pozornost k otázkám bezpečnosti se v tom případě snižují. Je třeba, aby manažeři předvíдали dopad neobvyklých situací či restrukturalizace organizace na zaměstnance, a tím se

vyhnuli možným problémům. Zaměstnanci mají odpovědnost za to, hlásí-li při nástupu, že jsou schopni práce.

- **Měření výkonu v bezpečnosti:** je důležité, aby organizace měřila svůj výkon v bezpečnosti a sdělovala výsledky měření a zjištěné trendy všem zaměstnancům. Zvláště důležité je měření činností určených pro zlepšování bezpečnosti a zde by se organizace neměla spoléhat pouze na statistiku úrazů. Takový přístup je příliš reaktivní.
- **Spolupráce a týmová práce:** je důležité, aby pracovníci byli schopni účinně pracovat v týmu obzvláště tehdy, má-li se předejít konfliktům, jde-li sestava týmu napříč odbornostmi. Úspěšné týmy by měly být uznávány systémem odměn v organizaci.
- **Řešení konfliktů:** organizace potřebuje mít odpovídající procesy pro řešení konfliktů, jinak hrozí nebezpečí buď eskalace konfliktu, nebo jeho skrytí a objevení se někde jinde. Snadnost, se kterou pracovníci mohou upozorňovat na problémy ostatní kolegy, je znamením pracovní síly, která má správnou sebedůvěru. Konflikty spojené s bezpečností jsou obzvláště škodlivé, protože mohou zdegenerovat do vzájemného obviňování se a do vzájemné nedůvěry.
- **Vztahy mezi manažery a zaměstnanci:** mezi zaměstnanci a manažery by měl být vztah vzájemného respektu a otevřenosti. Obě strany by měly mít důvěru ve schopnost přístupu jeden k druhému a nastolovat možné problémy. Některé organizace mohou být založeny více hierarchicky než jiné, ale hierarchie by neměla bránit vzájemnému respektu.
- **Dobré materiální a technické podmínky, údržba budov a pořádek:** tam, kde je nepořádek, je pravděpodobně i špatná morálka zaměstnanců a nezájem manažerů. Takováto kombinace je předpisem pro špatnou bezpečnost.
- **Vysoká priorita bezpečnosti:** mnoho organizací prohlašuje, že bezpečnost je u nich ta nejvyšší priorita. Ale činnost a chování ne vždy tuto uznávanou hodnotu potvrzují. Důvěryhodnost organizace je nižší, pokud skutečnost není v souladu s uznávanou hodnotou.
- **Otevřenost a komunikace:** dobrá komunikace je v organizaci potřebná, pokud mají pracovníci účinně pracovat. Zaměstnanci si musí důvěřovat ohledně svých znalostí a musí také mít příležitost sdělovat své obavy ať už jako skupina, nebo jako jednotlivci. Organizace může využívat mnoho komunikačních kanálů, způsobů komunikace, pro komunikaci se zaměstnanci. Pokud se organizace přihlásí k této hodnotě, bude potom trvale podporovat otevřenost mezi svými zaměstnanci.
- **Ochota učit se:** tato hodnota může být většinou nahlížena jako filozofie organizace, kdy přístup k jakémukoli problému je brán jako příležitost něco se naučit. Je to ochota učit se od druhých, a sdílet svou vlastní zkušenost s ostatními. Organizace neustále přehodnocuje okolní prostředí a přizpůsobuje se změnám tohoto prostředí. Snaha organizace učit se je velmi důležitá

pro poučení se z bezpečnostních problémů a pro určení jejich skutečných prvotních příčin.

- **Zaostření na čas:** je třeba vždy udržovat rovnováhu mezi minulostí, přítomností a budoucností. Přehnané soustředění se na jedno období a vyloučení druhých období může způsobit problémy. Měla by být nalezena rovnováha v plánování činností, ale je třeba, aby tato rovnováha byla přítomna i v práci zaměstnanců. Zaostření na čas bude ovlivňováno širšími sociálními a národními kulturami.
- **Názor na chyby:** na chyby lze nazírat jako na příležitost k poučení se nebo jako na příležitost k trestu. Volba je záležitostí širší sociální kultury. Organizace mohou ovlivnit u svých zaměstnanců jejich názor na chyby. Pro bezpečnost je velmi důležité, aby zaměstnanci byli schopni upozornit na chyby v bezpečnosti bez obav z potrestání, protože jinak bude tato znalost chyb potlačena. Některý jiný zaměstnanec může být v budoucnu tou samou chybou postižen.
- **Názor na člověka:** názor na člověka může mít velký vliv na to, jak se v organizaci s lidmi zachází. Jestliže jsou lidé považováni za nedisciplinované a zajímající se jen o sebe, potom budou neustále podrobováni kontrolám. Jejich činnost bude pod přísným dohledem. Na druhé straně, jestliže lidé usilují o uplatnění svých schopností pomocí svého rozvoje a svou důvěryhodností, potom mohou být řízeni mnohem flexibilnějším způsobem, který jim poskytuje větší pravomoci brát na sebe odpovědnost. Oba způsoby nazírání na člověka mohou mít svou úlohu při zlepšování bezpečnosti, ale převládá názor, že ten druhý uvedený přístup bude v delší perspektivě mít větší přínosy (Výzkumný ústav bezpečnosti práce, 2008).

5.6.3 Symptomy slábnoucí kultury bezpečnosti

Spouštěcím impulsem destabilizace může být něco, co se jeví jako relativně nevýznamná událost. Nastanou-li nepředvídané události, tak organizace, která vypracovala pozitivní kulturu bezpečnosti a která má dobrý systém řízení, bude méně náchylná na destabilizaci. Pozitivní kultura bezpečnosti a dobrý systém řízení sice nemohou eliminovat výskyt nepředvídaných událostí, ale mohou významně snížit jejich výskyt. To, co pozitivní kultura bezpečnosti vytváří, je odolnost k jakýmkoli nestabilizujícím silám. Na symptomy lze nahlížet jak z hlediska organizace, tak i z hlediska dozoru (Výzkumný ústav bezpečnosti práce, 2008).

Jelikož hlavní podíl na utváření kultury bezpečnosti má samotný podnik, zmíníme zde tzv. hlediska organizace, která mohou indikovat slábnoucí kulturu bezpečnosti. Jedná se především o:

- **Nedostatek systematického přístupu,** který může ovlivnit všechny aspekty činností organizace. Organizaci činí náchylnou k opakovaným krizím, z nichž

některé mohou mít i vážné dopady na bezpečnost. Přítomnost tohoto nedostatku se projevuje nejistou odpovědností, špatným rozhodovacím procesem a nedostatkem spolehlivých informací a omezeným pochopením procesu. Z hlediska bezpečnosti se tento nedostatek projevuje ve slabém procesu hodnocení. Organizace se systematickým přístupem nehodnotí svou účinnost pouze na základě plnění úkolů, ale hodnotí také svou efektivitu při získávání zdrojů, zpracování zdrojů, směřování výstupů a udržování stability a rovnováhy. V případě kultury bezpečnosti se systematický přístup projevuje existencí plánů na zlepšení, cílů a odpovědností, monitorováním pokroku a alokací odpovídajících zdrojů. Indikátorem nedostatku systematického přístupu je neexistence procesu řízení změn.

- **Nesprávně udržované postupy**, tedy postupy, které nejsou pravidelně prověřovány a aktualizovány, se stávají bezcenné a neplatné, s možnými následky pro bezpečnost. Příprava, vydávání a novelizace postupů by měly být předmětem řízení kvality. Mají být jasné odpovědnosti za prověřování postupů. Pozitivním znakem je fakt, že lidé, kteří mají postupy používat, jsou zapojeni i do jejich prověřování.
- **Nekvalitní analýza proběhlých mimořádných událostí** (nejen havárií ale i pracovních úrazů, skoronehod apod.). To vede k absenci poučení se z chyb a problémy se tak často opakují. Tento stav obvykle ukazuje, že nebyla správně určena základní příčina (nebo příčiny) problému. Systematická podrobná analýza úrazu, nehody, je nutná, pokud z ní má být získáno poučení a mají být stanoveny prvotní příčiny. Analýza prvotních příčin (root cause analysis) vyžaduje, aby se stanovily jak přímé, tak i nepřímé příčiny nehody. Příčiny mohou být technické, lidský faktor, kultura organizace, proces, postup, zařízení a prostředí. Minulé zkušenosti prokázaly, že kultura bezpečnosti hraje velkou úlohu v mnoha událostech s dopadem na bezpečnost. Analýza prvotních příčin umožňuje lépe pochopit událost v celé její složitosti. Opakování událostí může také naznačit, že organizace nemá dostatečnou kulturu učení se. Pozitivním znakem je, že je věnována pozornost systematické analýze nehod a že jsou na to školeni ti zaměstnanci, kteří tuto odbornost mají využívat.
- **Neshoda zdrojů**, která se může projevit ve formě přehnaných skluzů v dokončování projektů, přehnaném množství práce přes čas, nedostatkem zaměstnanců s vhodnou kvalifikací a praxí, zvýšeným počtem subdodavatelů klíčových činností organizace po dlouhou dobu a opakovanými žádostmi u dozorových orgánů o výjimky z požadavků předpisů. V plánovacím procesu není rezerva pro nepředvídané události, což má za následek nedostatek vůle pro dokončení práce. Při probírání neshody zdrojů se musí věnovat pozornost jak kvantitě, tak i kvalitě zdrojů a tomu, je-li neshoda zdrojů krátkodobá, či dlouhodobá. Neshoda zdrojů nastává často po období zmenšování (zeštíhlování) organizace.

- **Zvyšující se počet porušení předpisů** (vědomých odchylek od pravidel, např. zkrácení cesty), což poskytuje pohled na kulturu bezpečnosti z hlediska myšlení samotných pracovníků. Všechna porušení by se měla důkladně vyšetřit, aby se umožnilo zjistit prvotní příčinu. Pokud se počet porušení zvyšuje, může to být znamením netečnosti managementu nebo nějakým napětím v organizaci. Porušení by se neměla plést s chybami, způsobenými opomenutím, nebo omylem. To jsou neúmyslná odchýlení.
- **Narůstající seznam nesplněných akcí:** zvyšující se počet nápravných akcí, které nebyly v daném termínu dokončeny, jsou znamením toho, že bezpečnost nemá tu prioritu, kterou si zaslouhuje. Tento počet je indikátorem manažerské účinnosti v plánování, alokace zdrojů, udělování priorit a monitorování práce. Je třeba věnovat pozornost jak počtu nápravných akcí, které překročily termín dokončení, tak i velikosti onoho opoždění realizace.
- **Ověření připravenosti pro provoz, nebo údržbu:** nehody se často stávají při zahájení provozu po odstávce pro údržbu, nebo když zařízení není správně obsluhou připraveno pro plánovanou údržbu. Nehody mohou být způsobeny řadou faktorů: špatné plánování před zahájením prací, neodpovídající hodnocení rizik, špatná komunikace nebo špatný systém udělování povolení k práci, neodpovídající školení nebo nedostatek kvalifikovaných a zkušených zaměstnanců. Existence systematického procesu pro přípravu zařízení na spuštění nebo pro údržbu je indikátorem toho, že je věnována patřičná pozornost tomuto důležitému aspektu provozu. Zaměstnanci jak údržby, tak i provozní zaměstnanci by měli být zapojeni do jakéhokoli ověřování.
- **Obavy zaměstnanců nejsou bezodkladně řešeny:** zaměstnanci budou frustrovaní a demotivovaní, pokud postřehnou, že jejich obavy o bezpečnost jsou ignorovány, nebo že musejí několikrát své obavy hlásit, než dojde k akci. Získají tím dojem, že bezpečnost není důležitá – to je špatný základ pro rozvoj pozitivní kultury bezpečnosti. Nedostatek komunikace mezi zaměstnanci a vrcholovými manažery může bránit přenosu obav zaměstnanců k těm, kdo mají pravomoc zařídit nápravu. Vrcholoví manažeři, kteří pravidelně navštěvují pracoviště, budou mít mnohem pravděpodobněji vědomí o problémech s bezpečností. Měl by být zaveden systém, který umožňuje nebo podporuje zaměstnance, aby sdělovali své obavy o bezpečnost, a který umožňuje oznamovat pokrok v nápravných akcích.
- **Neúměrné soustředění na technické problémy:** tato slabina se projevuje nedostatečnou pozorností k lidskému faktoru práce. Problémy jsou vnímány pouze jako technická výzva a řeší se bez uvažování s jakýmkoli lidskými slabostmi. Pozitivním indikátorem, že tato slabina neexistuje, je začlenění lidského faktoru a problematiky kultury do školení zaměstnanců, zvláště pak do školení manažerů. Lidský faktor by měl být integrální součástí hodnocení rizik.

- **Absence hlášení skoronehod:** systém pro hlášení skoronehod není zaveden, což sice nemusí být nutně indikátorem oslabující se kultury bezpečnosti, ale je to spíše znamením, že organizace neuznává hodnotu informací získaných z tohoto druhu událostí. Může to být také proto, že se organizace nachází v raném stádiu rozvoje kultury učení se, nebo že zaměstnanci mají stále ještě základní předpoklad, že ti, co udělají chybu, budou potrestáni. Existence systému pro hlášení skoronehod je znamením, že organizace dosáhla vyšší úrovně sofistikovanosti ve svém přístupu k bezpečnosti.
- **Chybějící proces sebehodnocení** je výrazným indikátorem potenciální slabosti kultury bezpečnosti. Organizace bez takovýchto procesů bude slepá k nedostatkům v postojích k bezpečnosti a v chování a neuvědomí si prvotní příčiny mnoha událostí. Organizace, která neprovádí sebehodnocení, těžko přijme za svou filozofii “trvalého zlepšování” (Výzkumný ústav bezpečnosti práce, 2008).

Pořádek a údržba

Nízká úroveň pořádku a nedokonalá údržba zařízení, budov i drobných pomůcek obvykle signalizuje, že management je bez zájmu, snaží se za každou cenu šetřit náklady a pracovní síla je špatně motivována. Pracovníci nepociťují profesní hrdost a zaměstnání považují pouze jako zdroj svých příjmů, kam chodí neradi. Tyto slabosti se obvykle šíří i do kultury bezpečnosti. Úroveň pořádku a čistoty a udržovanosti je dobrým indikátorem všeobecného étosu organizace.

Problémy promítající se do utváření kultury bezpečnosti

Smyslem formování kultury bezpečnosti je v konečném výsledku dosahování co nejvyšší možné spolehlivosti lidského činitele, čili kvality pracovní síly zejména z hlediska spolehlivostních ukazatelů. Upevňování kultury bezpečnosti je jedním ze základních předpokladů prevence závažných havárií. K prioritním úkolům managementu by proto mělo patřit také trvalé zvyšování prestiže problematiky bezpečnosti a spolehlivosti.

Ovšem není žádnou výjimkou, kdy se v podniku běžně projevují, jakožto zřetelný projev nepříznivé bezpečnostní kultury, negativní postoje k problematice bezpečnosti i jejím reprezentantům. S takovými symptomy je třeba velmi opatrně, ale důrazně bojovat. K nepříznivé situaci často přispívají tlaky a postoje vrcholového vedení upřednostňující v některých situacích ekonomické (časové, výrobní) cíle před bezpečnostními hledisky. Postoje a jednání vedoucích pracovníků je pro celou organizaci viditelným indikátorem důležitosti přikládané managementem firmy k otázkám bezpečnosti. Významnou roli hraje postavení bezpečnostního managementu ve vztahu k vrcholovému řízení organizace – zejména přímý vstup do procesů podnikového rozhodování na nejvyšší řídicí úrovni. Není-li tomu tak, vysílá vrcholový management čitelný signál o tom, jak hodnotí přínosy bezpečnostního managementu pro podnik.

Cíle identifikace rizik v oblasti kultury bezpečnosti by proto měly být soustředěny zejména na:

- Zhodnocení jednání managementu z hlediska formování bezpečnostní kultury.
- Zhodnocení stavu, jak jsou aktivity managementu v organizaci vnímány.
- Zhodnocení nedostatků, deficitů, potenciálních zdrojů obtíží, silných a slabých stránek (tzv. SWOT analýzy).
- Identifikování rizik, resp. kritických faktorů úspěchu spojených s implementací opatření k rozvoji/zlepšování kultury (odstraňování zjištěných nedostatků).

Hodnocení prvků kultury bezpečnosti při bezpečnostní prověrce

Vedoucí pracovníci by měli být v neustálém aktivním kontaktu se zaměstnanci. Měli by se jich ptát na jejich názory a vyslechnout také jejich požadavky směřující ke zlepšení pracovního prostředí. Také při kontrolní činnosti, prováděné například bezpečnostními technikami, by měly být zaznamenávány názory jednotlivých zaměstnanců a vedle toho také pozorováno jejich počínání na pracovištích, z nichž lze vytvořit obraz o stavu kultury bezpečnosti v podniku. Screening úrovně kultury bezpečnosti by měl být zahrnut i do komplexní prověrky BOZP. Každý podnik by se měl totiž všemi dostupnými mechanismy snažit o dosažení co možná nejvyšší úrovně kultury bezpečnosti ve firmě. Tu je možno stručně charakterizovat tak, že každý zaměstnanec podniku (nehledě na profesi či postavení v hierarchii řízení) dělá to, co je po něm vyžadováno, dodržuje plně pracovní a bezpečnostní předpisy a nařízení, a to zcela automaticky a o své vlastní vůli, aniž by byl kontrolován jinou osobou.

Provést objektivní screening kultury bezpečnosti ve firmě není ale záležitostí pouhého náhodného dotazování zaměstnanců, nýbrž je nutné využít vhodných analytických nástrojů. Těmi bývají dotazníky, které formou sady tvrzení a k nim nabízenými variantami odpovědí nutí zaměstnance k zamyšlení a vyjádření svého náhledu na věc. Tyto odpovědi jsou tedy odrazem jeho vlastního, subjektivního vnímání jednotlivých prvků kultury bezpečnosti ve firmě. Aby nedošlo ke zkreslení výsledků, musí vyhodnocení sebraných dat provádět pouze zkušený psycholog.

Literatura ke kapitole

Advisory Committee on Major Hazards: First Report (HMSO). London: Health and Safety Commission, 1976.

BABINEC, F.; VACEK, L. 2008. Kritéria přijatelnosti společenského rizika. In *Sborník konference APROCHEM 2008: Odpadové fórum..* Milovy: CEMC – České ekologické manažerské centrum, 2008, s. 2284-2292.

BARTLOVÁ, I. 2002. *SEVESO III*. Ostrava: VŠB-TU, 2002. (Edice SPBI Spektrum).

BERNATÍK, A. 2006. *Prevence závažných havárií II.: učební skripta VŠB-TU*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2006. ISBN 80-86634-90-6.

CO-51-5 *Provozní havárie s výronem nebezpečných škodlivin: resortní předpis*. Praha: Ministerstvo národní obrany ČSSR, 1981.

Česká republika. Parlament ČR. Zákon č. 59/2006 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými přípravky a o změně zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a zákona č. 320/2002 Sb., o změně a zrušení některých zákonů v souvislosti s ukončením činnosti okresních úřadů, ve znění pozdějších předpisů, (zákon o prevenci závažných havárií). *Sbírka zákonů České republiky*, 2006, částka 25, s. 842-869. Dostupný z WWW: <<http://web.mvcr.cz/sbirka/2006/sb025-06.pdf>>.

Česká republika. Parlament ČR. Zákon č. 353/1999 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami a chemickými přípravky a o změně zákona č. 425/1990 Sb., o okresních úřadech, úpravě jejich působnosti a o některých dalších opatřeních s tím souvisejících, ve znění pozdějších předpisů (zákon o prevenci závažných havárií). *Sbírka zákonů České republiky*, 1999, částka 111, s. 7609-7629. Dostupný z WWW: <<http://www.mvcr.cz/sbirka/1999/sb111-99.pdf>>.

Česká republika. Parlament ČR. Zákon č. 262/2006 Sb., zákoník práce. *Sbírka zákonů České republiky*, 2006, částka 84, s. 3146-3241.

ČSN EN 61025. *Analýza stromu poruchových stavů (FTA)*. Praha: Český normalizační institut, 2007.

ČSN EN 61511. *Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů*. Praha: Český normalizační institut, 2005.

ČSN IEC 61882. *Studie nebezpečí a provozuschopnosti (studie HAZOP) – Pokyn k použití*. Praha: Český normalizační institut, 2002.

ČSN OHSAS 18001:2008. *Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky*. Praha: Český normalizační institut, 2008.

DEMING, W. E. *Out of the Crisis*. Cambridge: Center for Advanced Engineering Study, Massachusetts Institute of Technology, 1986

Directive 82/501/EEC „On the major-accident hazards of certain industrial activities“.

Directive 96/82/EC „On the control of major accident hazards involving dangerous substance“.

Directive 2003/105/EC of the European Parliament and of the Council of 16 December 2003 amending Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substance.

DIRNER, V. ... [et al.]. *Ochrana životního prostředí: základy, technologie, plánování, ekonomika, právo a management*. Praha: Ministerstvo životního prostředí, 1997. ISBN 80-7078-490-3

DRAHTEN, H.; HERMANN, B. 2007. Relevant characteristics of the human system as determining factors for the man-machine-interface in process plants. In *OECD-CCA Workshop on Human Factors in Chemical Accidents and Incidents, Proceedings*.

EISLER, J.; ROUSOVÁ, O. 2009. Praktické zkušenosti se snižováním fugitivních emisí VOC. In *Konference VOC 2009 – Emise organických látek z technologických procesů a metody jejich snižování: sborník přednášek*. Pardubice: Český svaz vědeckotechnických společností, 2009. S. 27-32. ISBN 978-80-02-01939-1.

European Organisation for the Safety of Air Navigation. *Human Factors Module: a Business Case for Human Factors Investment: HUM.ET1.ST13.4000-REP-02* [online]. European Organisation for the Safety of Air Navigation, 1999 [cit. 2009-05-06]. 44 s. Dostupný z WWW: <<http://www.eurocontrol.int/>>

humanfactors/gallery/content/public/docs/DELIVERABLES/HF17%20(HUM.ET1.ST13.4000-REP-02)%20Released.pdf>.

FERRY, T. S. 1988. *Modern Accident Investigation and Analysis*. 2nd ed. New York: John Wiley and Sons, 1988.

FOORD A. G...[et al.]. *Applying the laterst standard for Functional Safety: IEC 61511* [online]. 4-sight Consulting [cit. 2007-08-29]. Dostupný z WWW: <http://www.4-sightconsulting.co.uk/Current_Papers/Functional_Safety/functional_safety.html>.

FOOTE, A. J. 2003. Is Probabilistic Assessment the Answer? *The Journal of the RAC*, 2003, no. 1, s. 1-12.

Guidelines for Quantitative Risk Assessment: Purple Book (CPR 18E). Hague: Committee for the Prevention of Disasters, 1999.

HASAL, P...[et al.]. 2007. *Chemické inženýrství I*. Praha: Vydavatelství VŠCHT, 2007. 350 s. ISBN 978-80-7080-002-7.

HAVLÍKOVÁ, M. 2008. Člověk v systémech člověk – stroj. *Časopis výzkumu a aplikací v profesionální bezpečnosti* [online], 2008, roč. 1, č. 3[cit. 2009-04-08]. Dostupný z WWW: <http://www.bozpinfo.cz/josra/josra-03-2008/havlikova_clovek_mms.html>. ISSN 1803-3687.

HAVLÍKOVÁ, M. 2009. Lidský faktor v systémech MMS. *Časopis výzkumu a aplikací v profesionální bezpečnosti* [online], 2009, roč. 2, č. 1[cit. 2009-04-07]. Dostupný z WWW: <http://www.bozpinfo.cz/josra/josra-01-2009/havlikova_lidsky-faktor.html>.

HEINZE, M. R. 2001. *Functional safety of Programmable systems, device and components: requirements from global and national standards* [interní materiál]. TUV Rheinland of N. A., 2001.

HOREHLEDOVÁ, Š. Systémy managmentu bezpečnosti a ochrany zdraví při práci podle požadavků normy BS OHSAS 18001:2007 v kontextu integrovaných systémů řízení. *Časopis výzkumu a aplikací v profesionální bezpečnosti* [online], 2008, roč. 1, č. 2. Dostupný na www: <http://www.bozpinfo.cz/josra/josra-02-2008/ohsas_horehledova.html>. ISSN 1803-3687

HOVORKA, F. 2005. *Technologie chemických látek*. Praha: Vydavatelství VŠCHT, 2005. 180 s. ISBN 80-7080-588-9.

ILO-OSH 2001: guidelines on occupational safety and health management systems. Geneva: International Labour Organisation, 2001.

ISO/DIS 31000. Risk management – principles and guidelines on implementation: draft international standard. Geneva: International organization for standardization, 2008.

ISO/IEC Guide 73:2002. *Risk management – Vocabulary – Guidelines for use in standards*. Geneva: International organization for standardization, 2002

JAMBON, F. 1998. Taxonomy for Human Error and System Fault Recovery from the Engineering Perspective. In *International Conference on Human-Computer Interaction in Aeronautics (HCI-Aero'98)*. [s.l.]: [s.n.], 1998. s. 55-60.

KAO Ch.-S.; LAI W. H.; CHUANG T. F.; LEE, J.-Ch. Safety Culture Factors, Group Differences, and Risk Perception in Five Petrochemical Plants. *Process Safety Progress*, 2008, Vol. 27, No.2., pp. 145-152.

KARWOWSKI, W. 2006a. *International Encyclopedia of Ergonomics and human Factors*. 2nd ed. Boca Raton: CRC Press, 2006. Hollnagel, E., Accident Analysis and „Human error“, s. 1889-1892. ISBN 0-415-30430-X.

- KARWOWSKI, W. 2006b. *International Encyclopedia of Ergonomics and human Factors*. 2nd ed. Boca Raton: CRC Press, 2006. Hollnagel, E., Human Reliability Analysis, s. 753-757. ISBN 0-415-30430-X.
- KLETZ, T. A. 1991. *An Engineer View of Human Error*. 2. ed. Rugby: Institution of Chemical Engineers.
- KOSMOWSKI, K. T. 2003. Risk analysis and functional safety assessment with regard to human and organisational factors. In *SIPI Workshop*. Gdynia, 2003.
- KOTEK, L.; VOHRALÍKOVÁ, M. 2008. Jak zvyšovat spolehlivost lidské obsluhy. *AUTOMA: časopis pro automatizační techniku* [online], 2008, č. 5[cit. 2009-02-01]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=37315>.
- Kultura bezpečnosti a klima bezpečnosti: příručka pro inspektory JE*. 1. vyd. Praha: VÚBP, 2008. ISBN 978-80-86973-49-4.
- LANS, H. J. D.; BJORDAL, E. N. 1985. Application of risk analysis techniques. In *4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Harrogate 12-16 September*. Institution of Chemical Engineers. S. G46-G55.
- LEES, F. 1996. *Loss Prevention in the Process Industries: vol. 1*. 2nd. ed. Oxford: Butterworth-Heinemann, 1996. ISBN 0-7506-1547-8.
- Metodický pokyn odboru environmentálních rizik Ministerstva životního prostředí k rozsahu a způsobu zpracování dokumentu „Posouzení vlivu lidského činitele na objekt nebo zařízení v souvislosti s relevantními zdroji rizik“ podle zákona č. 59/2006 Sb., o prevenci závažných havárií. *Věstník Ministerstva životního prostředí*, 2007, ročník XVII, částka 3, s. 16-21.
- MAHN, J. A...[et al.]. 1995. *Qualitative Methods for Assessing Risk: SAND95-0320* [online]. 1995. 29 s. Dostupný z WWW: <<http://www.osti.gov/bridge/servlets/purl/54270-lseYGy/webviewable/54270.pdf>>.
- Management rizik. In *Leonardo da Vinci CZ/98/1/82530/PI/III.1.a/FPI*, česká verze. Ostrava: b.n., 2001. Modul 3, úroveň 3.
- Metodický pokyn odboru environmentálních rizik Ministerstva životního prostředí k rozsahu a způsobu zpracování dokumentu „Analýza a hodnocení rizik závažné havárie“ podle zákona č. 59/2006 Sb., o prevenci závažných havárií. *Věstník Ministerstva životního prostředí ČR*, roč. XVII, březen 2007. částka 3. s. 16-21.
- MILL, J. S. 1943. *A system of logic, ratiocinative, and inductive: being a connected view of the principle of evidence, and methods of scientific inquiry*. London: J. W. Parker, 1943.
- OHSAS 18001:1999. *Systémy managementu bezpečnosti a ochrany zdraví při práci – specifikace*. Praha: Český institut pro akreditaci, 2004.
- OHSAS 18002:2000 *Systémy managementu bezpečnosti a ochrany zdraví při práci – směrnice pro zavádění OHSAS 18001*. Praha: Český institut pro akreditaci, 2004.
- PALEČEK, M...[et al.]. 2006. *Prevence rizik*. 1. vyd. Praha: Oeconomica, 2006. 257 s. ISBN 80-245-1117-7.
- PRÁŠEK, R. Funkční bezpečnost – bezpečnost procesů a systémů. *TÜV SÜD Journal Česká Republika*, 2009, č. 3, s. 10-11.
- Program Bezpečný podnik*. Praha: Státní úřad inspekce práce, 2008.
- REASON, J. 1990. *Human Error*. Cambridge: Cambridge University Press; 1990.
- SADHRA, S. S.; RAMPAL, K. G. 1999. *Occupational Health: Risk Assessment in the Process Industries*. Blackwell Science, 1999. ISBN 0-632-04199-4.

SALVENDY, Gavriel. 2006. *Handbook of Human Factors and Ergonomics*. 3rd ed. Hoboken: John Wiley & Sons, Inc., 2006. SHARIT, Joseph, Chapter 27 Human Error, s. 708-760. ISBN 0-471-44917-2.

SKŘEHOT, P. 2007. Jak na prověrku bezpečnosti a ochrany zdraví při práci ve firmě. *BOZPinfo* [online], 16.04.2007 [cit. 2009-07-23]. Dostupný z WWW: <http://www.bozpinfo.cz/win/knihovna-bozp/citarna/tema_tydne/proverka_bozp07.html>.

SKŘEHOT, P. MALČÍKOVÁ, K. 2008. Nové metody a přístupy určené pro vyšetřování kořenových příčin selhání lidského činitele v procesním průmyslu. *BOZPinfo* [online], 13.02.2008 [cit. 2009-01-31]. Dostupný z WWW: <http://www.bozpinfo.cz/win/knihovna-bozp/citarna/clanky/lidsky_cinitel/lc_korenove080213.html>.

SKŘEHOT, P. 2008a. Kam jsme došli v ergonomii a oblasti spolehlivosti lidského činitele? *BOZPinfo* [online], 23.01.2008 [cit. 2009-04-14]. Dostupný z WWW: <http://www.bozpinfo.cz/knihovna-bozp/citarna/clanky/lidsky_cinitel/ergo080123.html>.

SKŘEHOT, P. 2008b. *Posuzování spolehlivosti člověka v pracovním systému pomocí analýz úkolů*. 1. vyd. Praha: VÚBP, 2008. 28 s. ISBN 978-80-86973-22-7.

SLUKA, V. [et al.]. 2005. Výkladový terminologický slovník některých pojmů používaných v analýze a hodnocení rizik pro účely zákona o prevenci závažných havárií [online]. Praha: VÚBP, 55 s. Dostupný z WWW: <http://www.vubp.cz/html_oppzh/metodiky/vykladovy_slovník_brezen05.pdf>.

TRPIŠ, J. *Analýza přístupů a metod použitelných pro pravděpodobnostní hodnocení spolehlivosti lidského činitele v procesním průmyslu*. 2009. 51 s. Fakulta bezpečnostního inženýrství. Vysoká škola báňská - TU Ostrava. Vedoucí bakalářské práce: RNDr. Mgr. Petr Skřehot.

Údržba a realizace průmyslových procesních zařízení [online]. Praha: Česká společnost chemického inženýrství [cit. 2007-09-08]. Dostupný z WWW: <<http://www.cschi.cz/urppz/havarie.asp>>.

