

ŘÍZENÍ RIZIK

Studijní opora

Obsah

Přístupy k posouzení rizika	3
Vymezení cíle analýzy a hranic systému a jeho důsledky	3
Cíle analýzy rizik jako součást rozhodovacího procesu	3
Vymezení systému s ohledem na funkce a činnosti	4
Vymezení v prostoru	6
Kontext problematiky posouzení rizik v rámci řízení rizik	6
Vazba analýzy rizik na management rizik	6
Model šíření nebezpečí a dopadu na cílový systém – myšlenková mapa a terminologie	9
Vymezení v čase	16
Identifikace nebezpečí a jeho zdrojů	18
Scénáře vedoucí k expozici zranitelného cíle	19
Hodnocení rizik – prostor rizik a matice rizik	21
Specifika multikriteriálního posouzení rizik	27
Principy managementu rizik	29
Identifikace nebezpečí	37
Návrh havarijních scénářů	38
Charakterizace a kvantifikace rizik	40
Zhodnocení rizik	41
Stanovení cílů ošetření rizik	42
Stanovení prostředků prevence	43

Realizace prevence.....	45
Zbytková rizika	46
Hodnocení rizik	46
Systém a metody řízení prevence závažných havárií v průmyslu	48
Management bezpečnosti v podniku	49
Literatura I	51
Komunikace	56
Teorie nebo praxe?	57
Funkce a cíle komunikace o rizicích	58
Kultura bezpečnosti	64
Co je to kultura bezpečnosti?	64
Analýza pojmu RESILIENCE v různých vědních oblastech.....	77
Ekologický a sociálně-ekologický systém.....	79
Výzkumné projekty nebo centra RESILIENCE v jednotlivých oblastech	83
Psychologie	83
Ekologie.....	83
Inženýrství	84
Počet výskytu pojmu RESILIENCE v jednotlivých oblastech	86

Přístupy k posouzení rizika

Vymezení cíle analýzy a hranic systému a jeho důsledky

Cíle analýzy rizik jako součást rozhodovacího procesu

Vymezení cíle analýzy a managementu rizik je klíčová, i když bohužel často kriticky podceňovaná činnost. Před tím, než započne samotná analýza rizik, je nezbytné věnovat důkladnou pozornost tomu, proč analýzu a management rizik děláme, tedy jaký má cíl. Tento cíl musí mít jednoznačné parametry cíle, tedy musí existovat kontrolovatelný způsob, jak poznáme jeho dosažení či nedosažení (musí být měřitelný, musí se týkat problému u vybraného systému, a umožňovat provedení rozhodnutí a jeho realizaci). Často se však setkáváme s tím, že cíl je formulován vágně a spíše proklamativně než konkrétně, popřípadě že není víceméně definován vůbec, prostě provádíme jakoukoliv analýzu rizik, která se tak nějak „naskytla cestou“ v důvěře, že když je to analýza rizik a my děláme analýzu rizik, musí být všechno v pořádku. Naneštěstí pro toho, kdo zvolil tuto cestu, různých analýz rizik může být veliké množství a nejsou libovolně zaměnitelné. Analýza rizik je jen nástroj a je to s ní jako s jinými nástroji – pro určitý konkrétní typ dosažení cíle potřebujeme specifický nástroj, tedy analýzu rizik, a jiný typ nám poslouží špatně nebo dokonce vůbec ne. Pilka lupenka, pilka na železo, oblouková pila, cirkulárka i motorová pila jsou všechno pily, ale vyřezávat cirkulárkou letecké modely ani připravovat lupenkou palivové dříví na zimu moc smysl nemá. A stejně jako u pily, i u analýzy rizik o správnosti výběru rozhoduje volba cíle, kterého chceme dosáhnout.

Při hodnocení, zda je volba cíle analýzy a managementu správná, nám mohou pomoci i některé formální, dokonce i sémantické (jazykové) pomůcky. Tak například cíl by měl obsahovat podstatné jméno udávající předmět, kterého se cílový stav týká, přídavná jména popisující kýžené vlastnosti (kvalitativní nebo kvantitativní, ale zjiitelné kontrolovatelným způsobem) a sloveso popisující činnost, kterou chceme cíle dosáhnout, a toto sloveso musí být ve vidu dokonavém, protože dosáhnout cíle znamená něco udělat, ne jenom dělat. Příkladem formulace vhodného cíle managementu rizik může být „Zlepšit úroveň BOZP tak, aby počet dnů pracovní neschopnosti způsobených pracovními úrazy klesl v příštích pěti letech o nejméně 25 %, a odpovídajícím cílem analýzy rizik je „Identifikovat rizika v oblasti BOZP, která nejvíce přispívají k úrazům s pracovní neschopností a mají potenciál ke

zlepšení“. Naopak příkladem nevhodné formulace cíle managementu je „Zvyšovat bezpečnost práce“ a analýzy „Analyzovat rizika v BOZP“. Druhá varianta cíle managementu rizik totiž neudává kontrolovatelný cíl, neboť jakákoliv, i sebenepatrnější a absolutně formální změna k lepšímu může být vydávána za splnění cíle, a je formulována jako průběžná aktivita, tedy může probíhat libovolně dlouho. Pod pojmem „Analyzovat rizika v BOZP“ pak může být téměř cokoliv s BOZP související. Obecně pak platí, že je vhodné se vyhnout cílům všeobecným, nekonkrétním, „všeobjímajícím“ a příliš rozsáhlým, naopak je vhodné hledat konkrétní a dostatečně úzké.

Je tedy zřejmé, že cíle analýzy a managementu rizik hrají klíčovou roli a je třeba se jim řádně věnovat. Stejně důležité pak je vymezení toho, čemu se máme věnovat, tedy analyzovanému nebo řízenému systému. Od cílů analýzy rizik se také odvíjí hloubka a detailnost prováděné studie (a tedy i náklady a množství práce s analýzou spojené) – v některých případech provádíme prakticky jen základní přehled – screening – a vystačíme s jednoduchými technikami, v jiných potřebujeme velmi detailní informace o možných rizicích a jejich vztazích a možnostech ošetření, a pak jsou nezbytné komplexní a náročné analytické metody. Příkladem je analýza rizik technologické havárie z hlediska havarijní připravenosti v rámci krizového řízení obce nebo kraje, kdy jsou dostatečné informace o možném průběhu, potenciálních dopadech havárie a možnostech včasného varování před blížící se událostí. U stejného rizika však v případě proaktivního provozovatele potřebujeme znát detaily odchylek od standardního provozu zařízení, které mohou ve vzájemné kombinaci vést k havárii, módy možného selhání, stejně tak jako cesty zamezení rozvoje příslušných událostí, navíc i detaily o pravděpodobnostech vzniku odchylek, jejich možném monitoringu atd. Analýza rizik je tak nepoměrně detailnější a tudíž i náročnější, navíc řeší jiné typy problémů – první popsany případ hlavně mitigaci následků, druhý prevenci vzniku havárie. Obě se však formálně dají nazývat „analýza rizik havárie technologie XY“.

Vymezení systému s ohledem na funkce a činnosti

Jedním ze zásadních požadavků při analýze rizik je zvolit adekvátní systém, který bude předmětem studie a řízení. Jinak řečeno, zvolený systém je to, čím se budeme zabývat v analýze rizik a co chceme řídit. Pod pojmem „systém“ spadají v první řadě potenciální zdroje nebezpečí, ohrožené cíle a vše, co zásadním způsobem ovlivňuje

možné scénáře, možné nežádoucí události a její dopady, a co bychom tedy mohli v rámci managementu rizik řídit, změnit nebo kontrolovat, aby se události nevyvinuly proti našim plánům. To se v praxi může ukázat jako nesnadný úkol a někdy je nezbytné vymezení systému i revidovat. Hrozí potenciálně dvě rizika. Nejčastější je riziko toho, že podlehneme dojmům, že „vše souvisí se vším“, do analyzovaného systému zahrneme příliš mnoho věcí a systém bude příliš rozsáhlý a nepřehledný. Nepůjde pak udělat racionální analýzu a místo ní získáme buď povrchní hodnocení ve smyslu „knížecích rad“ jako „je nutné zajistit bezpečnost“ nebo tak komplikovaný výčet dílčích výsledků, že nebude možné se v něm orientovat. Nebezpečný je i druhý extrém, tedy příliš zúžený systém, kdy sice analyzujeme rizika, ale neúplnost systému nám nedovolí najít a zvládnout příčiny.

Cenným pravidlem je zde při definici systému k analýze a k řízení vycházet z pozice vlastníka rizik a zahrnout všechny chráněné a oprávněné zájmy nositelů rizik, kteří jsou potenciálně ohrožováni zdroji nebezpečí, za které je vlastník rizik odpovědný. Nesmíme však zapomínat na to, že i komunita nebo společnost (obvykle reprezentované státem nebo samosprávou) mohou být jak nositeli, tak vlastníky rizik.

Zajímavá je situace v případech, kdy mezi ohrožené entity patří složky životního prostředí. Náš pohled je prakticky vždy antropocentrický, ale rostoucí uvědomění toho, že životní prostředí je nedílnou součástí nejen zdrojů pro život společnosti, ale i kvality života a vytváří základnu pro udržitelnost společnosti a jejích aktivit v budoucnosti, takže při ohrožení životního prostředí je nositelem rizik také lidská společnost jako taková. Opět zde nastupuje reprezentace státem a komunitou.

Základní způsob vymezení technologických částí systému, které budou předmětem analýzy, je vymezení podle technologických funkcí nebo podle prováděných činností. K analýze volíme takovou část technologie, která tvoří funkční celek, tedy která funguje jako samostatná nebo oddělitelná část technologie. Hranice systému pak tvoří například místa, kde lze zavřít a otevřít potrubí, odepnout nebo zapnout přívod energie, pohyb materiálu nebo přenos informací, zastavit nebo spustit operaci. Tím se vytváří zázemí pro preventivní a nápravné akce. Na základě funkcí lze dělit i životní prostředí, například vodní tok, nepropustný akvifer atd.

Do vymezení systému podle funkce patří i zahrnutí činností, které potřebujeme zachovat, a na něž může nežádoucí událost negativně působit, tedy například infrastruktura, činnosti vedoucí ke vzniku obživy či bohatství, k zajištění udržitelnosti

atd. Víceméně zde vycházíme z principů využívaných v rámci ISO 22 301 Business continuity management systems.

Vymezení v prostoru

Druhou možností vymezení systému, často kombinovatelnou s předešlou, je vymezení v prostoru, tedy podle geografických hranic. Základním kritériem je prostorové umístění zdroje rizika a odhad možných dosahů účinků nežádoucí události. To vede k nutnosti zohlednit vlastnické vztahy, protože majetek je obvykle dobře definován v prostoru, ale také chování složek životního prostředí, například směr toku podzemních i povrchových vod. Do analyzovaného systému by mělo patřit celý prostor, kam až se reálně může šířit přímý dopad nežádoucí události, tedy vše, co může být bezprostředně ohroženo nebezpečím, které hodnotíme.

Kontext problematiky posouzení rizik v rámci řízení rizik

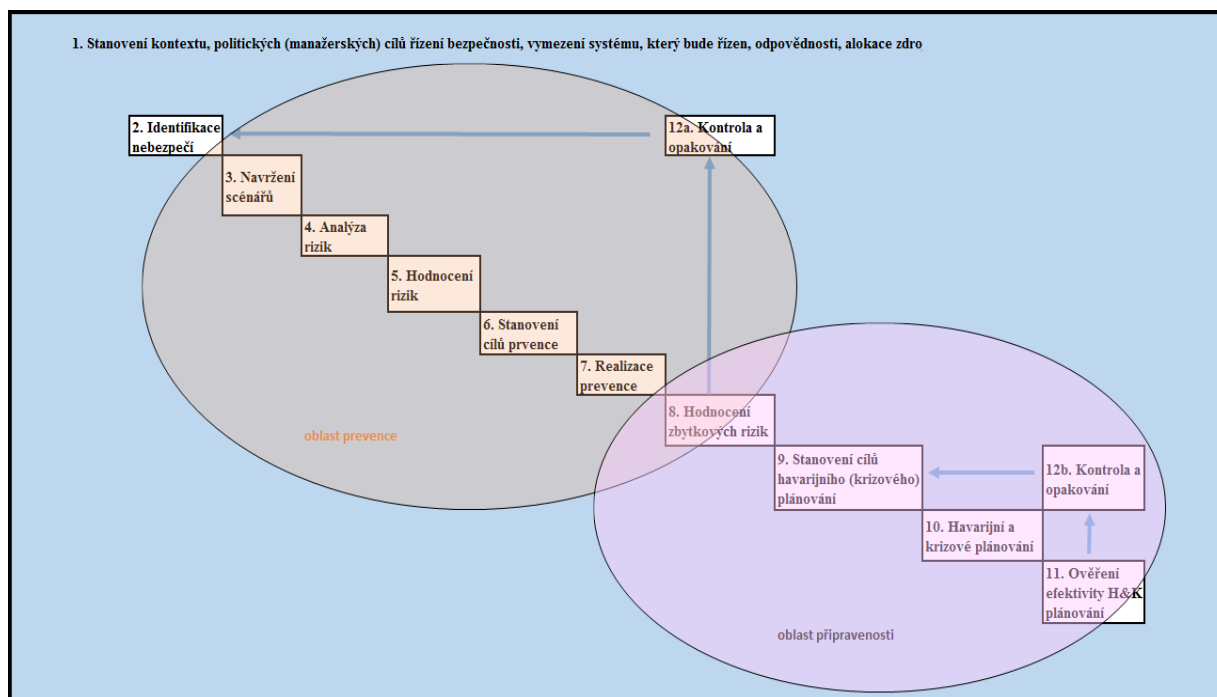
Vazba analýzy rizik na management rizik

Analýza (respektive posouzení) rizik a následující management rizik je proces, který provádíme, ať už intuitivně nebo organizovaně, prakticky každodenně. Při naprosté většině činností a myšlenek zaměřených na budoucnost si vytváříme představu (v organizační a technické praxi pak je to plán, model nebo strategie) toho, jak by se nějaká věc nebo záležitost měla vyvíjet k naší spokojenosti. Jsme si však vědomi toho, že vývoj může postupovat i jinými způsoby, pro nás nežádoucími, a přemýšlíme proto o tom, co by to pro nás znamenalo a jak postupovat, abychom směr vývoje udrželi pro nás žádoucí. To platí i v případě, že nějaký problém už nastal a situace se může, s naším přispěním, vyvíjet různými způsoby. Popsané myšlenkové schéma zahrnuje jak analýzu, tak management rizik a může být provedeno mimovolně a emotivně, ale také vysoce organizovanými způsoby a sofistikovanými technikami; pro dosažení úspěšnosti však vždy vyžaduje provedení série konkrétních kroků v řádném pořadí. Příkladem jednoduché emotivně řešené situace může být i tak banální věc, jako je přecházení frekventované cesty – i zde můžeme nalézt všechny základní kroky analýzy a managementu rizik, tedy identifikace nebezpečí, volba významných scénářů, odhad jejich dopadů a pravděpodobnosti, jejich zhodnocení v kontextu našich dalších potřeb a hodnot, volba preventivních opatření a připravenost pro případ, že by prevence selhala.

Představme si banální situaci, kdy je třeba přejít silnici. Rozhodnutí bezpečně přejít na druhou stranu cesty je rámec a smysl managementu rizik. Rozhlédnutí a konstatování „co jede“ slouží k identifikaci nebezpečí. Úvaha „jak rychle to jede a co by se mohlo stát“ znamená tvorbu scénářů. Zhodnocení, jak moc je pravděpodobný včasný přechod silnice a jaké by byly důsledky (srážka se subtilním děvčetem na in-line bruslích se nerovná přejetí nákladním autem), je analýza, kvantifikace a hodnocení rizik. Stanovení cílů managementu rizik je intuitivní a souvisí s pudem sebezáchovy a prostředky prevence jsou obvykle nasnadě (Počkat až nákladní auto přejede? Utíkat rychle, abych to stihnul? Dojít k přechodu či k podchodu? Vrátit se domů a jet raději autem?). Na zbytková rizika (tedy co zbyde za rizika po provedení prevence) za nás v tomto případě obvykle myslí jiní, a pokud tak prevence selže, připravená a vycvičená zdravotnická služba se pokusí minimalizovat škody. Laskavý čtenář si jistě najde mnoho dalších příkladů. Paradoxem je, že ačkoliv intuitivně je management rizik celkem lehce pochopitelný, v české odborné literatuře existuje jak řada rozporů v názvosloví, tak nedostatek koherence postupů, kdy jsou obvykle dílčí metody deklarovány jako kompletní nebo některé nezbytné kroky chybí.

Chápeme-li koncept rizika a jeho managementu jako projekci do budoucnosti v rámci našich představ o ní, je snadné a správné přijmout i koncept rizika jako vliv nejistoty na dosažení cílů, tedy koncept zpracovaný v normě ČSN ISO 31 000 Management rizik. Proto jsme tuto koncepci využili i v rámci této studie a níže uvedený rozbor procesu analýzy rizik z konceptu ČSN ISO 31 000 vychází a rozšiřuje jej.

Základní schéma jednotlivých kroků a jejich návaznosti v managementu rizik je uvedeno na následujícím obrázku 1:



Obrázek 1 Celkové schéma managementu rizik

Zásadním prvkem managementu rizik je analýza a hodnocení rizik (posouzení rizik). Jak bude ukázáno dále, u analýzy a hodnocení rizik nejde o procesy identické, ale na sebe navazující. Zřídka (pokud vůbec) je prováděno rozhodnutí pouze na základě samotné technické analýzy rizik. Obvykle je rozhodování založeno na širším hodnotovém kontextu toho, kdo rozhodnutí dělá a rozhodnutí je tak vždy ovlivněno vnímáním rizik a dalších hodnot rozhodujícím subjektem – „decision makerem“, tedy je do určité míry subjektivní. Stačí si uvědomit například to, s jakými emocemi je dodnes vzpomínáno na oběti teroristického útoku 11. září 2001 v USA, ale každý měsíc roku 2001 zemřelo na amerických silnicích více lidí, než při útoku na „dvojčata“ (počet obětí teroristu je necelých tři tisíce (START, 2015), počet úmrtí v USA při „motor vehicle accident“ v roce 2001 je přes 42 000 (Wikipedia, 2016)). Zajímavé je i to, že dokonce i počet úmrtí střelnou zbraní v USA je tak velký, že od teroristického útoku 11. září do konce roku 2001 zemřelo tolik lidí, počty úmrtí jsou srovnatelné. Každoročně v USA střelnou zbraní umírá 12 až 15 tisíc lidí.

Výsledek hodnocení rizik závisí také na potenciálním zisku založeném na existenci rizikové situace, na legislativě, na společenském tlaku atd. Jednoduše řečeno, „analytik“ a „decision maker“ nemusí být a často ani nejsou tatáž osoba. S aspektů vztahu mezi analýzou rizik a managementem rizik vyplývají dva fakty:

- Management rizik nemůže dobře fungovat bez správně provedené analýzy a následného hodnocení rizik; jednoduše řečeno, bez nich můžeme snadno řešit bezvýznamná rizika místo podstatných a alokovat naše (vždy omezené) zdroje na nepravé cíle.
- Analýza rizik bez přímého napojení na rozhodovací proces postrádá smysl, nanejvýš se stává samoúčelným technickým a logickým cvičením. Trochu s nadsázkou řečeno, jestliže není analýza rizik navázána na žádný rozhodovací proces, je lhostejné, zda ji provedeme profesionálně na vysoké úrovni, či zda zcela náhodně zvolíme jakákoliv čísla nebo hodnoty. A tato skutečnost platí i v tak absurdních případech, kdy jediným využitím analýzy rizik má být „vyplnění tabulky“ nebo public relations.

Protože analýza rizik, respektive její hodnocení, je propojeno s následujícím řízením (ošetřením) rizik, je nezbytné, aby analýza rizik vycházela z potřeb rozhodovacího procesu, kterému má poskytovat vstupní data. Jinak řečeno, analýza rizik slouží k následnému rozhodování a závisí na něm. Metody analýzy rizik, se kterými máme pracovat, pak musí tento fakt respektovat a analytické metody musí být voleny adekvátně potřebám rozhodování. Bohužel, v praxi se nezdá setkávat se situací, že není zvolena metoda analýzy rizik odpovídající požadavkům rozhodovacího procesu, ale do jisté míry náhodně metoda, řešící pouze některé aspekty problému nezbytné pro správná rozhodnutí, nebo je dokonce jen formálně zaměřená na některý z prvků analyzovaného systému, ale nepodporuje rozhodovací proces, ke kterému by měla být určena. Tato nesprávná volba je často způsobena tím, že pro rozhodovací proces je primárně hledaná metoda již „zaběhnutá“ (např. certifikovaná, ale k něčemu jinému, nebo využívána k rozdílnému typu rozhodování) a není provedena jasná identifikace cílů a rozbor toho, zda zvolená metoda k danému účelu může sloužit.

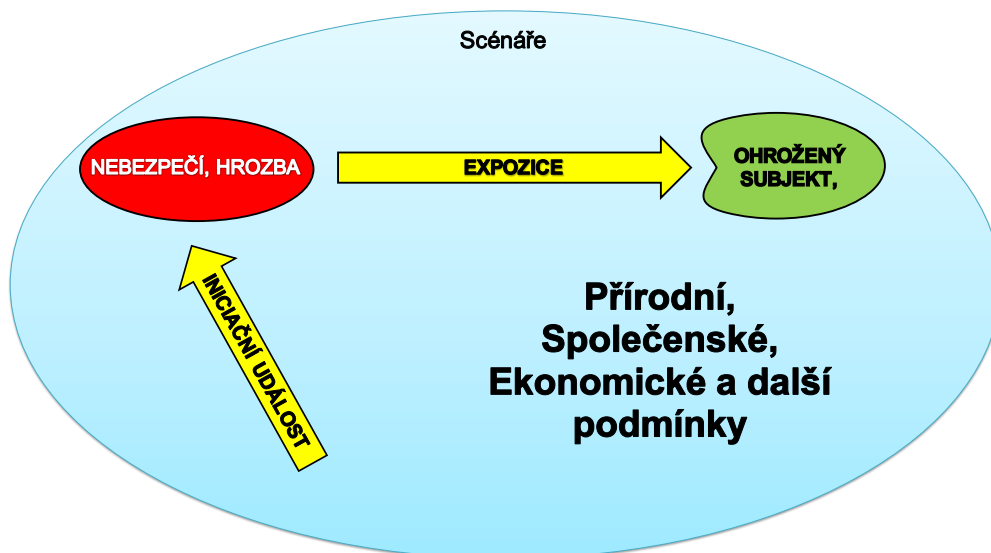
Model šíření nebezpečí a dopadu na cílový systém – myšlenková mapa a terminologie

Při hodnocení rizika je nezbytné nejprve definovat srozumitelnou a nekontroverzní terminologii a klíčové prvky základní teorie rizik, jinak s vysokou pravděpodobností dojde k nepochopení nebo i k nedorozumění. Termíny jako riziko, nebezpečí,

nebezpečnost, hrozba, bezpečí atd. se zdají být jasné a sebevysvětlující, často je však skutečností opak. Obecné povědomí, které většina lidí má o rizicích, vede snadno k pocitu „tohle přece znám“ a k banalizaci potřeby jasných definic. Stačí si však položit jednoduché otázky: „co tyto termíny opravdu znamenají?“, „v čem jsou shodné a v čem se liší?“ a zjistíme nejednoznačnost a rozpory v pohledech různých lidí či institucí. Při rozboru terminologie používané v různých oblastech bezpečnosti pak nezbyde než konstatovat, že terminologie používaná v bezpečnosti je nejednotná a někdy i protichůdná a bohužel v současné době ani neprobíhá celospolečenská aktivita k harmonizaci názvosloví v České republice. Nejedná se však o českou národní specifiku, s obdobným problémem se potýkají i globální organizace jako je OSN a v posledních dvou letech proto pracovala pod vedením UNISDR (Úřad OSN pro snižování rizik katastrof) skupina Open-Ended Intergovernmental Expert Working Group on Indicators and Terminology Relating to Disaster Risk Reduction, jejímž úkolem bylo také sjednocení alespoň základních termínů.

Při hodnocení rizik je řešen soubor problémů, vyplývajících z působení nebezpečí na zranitelný subjekt, objekt nebo záměr. Na celý proces působení nebezpečí tak můžeme hledět jako na interakci mezi nebezpečným zdrojovým systémem (zdrojem rizika) a cílovým systémem (ohroženou entitou), který může být negativně ovlivněn působením nebezpečí. Musí navíc existovat i způsob, kterým se účinek nebezpečí může šířit směrem od zdroje k cíli a mechanismus, kterým je celý proces přenosu nebezpečí odstartován, tedy iniciace nebezpečí nebo tzv. „spoušťový mechanismus“. Zasažený cíl také musí být působením nebezpečí negativně ovlivněn, „zraněn“, tedy být zranitelný.

Schematicky je to zobrazeno na obrázku, a nedodržení přesné terminologie vede nejen k nepochopení, ale snadno i k mylným manažerským rozhodnutím.



Obrázek 2 Schéma působení nebezpečí (procesu šíření nebezpečí)

Nebezpečnost (ekvivalent anglického slova „hazard“) je inherentní vlastnost materiálu nebo situace, která může působit nepříznivě na cílový (ohrožený) systém. Materiál nelze této vlastnosti zbavit, projeví se však pouze v určitých situacích (například hořlavost při hoření) a z pohledu rizik jen tehdy, je-li nějaký cílový systém vlivu vystaven a vliv nebezpečnosti je dostatečně silný na to, aby něco mohl ohrozit. Nebezpečnost u materiálů (chemických látek a směsí) je například hořlavost nebo toxicita, a nebezpečnost je v principu intenzivní vlastnost, tedy např. z pohledu nebezpečných chemických látek je stejnou vlastností jak nepatrného, tak obrovského množství látky. Přidáme-li k určitému objemu metanu ještě jednou stejný objem, hořlavost zůstává stejná. Jinak řečeno, zemní plyn je hořlavý, ať už je ho hodně nebo málo, kyanid má toxicitu v malém i velkém množství atd. U chemických látek, hlavně u těch uváděných na trh nebo průmyslově využívaných, je dobrým zdrojem pro identifikaci nebezpečnosti povinný bezpečnostní list.

V praxi může být dobrým pomocníkem při identifikaci nebezpečnosti v případě chemických látek a směsí, systém norem a bezpečnostních předpisů (CLP a REACH legislativa) včetně bezpečnostních listů. Je však nezbytné nespouštět ze zřetele, že tyto předpisy a normy identifikují významné a předem určené formy nebezpečnosti, nikoliv však nezbytně **všechny** formy. To vede k situacím, kdy sice není nějaká forma nebezpečnosti identifikována, například protože vůbec není podle legislativy testována, avšak se může projevit, a to někdy i velmi dramatickým způsobem.

Uveďme si několik příkladů:

- Při požáru v silničním tunelu pod horou Mont Blanc (1999), stejně tak jako při požáru lanovky v lyžařském středisku v Kaprunu (Rakousko, 2000) se projevila nebezpečnost zplodin hoření materiálů jinak považovaných za neškodné – plastů, mouky, margarínu, lyžařského vybavení...
- V průmyslu je známo mnoho případů, při nichž došlo k explozím způsobeným rozvířeným prachem materiálů nepovažovaných běžně za nebezpečné, jako jsou uhlí, mouka, cukr...
- V koksovně Šverma v Ostravě došlo před několika lety k explozi, způsobené pozvolným vypařováním benzenu z odpadní vody do zásobníku, ačkoliv testy podle standardních požadavků neprokázaly bod vzplanutí při žádné teplotě. Jev byl způsoben pomalým odpařováním hořlavé složky, což je mimochodem jedno z možných nebezpečí i pro zemní plyn z opuštěných, ale netěsnících vrtů.
- Při havárii odkaliště v Ajka (Maďarsko, 2010) se zpočátku provozovatel bránil tím, že materiál odkaliště není klasifikován jako nebezpečná látka podle CLP (REACH). Značné škody způsobené zvýšením pH, suspendovaným materiálem ve vodě a patrně i vysokým CHSK ovšem tuto argumentaci rychle vyvrátily.

Nebezpečnost (hazard) je často definována jako zdroj nebezpečí a termíny nebezpečnost a nebezpečí není možné volně zaměňovat.

Nebezpečí (ekvivalent anglického slova „danger“) je situace nebo stav, kdy může dojít k projevu nebezpečnosti, tedy musí být přítomen i cílový systém. Nebezpečnost se mění v nebezpečí tehdy, jestliže:

- se nahromadí dostatek nebezpečnosti – nebezpečné látky je dost velké množství, aby způsobila škodu, nebezpečná situace má dostatečně velký potenciál způsobit škodu, například dostatkem energie k dispozici.
- zároveň existuje potenciálně ohrožený subjekt – cíl, na který mohou účinky dopadnout. Tím může být život a zdraví člověka nebo kvalita života, životní prostředí, majetek, zdroje obživy nebo funkce společnosti, ale i naše plány do budoucna nebo kvalita života.

Na rozdíl od nebezpečnosti v sobě pojem nebezpečí latentně ukrývá existenci ohroženého cíle – proto se říká, že někdo či něco je v nebezpečí. Nebezpečí je tedy jakási potenciální materializace nahromaděné nebezpečnosti vůči ohroženému cíli,

ale stále ještě bez bližšího určení velikosti dopadu, způsobu dopadu a nejistoty toho, zda vůbec může nastat. Z pohledu našeho případu to znamená, že nebezpečí není samotná chemická látka či směs (ropa, zemní plyn), jak je někdy i v odborné literatuře mylně vykládáno. **Nebezpečí je tedy existence dostatečného množství nebezpečného materiálu (materiálu, jehož vlastností je nebezpečnost) nebo situace s dostatečným potenciálem nebezpečnosti, a to na místě, kde nelze vyloučit zasažení zranitelného cíle.** Nebezpečí je tedy veličina extenzivní – přidáme-li k určitému objemu ropy ještě jednou stejné množství, nebezpečí jí tvořené se zvětší, ale jak bylo uvedeno výše, nebezpečnost ropy zůstane stejná. Dvě stejně velká nebezpečí jsou v sumě větší nebezpečí než každé samo o sobě, neexistuje však vědecký důkaz, že by mělo být nebezpečí lineárně aditivní. To souvisí jednak s projevy nebezpečí z hlediska jejich šíření a kinetiky, jednak s tím, že zranitelnost není konstanta.

Ze vztahu mezi nebezpečím a ohroženým cílem je zřejmé, že aby se mohlo nebezpečí projevit, musí být cíl (pro jednoduchost budeme nadále takto nazývat ohrožený subjekt, zájem, plán nebo materiální statek) vystaven (exponován) působení nebezpečí. Odtud se odvíjí význam **expozice**, kterou je situace, ve které je ohrožený cíl vystaven působení nebezpečí. Aby mohlo dojít k expozici, musí existovat realistický **scénář**, jak může dojít k přenosu nebezpečí a jeho účinku od zdrojového systému k cílovému.

V praxi se setkáváme i s důležitým pojmem **zranitelnost** (ekvivalent anglického „vulnerability“), což je vlastnost cíle (ohroženého systému) projevená formou negativní reakce (poškození, zranění, ztráta kvality...) na působení nežádoucího jevu, např. působení chemické kontaminace, sálavého tepla nebo tlakové vlny. Jedná se o vnitřní vlastnost systému cíle, kterou nelze poznat bez působení nežádoucího jevu minimálně ve formě modelu. Jinými slovy je to vyjádření, jak moc je cílový systém negativně ovlivňován projevem nebezpečí. Inverzní hodnota ke zranitelnosti je odolnost. Celkový dopad havárie je tak kombinace projevu havarijního děje a zranitelnosti / odolnosti cíle. Typickým případem, kdy se dopadům nehod v průmyslu chceme vyhnout zvyšováním odolnosti, jsou požárně odolné konstrukce a požární stěny, z aktivních prvků pak protivýbuchové klapky.

Exaktně vzato není zranitelnost konstanta, ale je funkce velikosti škodlivého účinku, matematicky vzato, je to první derivace velikosti škod podle velikosti škodlivého účinku. Jako taková je tedy zranitelnost funkce.

Jakmile tedy určíme nejen nebezpečí, ale i jeho potenciální dopad a jeho pravděpodobnost, přecházíme do další kategorie, a to k riziku. Riziko v sobě zahrnuje ve skutečnosti obvykle tři aspekty, kterým se budou podrobněji věnovat další kapitoly:

- velikost dopadu,
- pravděpodobnost (nejistota), že havárie nastane,
- naše hodnocení, obvykle skryté ve vnímání rizik.

Na rozdíl od nebezpečí riziko již obsahuje jeden konkrétní nebo více scénářů, co a jak se může stát. Skutečnost, že riziko v sobě zahrnuje scénáře, přináší významný prvek, a to je možnost ovlivnění rizika metodami řízení, tedy managementem bezpečnosti. Zvláště významný je tento prvek v případě, kdy nemůžeme úplně odstranit zdroj rizika (nebezpečí). Jednoduchý ilustrativní příklad toho, jaký je rozdíl mezi nebezpečím a rizikem, je uveden na obrázku 3.



Obrázek 3 Nebezpečí a riziko

Představme si v domácnosti lahvičku s jedem. Nebezpečnost je toxicita tohoto jedu a je stejná, ať už jedu máme mnoho nebo málo. Nebezpečí je skryto v možnosti, že někdo, třeba malé dítě, tento jed pozře v množství, které mu ublíží. Velikost nebezpečí (schopnost otrávit) je stejná, ať už je lahvička s jedem v sejfě nebo mezi

hračkami v dětském pokoji, protože je stejná nebezpečnost i množství nebezpečné látky. Různé však je riziko jako pravděpodobnost vzniku škody, a tak i při stejném nebezpečí lze dosáhnout toho, aby riziko bylo dostatečně malé. Způsoby, kterými toho dosahujeme, jsou předmětem managementu rizik, respektive jeho části zvané ošetření rizik (anglicky risk control).

Celkové schéma managementu rizik, adaptované z ISO/ČSN 31 000 „Řízení rizik“, bylo uvedené výše. Je zde nezbytné připomenout, že se jedná o řetěz navazujících kroků a má-li management rizik dobře fungovat, musí být každý článek tohoto řetězu dostatečně pevný. Zde je skryta nejčastější příčina selhání managementu rizik – některý z kroků nebyl vůbec proveden, popřípadě byl proveden jen symbolicky nebo intuitivně. Management rizik je projekce do budoucnosti, a tak může být snadno náchylný k podcenění nebezpečí nebo rizika, k vypracování pouze symbolického managementu a dokonce i k potlačení „nepříjemných“ stránek managementu vedením. Nejčastější chyby při managementu rizik jsou:

- Rozhodující autorita nepřijme bezpečnost jako skutečnou prioritu, ale uspokojí se pouze s formální dokumentací o bezpečnosti, která nemá oporu v realitě.
- Podvědomě se vytlačí události s velkým dopadem, ale s malou pravděpodobností s tím, že „to se nám nemůže stát“ nebo „to se stane až někomu po nás“.
- Opomenou se významné zdroje rizik.
- Opomenou se významné scénáře.
- „Upraví“ se výsledky analýzy rizik, aby nepůsobily negativně.
- Management skončí u konstatování rizik a nenásleduje rozhodnutí o změnách a alokaci prostředků.
- Není kontrolováno, zda bezpečnostní opatření a havarijní plány opravdu fungují.
- Management bezpečnosti se provede jako jednorázová akce (a je rychle zapomenut) a není následován cyklickým opakováním a neustálým zlepšováním.

Při diskusi názvosloví je třeba zmínit ještě dva důležité termíny, a to je **vlastník rizika a nositel rizika**; tyto subjekty obecně nejsou stejné. Vlastník rizika je ten, komu patří nebo kdo ovládá zdroj rizika, tedy nebezpečný materiál nebo rozhodující

složky nebezpečné situace. **Vlastník rizika** z něj často má nebo v minulosti měl profit, ale je také za něj zodpovědný, tedy může být hnán k odpovědnosti nebo být nucen k nápravě škod či k odstranění rizika. Bohužel, zvláště v souvislosti s životním prostředím vlastnictví rizika je někdy komplikované a nejednoznačné a často se setkáváme se situací nebo i snahou dosáhnout toho, že vlastník rizika není identifikován a odpovědnost za rizika je připisována „vyšší síle“ – *vis major*. Záležitost má faktickou a právní rovinu. V našem případě likvidovaných vrtů se tak objevují důležité otázky jako je odpovědnost původního provozovatele, státu a současného i budoucího majitele pozemku, na kterém vrt je.

Nositel rizika je subjekt, který má nebo může mít z rizika škodu, tedy je to ten, jehož zájem je ohrožen. Jak už bylo zmíněno, nositel rizika není obecně identický s vlastníkem rizika (i když může být), a tedy může být v situaci, kdy nemá a nikdy neměl z rizika žádný zisk, ale jen komplikace a ztráty. Jeho situace je tedy nevýhodná a měl by používat ochrany ze strany společnosti, ve zjednodušení státu. Ten reguluje například předpisy nebo legislativními akty, ale i dalšími ekonomickými i ostatními nástroji, vztahy mezi vlastníkem a nositelem rizik a je tedy v roli **regulátora**.

Vymezení v čase

Toto vymezení je významné zvláště začneme-li uvažovat o tom, zda hodnotíme rizika vyplývající z už existující aktivace hrozeb, tedy například jestliže již došlo ke kontaminaci určitého území (např. úniku ropy ze sondy) a smyslem analýzy bude zjistit potenciální dopady na okolí, a tedy se vlastně nejedná o analýzu rizik v plném rozsahu, ale spíše o analýzu možných dopadů, nebo jestli je uvažována skutečná úplná analýza rizik, tedy kombinace dopadu a pravděpodobnosti, že k tomuto dopadu dojde někdy v budoucnosti.

V praxi se lze setkat se třemi alternativami analýzy týkající se rizik s ohledem na čas, respektive se dvěma analýzami rizik a jedním postupem v analýze rizik využívaným, i když poněkud zjednodušujícím. Nejúplnějším případem analýzy rizik je takové vyjádření v čase kdy se za nejistotu používá pravděpodobnost vzniku v budoucnosti, tedy pravděpodobnost, že nějaká situace nastane ve vymezeném čase popřípadě očekávaná frekvence události nebo to čemu se říká čas opakování chyby, nebo čas opakování události spolehlivosti. Vymezení v čase může být dvojí, relativně nejčastější je vyjádření ve formě frekvence, tzn., že jako jedna proměnná rozhodující

o riziku např. vyjadřována na grafu rizika ve formě dvojrozměrné plochy nebo matice, je frekvence. Frekvence události je vyjádřena jako reciproká hodnota času, tedy hodnota, se kterou se s největší pravděpodobností bude jev opakovat. Tato hodnota může být trochu matoucí, pokud si neuvědomíme skutečný význam frekvence, což si znázorníme na příkladu a to, že častou formou frekvence jsou hodnoty u povodní, například termín sto letá voda, tento termín nám udává očekávanou frekvenci jedenkrát za 100 let. Musíme si ale uvědomit, že průměrná frekvence jednou za 100 let vůbec neznamená, že se bude příslušná událost povodeň cyklicky opakovat jednou za 100 let a mezitím nenastane. Jedná se čistě o pravděpodobnostní vyjádření a klidně se může stát, že 100 letá povodeň může být dva roky po sobě nebo dokonce v jednom roce dvakrát. Ukázka toho může být povodně v Praze, kdy před rokem 2002 kdy byla více než stoletá (cca třisetletá) povodeň, téměř 150 let žádná stoletá povodeň nebyla, ale v předcházejících 45 letech byly tři. Určitá výhoda vyjádření ve formě frekvence spočívá v tom, že se dá použít na velmi dlouhé časové úseky, ale to je však poměrně ošidné. Systém tak jak je analyzován, se v čase také vyvíjí a jeho vlastnosti se za několik let, nebo desetiletí nebo století, jak udávají analýzy rizik, zdaleka nebudou takové, jaké byly v době provádění analýzy a proto je potřeba se na toto vyjadřování dívat velmi opatrně a vždy zvažovat hranice jeho možnosti.

Druhou možností vyjádření v čase, je taková situace, kdy zvolíme časový úsek, pro který analýzu děláme např. dobu využívání, dobu stavby v podnikatelské sféře, očekávaná doba existence podniku, pro tento časový úsek určíme pravděpodobnost, že v jeho průběhu dojde k nežádoucí události. V takovém případě je významné zvažovat, jaký časový úsek bereme v úvahu a tomu analýzu přizpůsobit, protože při dalším časovém úseku je pravděpodobnost z nežádoucí události větší. Z environmentálního a legislativního hlediska je potřeba si uvědomit, že některé odpovědnosti trvají v podstatě stále, ale jenom mohou v budoucnosti přecházet z jednoho subjektu na druhý, například lze přecházet z podniku na stát nebo na komunitu. Z formálního hlediska se tyto dva způsoby vyjádření dají rozlišit velmi snadno., A to, že první případ frekvence musí mít v kvantitativním hodnocení uvedenou reciprokou hodnotu času, tedy např. jedenkrát za 100 let nebo že frekvence je 10^{-4} za rok. Naproti tomu pravděpodobnost je bezrozměrná veličina, a proto je uváděná jako pouhé číslo. Na druhou stranu je potřeba dbát na to aby

nedošlo k záměně a při vyjadřování ve formě frekvence se neopomenula časová veličina tedy respektive veličinu reciprokého času k hodnotě uvést. Obě dvě dosud zmíněné metody vyjádření v čase se dají zařadit jako probabilistické metody, tedy pracující s pravděpodobnostmi. A tím se liší od poslední z využívaných metod, která je pro svou jednoduchost využívána relativně často, jedná se o metodu nazývanou deterministická, na rozdíl od předchozích probabilistických. Deterministická metoda je založená na předpokladu, že jestliže najdeme nejhorší možný scénář a tento dostatečně ošetříme tak tím v dostatečné míře snižujeme také ostatní rizika. Deterministická analýza tedy víceméně s vymezením v čase nepočítá, předpokládá se, že nastane nejhorší možná situace. V praxi se tato metoda využívá pro velmi vysoká rizika s nízkými pravděpodobnostmi. Například v případě výjimečných jaderných havárií a jiných existenciálních rizik. Princip deterministické metody je také využíván také v případech, kdy už významná část scénáře nežádoucí události nastala, například v případě starých zátěží a již existující kontaminace. V těchto případech nemá smysl zabývat se pravděpodobností nebo nejistotou toho, že ta situace nastane, protože už je zřejmé, že už nastala. Ve skutečnosti analýzu, kterou provádíme, bychom měli nazývat analýza dopadu ne analýzu rizik. Ve skutečnosti je však i v tomto případě termín analýza rizik často používána a vychází ze z předpokladů, že dopad ještě nenastal, může nastat v budoucnosti a například po rozšíření kontaminace do zranitelných míst a ta analýza rizik má smysl se rozhodnout, jestli máme zabránit tomu, aby děj dále pokračoval, ale nebo ho necháme volně probíhat. Pro případ ropných sond by to šlo ilustrovat například tím, že jestliže únik ze sondy je takový, že přirozenou atenuací je zlikvidován dříve, než dojde k nějakému zranitelnému cíli, v tom případě není potřeba dělat další opatření k jeho likvidaci.

Identifikace nebezpečí a jeho zdrojů

- Zdroje nebezpečí a jejich typy, nebezpečné materiály a nebezpečné situace, metody jejich identifikace
- Multihazardy (vícenásobná nebezpečí), způsobená jedním nebo více zdroji
- Hodnocení a výběr nebezpečí včetně multihazardů

Scénáře vedoucí k expozici zranitelného cíle

Návrh a vyhodnocení potenciálních scénářů negativních dopadů na cílový systém představuje další klíčový krok v posouzení rizik. V celém procesu managementu rizik se ve skutečnosti zřídka řeší detailní individuální scénáře, protože by jich byl příliš velký počet, ale důraz je kladen na kombinaci mnoha jednotlivých scénářů.

Při návrhu scénářů platí totéž, jako u identifikace nebezpečí – nenalezený scénář jako by neexistoval pro následující proces rozhodování, tím může dojít k nedostatečné prevenci a nepřiměřené reakci na negativní vlivy. Avšak existuje-li v realitě, může tím pádem zásadním způsobem překvapit nepřipravenou společnost.

Při návrhu scénářů je užitečné obecně respektovat následující zdroje:

- Historii proběhlých událostí v analyzovaném území, a to včetně událostí s malým dopadem, které by se mohly vyvinout hůře.
- Významná je i dávná historická paměť – kroniky, zmínky v archivních dokumentech, vzpomínky pamětníků, jsou-li k dispozici.
- Historie nežádoucích událostí v obdobných podmínkách, ať už v okolí nebo ve vzdálených místech.
- Existující informace o prostorovém rozložení hrozeb (např. mapy rizik, povodňové mapy, mapy nestabilních svahů atd.).
- Existující analýzy rizik, vypracované v minulosti i pro jiné účely.
- Názory expertů na jednotlivé hrozby, např. hydrologů, geologů, meteorologů atd.
- Intuitivní a na obecné zkušenosti založené metody jako je metoda „What-If“ – „Co kdyby“.

Pro vytvoření kvalitních scénářů potenciálních negativních dopadů je nezbytná spolupráce mezi analytikem, znalcem místních podmínek a specialisty; podcenění této součinnosti bylo příčinou mnoha událostí, které svým rozsahem nebo průběhem překvapily. Bezpečnost musí být vždy svázána s konkrétními podmínkami a neexistuje bezpečnost jako taková, ale vždy jen bezpečnost konkrétního území, společnosti, zařízení atd. Historické zkušenosti ukazují, že soustředění se na nejdéle trvající, tedy běžné stavy, nedostačuje a je nezbytné přemýšlet o možných extrémech. Velká část nežádoucích situací nastává za nestandardních okolností vlivem nejen přírodních dějů v okolí, ale i komunity samé, a mnohdy má svůj původ

už v nevhodné koncepci, například v územním plánu. Typické jsou například povodňové škody při ignoraci historických zkušeností, kdy zástavba v záplavovém území zhoršuje průběh povodně tím, že stavby zpomalují průtok vody a mezi nimi a na plotech se vytvářejí dočasné hráze z trosek.

Při tvorbě scénářů, ale i při jejich vyhodnocování v rámci analýzy rizik, je výhodné používat grafická znázornění umožňující pochopení komplexních scénářů. Jedním z vhodných způsobů jsou tzv. stromy poruch (Fault Trees), kdy analýzy pomocí logických schémat poruch umožní nejen vizualizovat scénář havárie, ale také pomocí Booleovské algebry vypočítat pravděpodobnost či frekvenci události a racionálně provádět preventivní opatření. Z tohoto důvodu je analýza stromem poruch (FTA, Fault Tree Analysis) široce využívána v letectví, jaderném i chemickém procesním průmyslu při řízení rizik. FTA je předmětem normy ČSN EN 61025 (010676) „Analýza stromu poruchových stavů“. Tak jako identifikace nebezpečí odpovídá na otázku „co může neštěstí způsobit“, scénáře nám ukazují, „jak se to může přihodit“. Zůstávají však na čistě kvalitativní úrovni a pro kvantifikaci možných problémů musíme přejít k charakterizaci rizik.

Cílem analýzy rizik je charakterizovat riziko, tj. určit šanci, s jakou sledovaný cílový subjekt (typicky obyvatelstvo, životní prostředí, majetek, infrastruktura apod.) utrpí poškození a jaká bude závažnost tohoto poškození. Charakterizace rizika pak slouží jako podklad pro rozhodovací proces o přijatelnosti rizika a často nahrazuje termín „analýzy rizik“, zvláště pak ve frekventovaných případech, kdy některé veličiny v předpovědích nelze exaktně zjistit a analytik se uchyluje ke kvalifikovanému odhadu, nebo když je analýza prováděna semikvantitativně. Postupné kroky charakterizace rizik jsou tři:

- Stanovení intenzity posuzovaného jevu, např. velikost povodňové vlny, rozsah a trvání kontaminace, síla a směr vichřice, rozsah sesuvu nebo množství uniklé toxické látky a modelování šíření tohoto jevu a jeho dopadů. Zde je na místě připomenout, že takováto analýza je vždy nejistá projekce do budoucnosti a že ani sebelepší analýza nemůže přesně predikovat, co se opravdu stane – realita je vždy složitější než naše modely.
- Odhad účinků na základě znalostí vztahů mezi velikostí působícího jevu a účinkem. Tento vztah (mezi velikostí působícího jevu a účinkem) reprezentuje poškození cílového systému (lidské organismy, zařízení, životní

prostředí, funkce komunity, funkce infrastruktury atd.) důsledkem krizových jevů a je vyjádřením funkce zranitelnosti cílového systému. I tady platí totéž, co v předcházejícím bodě – predikce do budoucnosti je nesnadná a ošidná, ale je to to nejlepší, s čím můžeme pracovat.

- Stanovení nejistoty vzniku jevu. V češtině často používaný termín „pravděpodobnost“ může být zavádějící, protože může zahrnovat skutečnou pravděpodobnost, tedy bezrozměrnou veličinu udávající poměr mezi počtem případů vedoucích k neštěstí ke všem případům (např. pravděpodobnost havárie raketoplánů Space Shuttle při jednom letu se ukázala být kolem 0,018). Při řešení mimořádných událostí se ale častěji setkáváme s frekvencí, tedy reciprokou hodnoty očekávané průměrné doby mezi dvěma událostmi (v předchozím případě závisí na počtu letů; u stejného typu raketoplánu činila 0,092/rok). Typickým případem vyjádření frekvence je „stoletá povodeň“, tedy povodeň, jejíž průměrný výskyt je jedenkrát za sto let. Při hodnocení nejistoty („pravděpodobnosti“) hrozí dvě časté chyby:
- Záměna mezi frekvencí a pravděpodobností vede k mylným závěrům a je jednou z nejčastějších chyb při charakterizaci rizika. Všechny děje, vztažené k časovému údaji, jsou frekvence a musíme s nimi jako s frekvencemi zacházet, v první řadě vždy a pečlivě uvádět, k jakému času se váží. Jedenkrát za rok prostě znamená něco jiného než jedenkrát za den.
- Rozložení kritických událostí v čase není pravidelné.

U analýzy rizik je velmi důležité uvést úroveň nejistoty, která je vlastní konečnému odhadu. Je potřeba si uvědomit, že vzhledem k tomu, že charakterizace rizik vychází z integrace dat z předchozích kroků, je potřeba do finální nejistoty zahrnout všechny nejistoty, které s sebou přináší jednotlivé dílčí kroky.

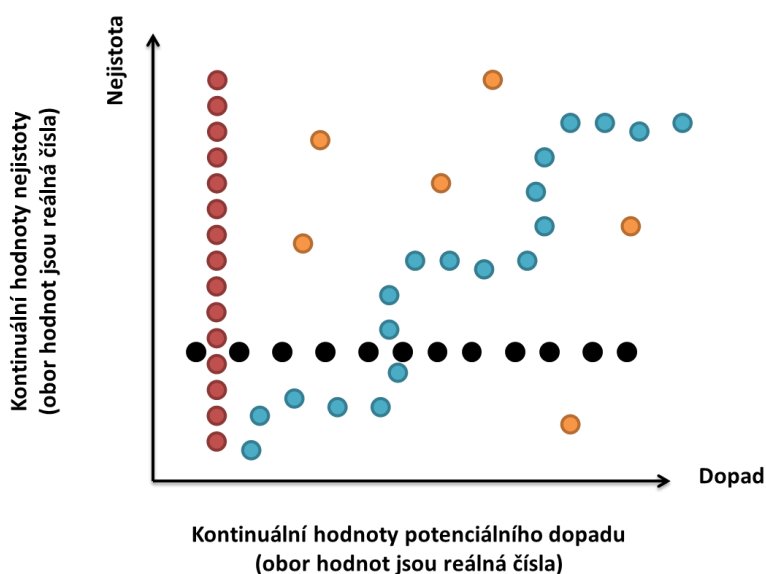
Hodnocení rizik – prostor rizik a matice rizik

Samotné hodnocení rizik je proces, při němž je vyjádřeným rizikům ve formě závažnosti a pravděpodobnosti havárií přiřazována hodnota s ohledem na hodnotový systém organizace či společnosti, která rozhoduje o řízení rizik. Je to tedy přechod mezi čistě technickou a organizační částí řízení rizik. Přejít mezi analýzou (charakterizací) a hodnocením rizika je založen na vnímání a akceptovatelnosti rizik.

Riziko je chápáno jako komplexní funkce zahrnující dopad a jeho nejistotu (pravděpodobnost, frekvenci). To umožňuje nejen vizualizovat rizika ve dvojrozměrném prostoru, ale také je srovnávat a prioritizovat, v konečném důsledku tedy i alokovat prostředky na jejich řešení. Prioritizace zahrnuje i vyřazení těch scénářů, které nebude analytik dále hodnotit. Jsou to především všechny scénáře vedoucí k marginálním dopadům, dále pak scénáře krajně nepravděpodobné, ale vedoucí jen ke středně závažným událostem. Není však správné takto vyřazovat i nepravděpodobné události s extrémně velkým dopadem, protože u tak závažných událostí je již často opouštěna probablistická metoda hodnocení založená na kombinaci pravděpodobnosti a dopadu a je využíván deterministický princip, založený pouze na velikosti dopadu.

Proces analýzy rizik je zakončen odhadem a vyjádřením rizika. Obecně existuje více způsobů, jak riziko pro účely dalšího hodnocení vyjadřovat. K následnému rozhodování je třeba rizika vzájemně porovnat. Ke komparaci můžeme přistupovat různými způsoby.

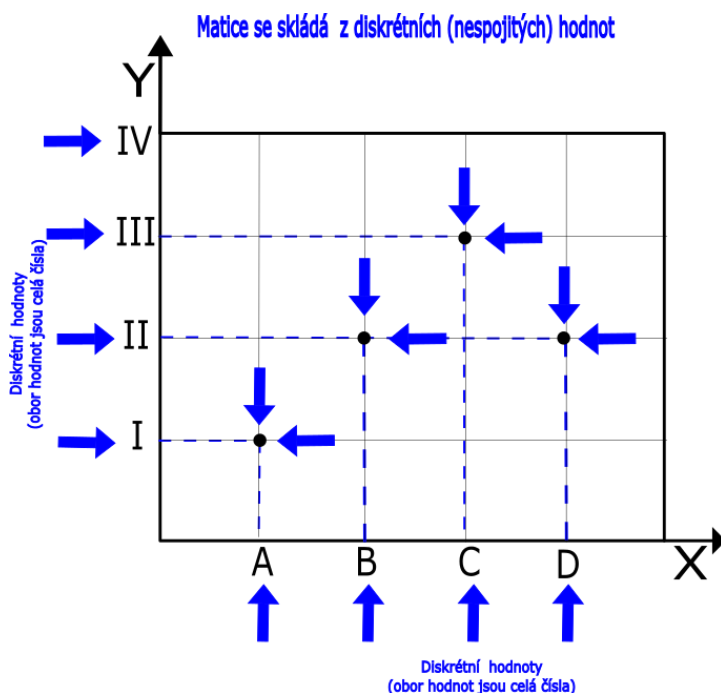
Osy X, Y mohou umožňovat řešení a to jak kontinuální, neboli spojitě, tzn., že všechny proměnné musí být rovněž kontinuální a mohou nabývat všech hodnot v předem definovaném oboru, tak diskrétní (nespojitě) hodnoty. Graficky je matice založená na kontinuitě znázorněna na Obrázku 4.



Jednotlivé body vyznačují rizika; hypoteticky mohou být umístěné libovolně.

Obrázek 4 Dvojrozměrný prostor rizik při kvantitativní analýze

Spojité hodnoty jsou charakteristické pro případ určování jednotlivého pořadí rizik. V případě, že využíváme semikvantitativní metodu, mohou proměnné nabývat pouze konkrétních hodnot (celých čísel) a tyto se mění pouze skokem. Dalo by se také říct, že máme omezený diskrétní počet možností. Diskrétní hodnoty jsou pak charakteristické pro rozdělení do skupin a graficky jsou znázorněny na Obrázku 5. V případě samotné matice rizik může nastat případ, kdy jedna osa bude nabývat kontinuálních hodnot a druhá diskrétních hodnot.

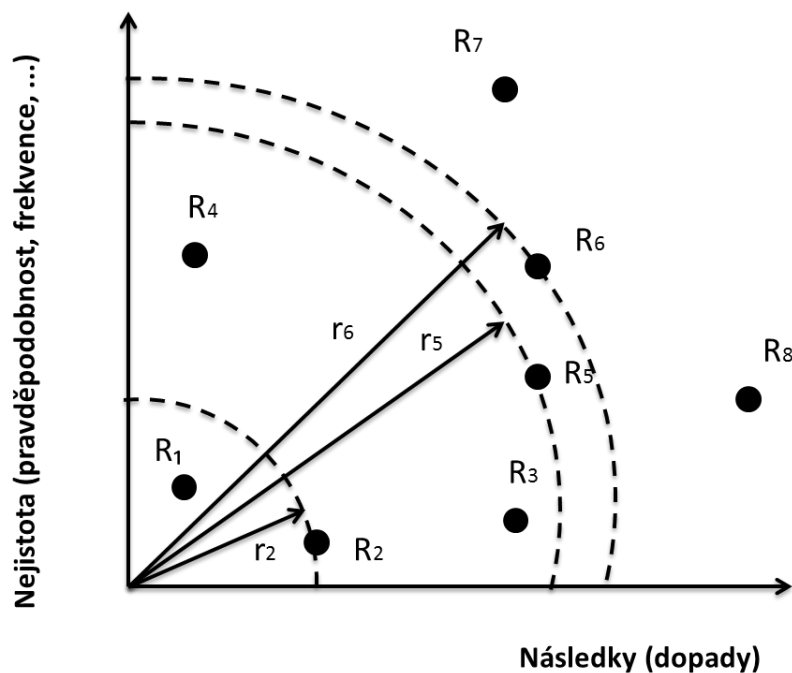


Obrázek 5 Diskrétní zobrazení hodnot

Ukázka matice pro diskrétní hodnoty (kategorie, skupiny atd.) Ve skutečnosti mohou jednotlivá rizika obsadit kterýkoliv „uzlový bod“ – průsečík na grafu, ale ne pozice mezi nimi. Celkový počet možností pak není neomezený jako v případě kontinuálních proměnných, ale obecně jen násobek počtu možných hodnot na obou osách.

K tomu, abychom mohli provést samotnou prioritizaci, ať už kontinuálních nebo diskrétních hodnot konkrétních sond, musíme nejprve provést tzv. síťování. Síťování znamená určení limitních mezí, na jejichž základě budou určovány priority. Jinak řečeno, je potřeba nadefinovat kategorie/úrovně, které umožní komparaci hodnot (vzájemné porovnání). Výsledné hodnocení může být založeno čistě na pragmatickém technokratickém přístupu, nebo může zahrnovat i proces percepce (vnímání) rizik, tedy akceptovatelnost daného rizika společností. Jednou z možností čistě pragmatického hodnocení je měření vzdálenosti kružnice protínající zaznačené

riziko (bod R) od počátku (bod X) s uvedením konvexního úhlu (α) určující koeficient váhy. Tento způsob hodnocení je znázorněn na Obrázku 6.



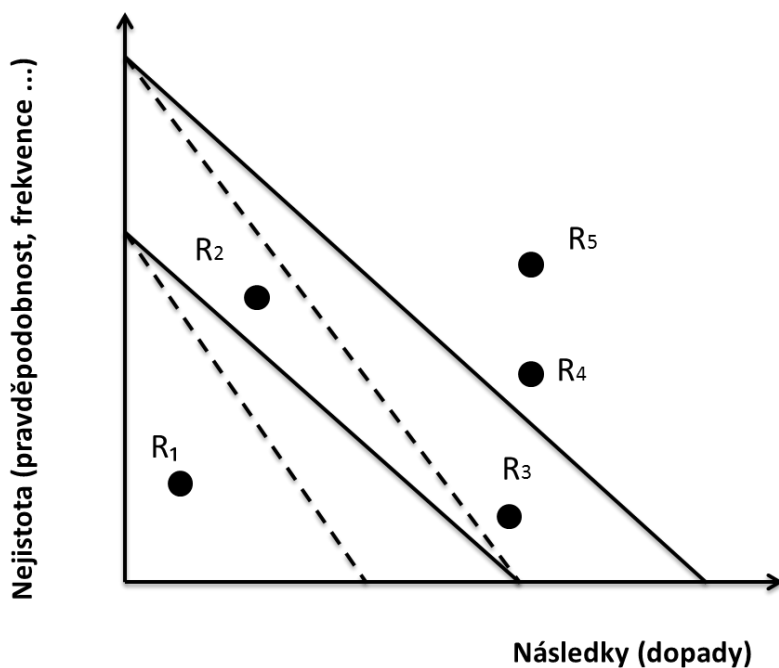
R_n = n – té riziko

r_n = formální velikost n – tého rizika

Jednotlivé body vyznačují rizika; hypoteticky můžou být umístěné libovolně.

Obrázek 6 Velikost rizika v dvojrozměrném prostoru

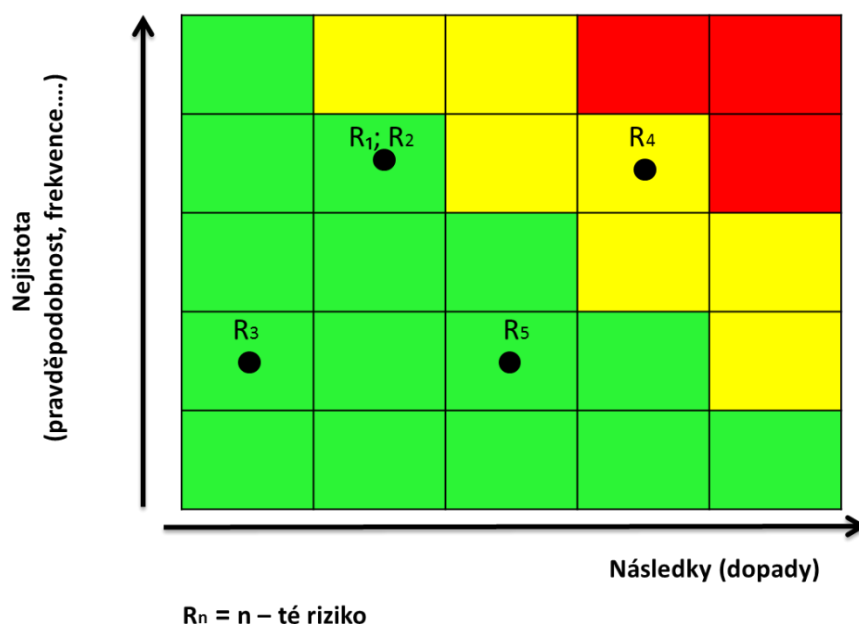
Dalším možným postupem pro hodnocení je rozdělení prostoru diagonálami, u kterých platí pravidlo, čím dále od počátku (od X) tím představuje větší riziko (viz Obrázek 7).



Obrázek 7 Velikost rizika v dvojrozměrném prostoru

Diagonální rozdělení je založeno na vyjádření tzv. izolinií rizika pomocí diagonálně vedených čar. Dvě plně vyznačené linie reprezentují dvě rizika – větší je dále od počátku – a riziko kdekoliv na této linii chápeme jako velikostí stejné. Toto vyjádření již zahrnuje proces percepce rizika na rozdíl od předchozího způsobu hodnocení. Rozdíl ve vnímání je patrný ze sklonu izolinií rizika – čárkované izolinie odpovídají větší averzi k rizikům s kumulovanými (početně velkými) dopady. Zjednodušeně řečeno to znamená například, že jedno úmrtí každý rok nám vadí méně, než nakumulovaných deset úmrtí jednou za deset let. Obecně vzato, izolinie rizika nemusí být přímka, například v případě předepsaného postupu hodnocení přijatelnosti rizika závažné havárie podle zákona č. 224/2015 Sb. je zvolena závislost na druhé mocnině počtu obětí ve vztahu k frekvenci události. To mimochodem potvrzuje nesmyslnost často využívané techniky „výpočtu“ rizika násobením pravděpodobnosti a závažnosti.

Další možností zohledňující akceptovatelnost rizika je způsob zobrazení za pomoci celkového plošného rozdělení do kategorií (např. barevně rozlišených), které představují různou míru přijatelnosti rizika (viz Obrázek 8), tedy v matici rizik.



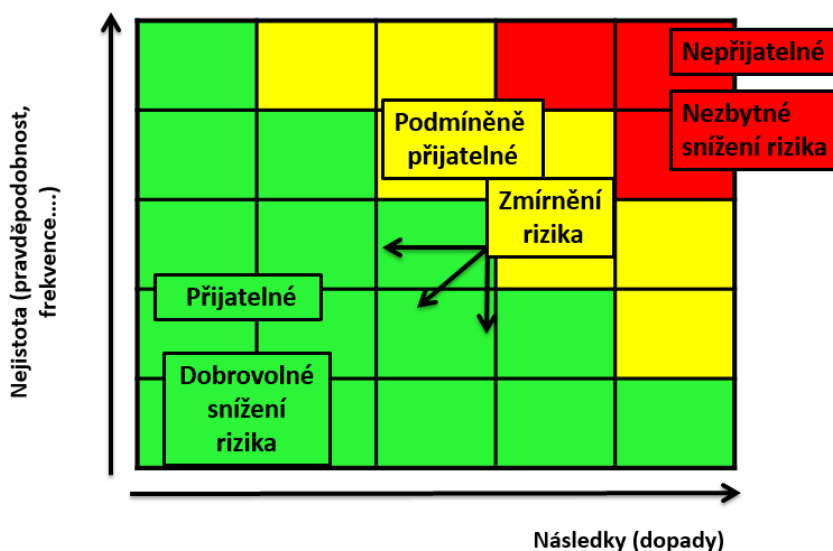
Obrázek 8 Matice rizik

V praxi se setkáváme se dvěma způsoby vyjádření rizika v matici a to kombinací pravděpodobnosti a závažnosti, anebo expozice a zranitelnosti. Základním pravidlem matice je, že s rostoucí expozicí/pravděpodobností současně poroste riziko, stejně tak se bude také zvyšovat spolu se závažností/zranitelností. S konstrukcí matice souvisí i její symetričnost. Můžeme se tedy setkat s maticí čtvercovou, stejně tak i s obdélníkovou.

Jedním z hledisek může být počet kritérií, která budeme hodnotit, tudíž se setkáváme s hodnocením jednoho kritéria nebo s multikritériálním přístupem. V případě jednokritériální metody se hodnotí pouze míra přijatelnosti daného rizika, a to na několika úrovních (např. riziko přijatelné, podmíněně přijatelné a nepřijatelné). Přijatelná rizika není nezbytně bezprostředně řešit, přestože je vždy vhodné snižovat jakákoli rizika. Tolerovatelné riziko je riziko, se kterým je společnost ochotná žít pro zabezpečení blahobytu a v důvěře, že toto riziko je správně řízeno, kontrolováno a dále redukováno, když je to možné. Rizika zhodnocená jako nepřijatelná je nutné co nejdříve eliminovat, jelikož společnost není ochotna nést jejich následky s očekávanou frekvencí.

Právě zařazení do kategorií přijatelnosti vytváří rozdíl mezi analýzou (charakterizací) a hodnocením rizik. Na druhou stranu, jak již napovídá název, multikritériální metoda hodnotí dvě a více kritérií. K tomu slouží primárně vyjádření pomocí takzvané matice rizik, ve které jsou jednotlivá rizika umístěna podle předpokládané úrovně závažnosti

a podle pravděpodobnosti (frekvence). Příklad matice je uveden na obrázku 9. V rámci matice jsou rizika rozdělena do tří kategorií – rizika přijatelná, rizika podmíněně přijatelná a rizika nepřijatelná; v některých zjednodušených případech pouze na dvě. Do matice se na základě analýzy rizik umístí všechny hodnocené scénáře formou bodů.

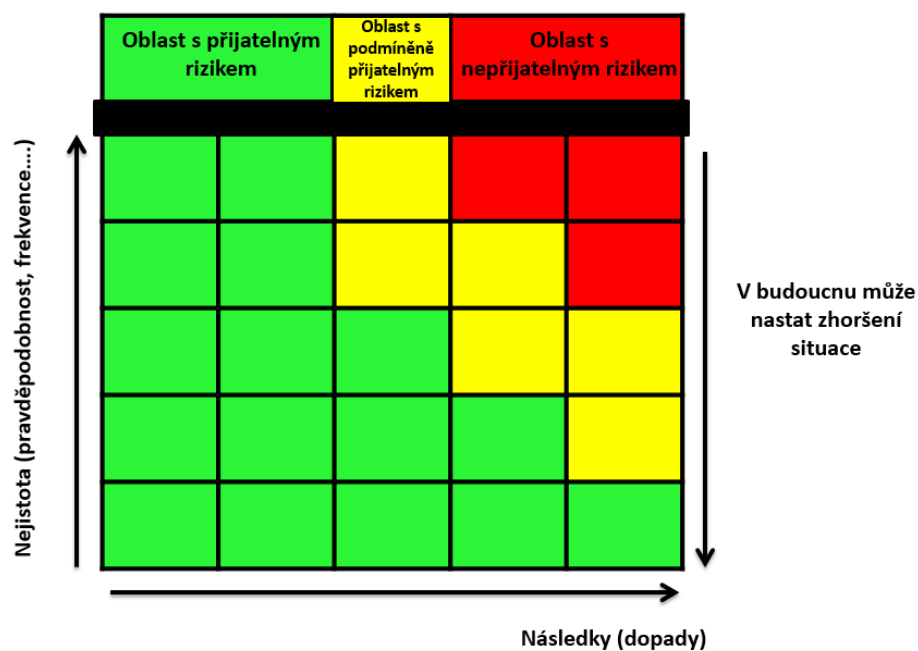


Obrázek 9 Přijatelnost matice rizik

Umístění jednotlivých scénářů formou bodů do matice bez vymezení přijatelnosti reprezentuje analýzu rizik, s vymezením přijatelnosti (v našem ukázkovém případě barevně odlišených oblastech), pak jejich hodnocení; vzdálenost od hranice s další kategorií přijatelnosti pak lze chápat, jako další míru přijatelnosti či nepřijatelnosti, a tudíž využít k přiřazení priorit k jednotlivým scénářům.

Specifika multikriteriálního posouzení rizik

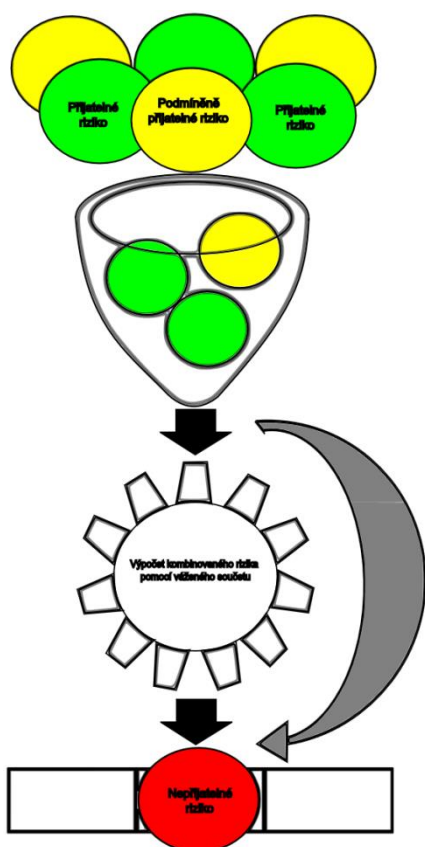
Jak již bylo zmíněno, multikriteriální posuzování rizik je založeno na hodnocení dvou a více kritérií. K vyjádření slouží primárně matice rizik, kde je konkrétně v jednom směru přijatelnost kontaminace a v druhém směru pravděpodobnost opětovného úniku nebezpečných látek z ropoplynové sondy. Tento pohled na posouzení je ovlivněn skutečností, že může s odstupem času dojít k opětovnému úniku a další kontaminaci území. Grafické znázornění upravené matice rizik je uvedeno na Obrázek 10.



Obrázek 10 Matice rizik vyjádření nesymetrie přijatelnosti

Hodnocená kritéria mohou být kvantitativní, využívající číselné hodnoty nebo kvalitativní, jež je založeno na slovních klasifikačních stupnicích. Rozhodování při posouzení rizik může být postaveno na:

- nejvyšší hodnotě;
- součtu nebo váženém součtu;
- součinu nebo váženému součinu;
- jiné matematické operaci;
- aritmetickém nebo geometrickém průměru;
- úsudku experta.



Obrázek 11

Principy managementu rizik

K principům managementu a řízení rizik existuje velké množství literatury zabývající se managementem rizik ve specifických odvětvích. Velmi málo postupů a metod je ovšem univerzálně použitelných a obecně přenositelných. Dalším problémem publikovaných metod je to, že často popisují postupy a činnosti, které sice v daném kontextu slouží svému účelu, ovšem často je obtížně pochopitelné a představitelné, co se při nich vlastně provádí a k jakému účelu slouží. Pro lepší představu je smysl a účel analýzy a hodnocení rizik popsán na jednoduchých a příkladech, vycházejících z běžného života.

Žijeme v nebezpečném světě. Prvním a neměnným pravidlem je to, že nulové riziko neexistuje. Druhým důležitým pravidlem je, že rizika jen zřídka opravdu odstraňujeme, obvykle jen vyměňujeme riziko za jedno nebo více jiných, která považujeme za menší. Abychom se vyhnuli dopadům rizik, provádíme soubor

činností, které můžeme nazývat „management rizik“. Ve skutečnosti jej provádíme každodenně a ve většině svých činností, ale jen neorganizovaně a mnohdy pouze intuitivně. Stačí si uvést jednoduchý příklad, ilustrující kroky managementu rizik:

Představme si banální situaci, kdy je třeba přejít silnici. Rozhodnutí bezpečně přejít na druhou stranu cesty je rámec a smysl managementu rizik. Rozhlédnutí se je identifikace nebezpečí. Úvaha „co jede, jak rychle a co by se mohlo stát“ znamená tvorbu scénářů. Zhodnocení, jak moc je pravděpodobný včasný přechod silnice a jaké by byly důsledky (srážka se subtilním děvčetem na in-line bruslích se nerovná přejetí nákladním autem), je analýza, kvantifikace a hodnocení rizik. Stanovení cílů managementu rizik je intuitivní a souvisí s pudem sebezáchovy a prostředky prevence jsou obvykle nasnadě (Počkat až nákladní auto přejede? Utíkat rychle, abych to stihnul? Dojít k přechodu či k podchodu? Vrátit se domů a jet raději autem?). Na zbytková rizika za nás v tomto případě obvykle myslí jiní, a pokud tak prevence selže, připravená a vycvičená zdravotnická služba se pokusí minimalizovat škody. Laskavý čtenář si jistě najde mnoho dalších příkladů. Paradoxem je, že ačkoliv intuitivně je management rizik celkem lehce pochopitelný, v české odborné literatuře existuje jak řada rozporů v názvosloví, tak nedostatek koherence postupů, kdy jsou dílčí metody deklarovány jako kompletní.

S managementem rizik se tedy setkáváme ve všech oblastech a fázích života. Tento proces, jehož cílem je optimalizace rizik, sestává ze dvou základních částí – z analýzy rizik a ošetření rizik. Názvosloví v oblasti managementu rizik se v současnosti dynamicky vyvíjí a v literatuře i praxi najdeme mnoho příkladů protichůdných nebo i nesprávných názvů, počínaje roztomilým komickým anglikanismem „riziková analýza“, což je podle pravidel českého jazyka „analýzy přinášející rizika“. Z tohoto důvodu se autoři drží názvosloví, které jim připadá nejlogičtější, a to názvosloví používaného v normě ISO/EN/ČSN 31 000 „Řízení rizik“.

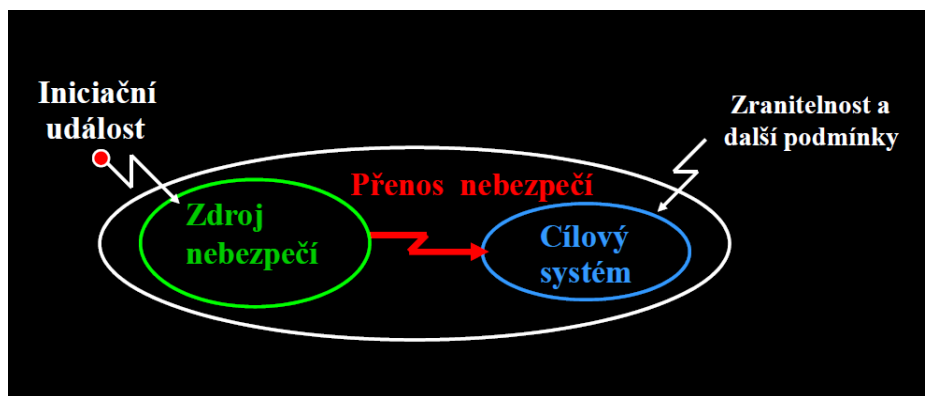
Základními pojmy celého managementu rizik jsou „nebezpečnost“, „nebezpečí“ a „riziko“. Tyto pojmy bývají často zaměňovány, což vede k nepochopení a někdy i k nehodám. Nebezpečí chápeme jako zdroj potenciálního poškození nebo újmy [112].

Riziko je pak účinek nejistoty na dosažení cílů. Účinek je zde chápán jako odchylka od očekávaného a obecně může být nejen záporná, ale i kladná. Cíle mohou mít

různá hlediska (jako jsou finanční, zdravotní a bezpečnostní a environmentální cíle) a mohou být uplatňovány na různých úrovních (jako je strategická úroveň, úroveň týkající se celé organizace, projekt, úroveň produktu a procesu).

Rizika jsou obvykle charakterizována odkazem na potenciální události a následky nebo na jejich kombinaci. Riziko se často vyjadřuje jako kombinace následků události (včetně změn okolností) a s ní související možnosti výskytu [112]. Nebezpečí tak může být chápáno jako zdroj rizika. V praxi a v odborné literatuře se opět setkáváme s nejednotnou terminologií. Často není rozlišováno také mezi pojmy nebezpečnost a nebezpečí. Pro lepší porozumění si uvedeme zjednodušené, ale ilustrativní příklady.

Na celý proces šíření nebezpečí můžeme hledět jako na interakci mezi zdrojovým systémem (zdrojem rizika) a cílovým systémem, který je ohrožován působením nebezpečí. Musí navíc existovat i způsob, kterým se účinek nebezpečí může šířit směrem od zdroje k cíli. Schematicky je to zobrazeno na obrázku 12, a nedodržení přesné terminologie vede nejen k nepochopení, ale i k mylným manažerským rozhodnutím. Detailnější popis schématu procesu šíření nebezpečí byl rozebrán na obrázku 12.



Obrázek 12: Schéma přenosu nebezpečí. Adaptováno z metodologie MADS-MOSAR [74]

Nebezpečnost (ekvivalent anglického slova „hazard“) je inherentní vlastnost materiálu nebo situace, která může působit nepříznivě na cílový systém [109]. Látku nelze této vlastnosti zbavit, projeví se však pouze tehdy, je-li nějaký cílový systém vlivu vystaven. Nebezpečnost je například hořlavost nebo toxicita, a je to v principu

intenzivní vlastnost, tedy z pohledu nebezpečných chemických látek je stejnou vlastností jak nepatrného, tak obrovského množství látky. U chemických látek je nejlepším zdrojem pro jejich nalezení povinný bezpečnostní list. Nebezpečnost (hazard) je často definována jako zdroj nebezpečí [109].

Nebezpečí (ekvivalent anglického slova „danger“) je situace nebo stav, kdy může dojít k projevu nebezpečnosti, tedy musí být přítomen i cílový systém. Nebezpečnost se mění v nebezpečí tehdy, jestliže nebezpečné látky je dostatečně velké množství, aby způsobila škodu, a jestliže existuje potenciálně ohrožený subjekt – cíl, na který mohou účinky nebezpečí dopadnout. Tím může být život a zdraví člověka nebo kvalita života, životní prostředí, majetek nebo funkce společnosti. Nebezpečí je tedy jakási materializace nebezpečnosti vůči ohroženému cíli, ale stále ještě bez bližšího určení velikosti dopadu a nejistoty toho, zda nastane. Nebezpečí není samotná chemická látka (v případě energetiky nejčastěji palivo), jak je někdy i v odborné literatuře mylně vykládáno. Na rozdíl od nebezpečnosti v sobě tento pojem latentně ukrývá existenci ohroženého cíle – proto se říká, že někdo či něco je v nebezpečí. Oproti nebezpečnosti v sobě navíc zahrnuje množství látky. Například nebezpečnost zemního plynu, tedy schopnost vybuchovat ve směsi se vzduchem, bude stejná, ať už se uvažuje 1 kg nebo 100 tun. Nebezpečí však bude u 100 tun určitě vyšší. Příkladem nebezpečí může být nebezpečí výbuchu metanu v uvnitř kotle, nebezpečí požáru apod. Nebezpečí už je tedy extenzivní veličina, dvě stejně velká nebezpečí jsou v sumě větší nebezpečí než každé samo o sobě, neexistuje však vědecký důkaz, že by mělo být nebezpečí lineárně aditivní.

V praxi se setkáváme i s pojmem zranitelnost (ekvivalent anglického „vulnerability“), což je vlastnost cíle (ohroženého systému) projevená formou negativní reakce (poškození, zranění, ztráta kvality...) na působení nežádoucího jevu, např. působení sálavého tepla nebo tlakové vlny. Jedná se o vnitřní vlastnost systému cíle, kterou nelze poznat bez působení nežádoucího jevu alespoň ve formě modelu. Jinými slovy je to vyjádření, jak moc je cílový systém ovlivňován projevem nebezpečí. Inverzní hodnota ke zranitelnosti je odolnost. Celkový dopad havárie je tak kombinace projevu havarijního děje a odolnosti cíle. Typickým případem, kdy se dopadům nehod chceme vyhnout zvyšováním odolnosti, jsou požárně odolné konstrukce a požární stěny, z aktivních prvků pak protivýbuchové klapky.

Exaktně vzato je zranitelnost funkce velikosti škodlivého účinku, matematicky vzato první derivace velikosti škod podle velikosti škodlivého účinku. Jako taková není zranitelnost konstanta, ale funkce.

Jakmile tedy určíme nejen nebezpečí, ale i jeho potenciální dopad a jeho pravděpodobnost, přecházíme do další kategorie, a to k riziku. Riziko havárie v sobě zahrnuje nejméně dva a ve skutečnosti obvykle tři aspekty, kterým se budou podrobněji věnovat další kapitoly:

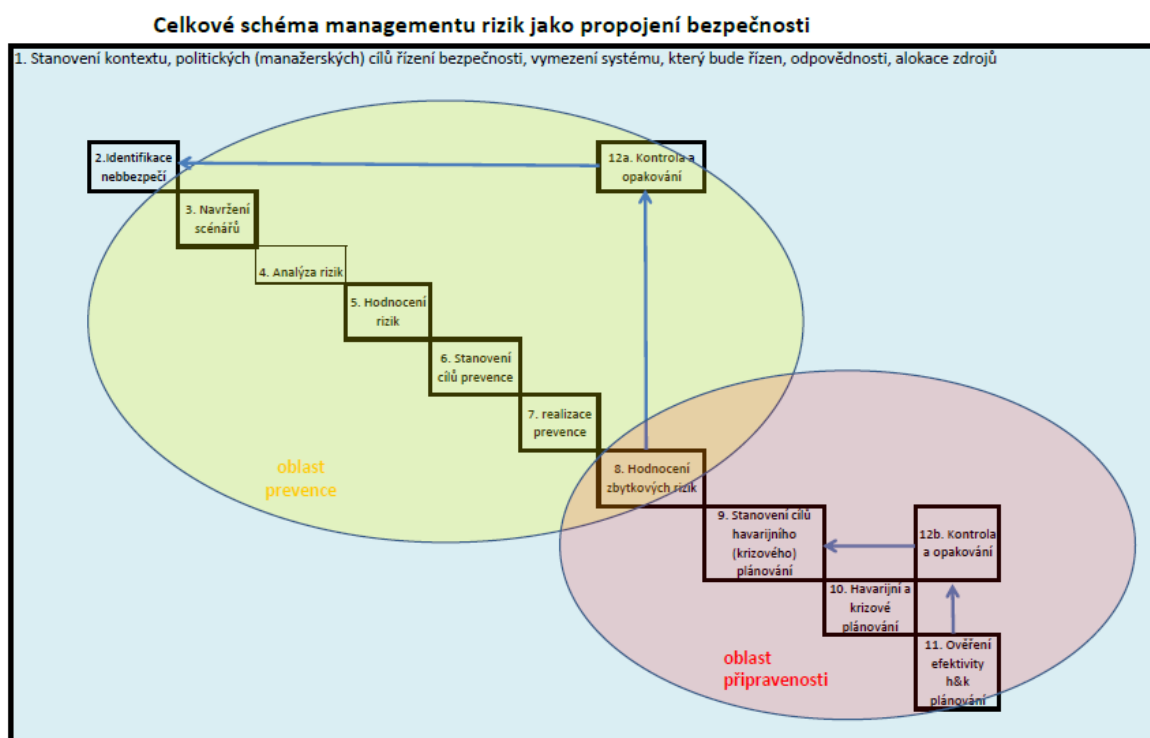
- velikost dopadu
- pravděpodobnost (nejistota), že havárie nastane
- naše hodnocení, obvykle skryté ve vnímání rizik

Na rozdíl od nebezpečí již riziko obsahuje jeden konkrétní nebo více scénářů, co a jak se může stát. Skutečnost, že riziko v sobě zahrnuje scénáře, přináší významný prvek, a to je možnost ovlivnění rizika metodami řízení, tedy managementem bezpečnosti. Zvláště významný je tento prvek v případě, kdy nemůžeme odstranit zdroj rizika (nebezpečí), a paliva v energetice jsou toho typickým příkladem. Není možné vyrábět energii bez paliv (alespoň zatím), ale je možné s nimi zacházet tak, aby rizika nebyla příliš vysoká.

Celkové schéma managementu rizik, adaptované z ISO/EN/ČSN 31 000 „Řízení rizik“, je uvedené na obrázku 13. Je nezbytné připomenout, že se jedná o řetěz navazujících kroků a má-li management rizik dobře fungovat, musí být každý článek tohoto řetězu dostatečně pevný. Zde je skryta nejčastější příčina selhání managementu rizik – některý z kroků nebyl vůbec proveden, popřípadě byl proveden jen symbolicky nebo intuitivně. Management rizik je projekce do budoucnosti a tak může být snadno náchylný k podcenění nebezpečí nebo rizika, k vypracování pouze symbolického managementu a dokonce i k potlačení „nepříjemných“ stránek managementu vedením. Nejčastější chyby při managementu rizik jsou:

- Vedení podniku nepřijme bezpečnost jako skutečnou prioritu, ale uspokojí se pouze s dokumentací o bezpečnosti, která nemá oporu v realitě.

- Podvědomě se vytlačí události s velkým dopadem, ale s malou pravděpodobností s tím, že „to se nám nemůže stát“ nebo „to se stane až někomu po nás“.
- Opomenou se významné zdroje rizik.
- Opomenou se významné scénáře.
- „Upraví“ se výsledky analýzy rizik, aby nepůsobily negativně.
- Management skončí u konstatování rizik a nenásleduje rozhodnutí o změnách a alokace prostředků.
- Není kontrolováno, zda bezpečnostní opatření a havarijní plány opravdu fungují.
- Management bezpečnosti se provede jako jednorázová akce (a je rychle zapomenut) a není následován cyklickým opakováním a neustálým zlepšováním.



Obrázek 13: Obecné schéma managementu rizik

Jak je z obrázku 13 patrné, celý proces řízení rizik dle ISO 31 000 se sestává ze dvou velkých částí, z analýzy rizik a z jejich ošetření (v anglickém originále „risk control“). Významné jsou kompetence nezbytné pro jednotlivé části – analýzu rizik vypracovávají analytici, ošetření rizik je v rukou managementu, přičemž obě skupiny musí spolupracovat s technikou.

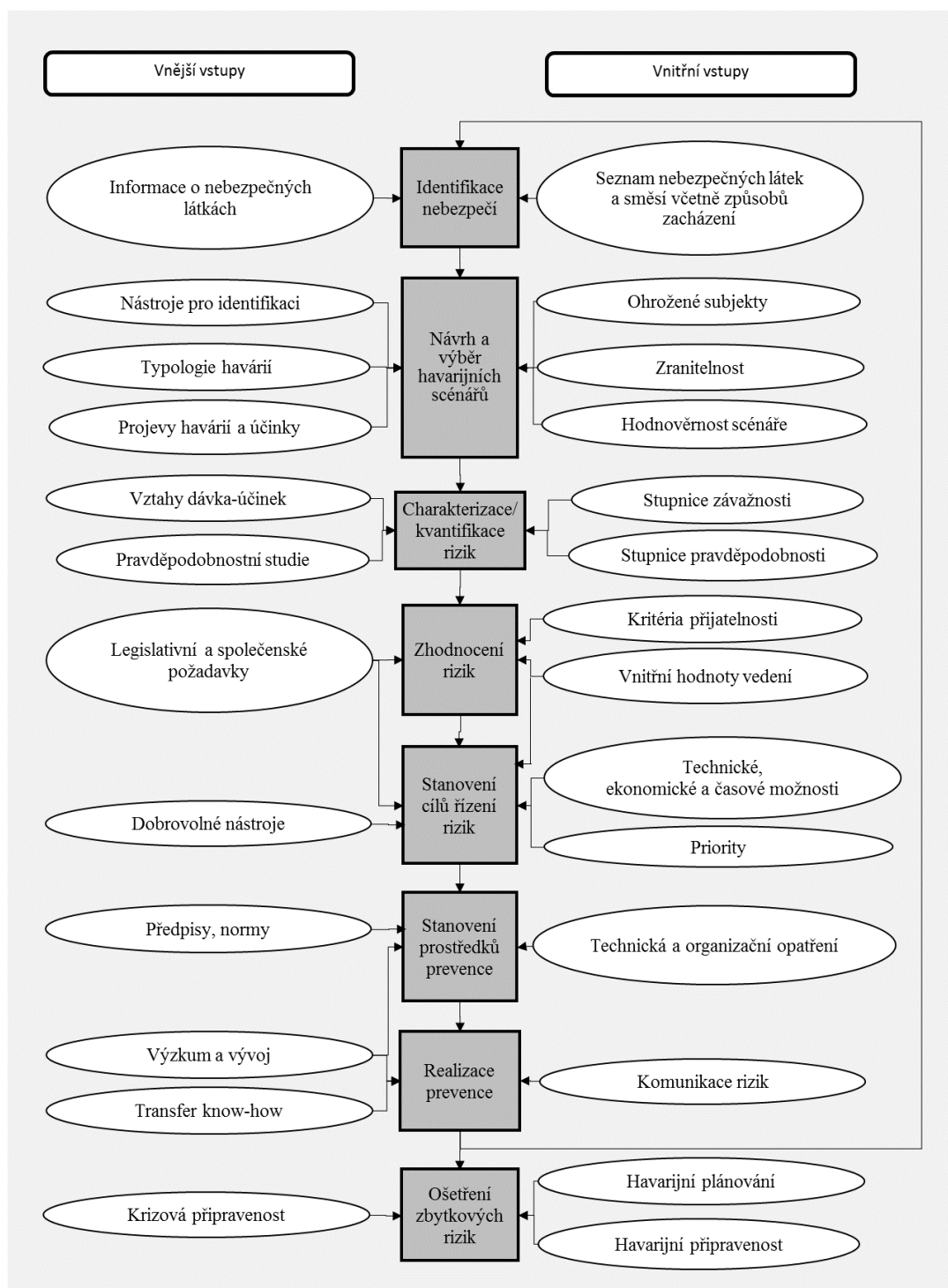
Jednotlivým krokům managementu rizik se věnují další kapitoly. Určitá úroveň snahy o řízení rizik existuje v každém energetickém provozu, avšak systematický

management bezpečnosti je mnohem efektivní. To vede například k tomu, že legislativa EU i ČR vyžaduje po provozovatelích, v jejichž zařízeních je přítomno významné množství nebezpečných látek, vypracovat systém řízení prevence závažných havárií. To se týká i velkého počtu provozů v energetice, počínaje sklady surovin, přes zpracování paliv a jejich skladování až po výrobu energie. Skutečnost, že podnik tuto zákonnou povinnost nesplní, může být důvodem k citelným sankcím, včetně zastavení jeho provozu.

Před tím, než je proces managementu rizik spuštěn, musí si vedení podniku ujasnit svoje strategické cíle v oblasti řízení rizik a deklarovat jasně svoji politiku.

Samozřejmě, tyto stanovené cíle určují rozsah a hloubku jak analytické části, tak ošetření identifikovaných rizik.

Proces managementu rizik na příkladu prevence závažných havárií se zahrnutím nebezpečných látek a jeho jednotlivé kroky jsou znázorněny na obrázku 14. Vstupy zprava reprezentují to, co musí zajistit podnik a vstupy zleva to, co podnik potřebuje k tomu, aby byl schopen požadované kroky provést, a co mu může dodat společnost nebo věda a výzkum. Každý krok je důležitý, žádný nelze obejít či vynechat.



Obrázek 14: Vstupy do procesu managementu rizik. Zleva vstupují údaje a metody zvenku, zprava pak to, co musí vyřešit sám provozovatel nebo jeho expertní tým

V následujícím textu jsou popsány jednotlivé kroky obecného schématu managementu rizik, specifikace pro energetiku pak v další kapitole.

Identifikace nebezpečí

Identifikace nebezpečí je prvním základním krokem managementu rizik a je zároveň jednou z jeho kritických částí. Cílem tohoto kroku je zjistit, jaká nebezpečí se mohou ve zkoumaném systému vyskytovat. K tomu je v první řadě nezbytné rozhodnout, co spadá do analyzovaného systému a co již nespadá; toto rozhodnutí nebývá lehké, protože:

- jestliže analytik začne usilovat o co nejúplnější analýzu, povede ho to k zahrnutí příliš širokého zkoumaného systému, analýza se stane příliš obsáhlou a nepřehlednou, ale i časově a finančně příliš náročnou.
- opačný trend, zúžení a zjednodušení analyzovaného systému, povede k tomu, že budou podceněny vnější vlivy a nehody, způsobené přenosem z jednoho malého systému (subsystému) do druhého. Může tak dojít k zásadnímu podcenění nebo dokonce úplnému ignorování některých jakoby z vnějšku přicházejících rizik. Typickou ukázkou jsou domino efekty nebo havárie iniciované přírodními vlivy, tzv. NATECH [58], a praktickou realizací takového podcenění byla havárie jaderné elektrárny ve Fukušimě.

Při vyhledávání zdrojů nebezpečí je vhodné postupně identifikovat zdroje různého původu, přinejmenším následující [28]:

- Zdroje nebezpečí mechanického původu (tlak, setrvačnost, hmotnost, možnost pádu a zhroucení, ostré předměty atd.)
- Zdroje nebezpečí chemického původu – viz další kapitoly
- Zdroje nebezpečí elektrického původu
- Zdroje nebezpečí požáru budov a zařízení
- Nebezpečí záření a tepelných zdrojů jiných než požár
- Zdroje biologických nebezpečí
- Lidský faktor jako zdroj nebezpečí
- Zdroje nebezpečí vyplývajícího z okolního prostředí
- Nebezpečí vyplývající z nesprávného přenosu informací
- Socio-ekonomické zdroje nebezpečí

Při identifikaci nebezpečí hrozí to, že analytik nebude pracovat systematicky a soustředí se pouze na nebezpečí, která jsou mu známá a se kterými obvykle pracuje. Typickou ukázkou v činnosti, která reprezentuje významnou kategorii managementu rizik, tedy ve vojenství, je situace známá jako „připravovat se na minulé války“. Neschopnost předvídat a neschopnost poučit se jsou proto Cohenem a Goochem [23] považovány za dvě ze tří hlavních příčin neúspěchu a není pochyb o tom, že neschopnost nalézt nebezpečí spadá to této kategorie.

Výstupem je seznam jednotlivých nebezpečí. Zásadním faktorem je, že pokud se nepodaří se identifikovat nebezpečí, bude ignorováno a bude se tak moci projevit naplno a vůči nepřipravenému podniku. Identifikace nebezpečí zahrnuje kromě nalezení zdrojů nebezpečí i ohodnocení jejich velikosti, např. hmotnosti nebezpečné látky, množství plynu pod tlakem, kinetické energie rotujících částí atd.) a přítomnosti zasažitelného cíle. Možnost realizace nebezpečí ve formě nehody už pak hodnotí další část – nalezení scénářů.

Návrh havarijních scénářů

Návrh a vyhodnocení potenciálních havarijních scénářů představuje druhý klíčový krok v managementu rizik. Jeden zdroj rizika může obecně vytvářet více než jeden havarijní scénář, například pro hořlavý zkapalněný plyn to může být požár, výbuch mraku plynu i výbuch zásobníku typu BLEVE.

V managementu rizik se ve skutečnosti zřídka řeší detailní individuální scénáře, protože by jich byl příliš velký počet, ale kombinují se všechny jednotlivé scénáře vedoucí ke stejnému typu nehody, např. k úniku plynu ze zásobníku a jeho explozi. Scénář je proto nutno vnímat jako časovou a prostorovou souslednost všech událostí, které vedou ve svém důsledku k určitému typu havárie. Jedná se tedy o variantní popis rozvoje havárie, zahrnující popis rozvoje příčinných a následných na sebe navazujících a vedle sebe i posloupně probíhajících událostí, a to jednak probíhajících spontánně, a jednak událostí probíhajících jako činnosti lidí, které mají za účel havárii předejít nebo omezit její průběh. Iniciační událost je rozvíjena dalšími mezilehlými událostmi až do koncového bodu scénáře. Zdroj rizika ve stavu odpovídajícímu koncovému bodu scénáře působí na své okolí specifickými fyzikálními účinky (projevy), kterým odpovídají určité následky (dopady). Rozvíjející události scénáře, které předcházejí vzniku nehody, jsou selháním nebo úspěchy preventivních ochranných bariér. Věrohodnost scénářů je založena na inženýrském úsudku opírajícím se o znalosti fyzikálních a chemických zákonů a na zkušenostech získaných vyhodnocením nehod proběhlých v minulosti [88].

Při návrhu havarijních scénářů platí totéž, jako u identifikace nebezpečí – nenalezený scénář jako by neexistoval pro vedení podniku, které mu tak nevěnuje pozornost ani v rámci prevence ani při havarijní připravenosti, avšak existuje v realitě a může zásadním způsobem překvapit nepřipravenou společnost. Typickými příklady jsou jak havárie s methyloxyanem v indickém Bhópálu v roce 1984, doposud nejhorší

chemická havárie v historii, tak havárie v Sevesu, která dala jméno evropské legislativě o prevenci závažných havárií [28].

Při návrhu scénářů je užitečné respektovat následující zdroje:

- Historii nehod a skoronehod v analyzovaném podniku, včetně názorů odborníků z konkrétních provozů
- Historii nehod a skoronehod v příslušném průmyslovém segmentu. Zde jde s výhodou využít databáze jako e-MARS, BARPI, ZEMA.
- Existující kontrolní seznamy – Check Listy.
- Sofistikované metody identifikace nebezpečných stavů jako je Dow Fire & Explosion index, HAZOP, FMEA, FMECA
- Intuitivní a na obecné zkušenosti založené metody jako What-If

Pro vytvoření kvalitních scénářů potenciálních havárií je nezbytná spolupráce mezi analytikem, bezpečnostním technikem v provozu a technologem nebo znalcem technologie; podcenění této součinnosti bylo příčinou mnoha nehod. Bezpečnost musí být vždy svázána s konkrétními podmínkami a neexistuje bezpečnost per se, ale vždy jen bezpečnost konkrétního zařízení. Statistiky a databáze jako e-MARS, BARPI, ZEMA ukazují, že soustředění se na nejdéle trvající část procesů, tedy na výrobu, nedostačuje. Velká část havárií jako nestandardních událostí se stává v nestandardních situacích, tedy při údržbě, opravách, v rámci změn a mnohdy má svůj původ už v koncepci technologie samé. Různé fáze životního cyklu zařízení navíc přináší různá rizika, a proto musí být analyzovány všechny životní fáze technologie, minimálně však tyto:

- Projektová fáze
- Konstrukce zařízení
- Spouštění zařízení a provozní testy
- Běžný provoz
- Údržba a opravy
- „Teplá“ odstávka a zastavení provozu včetně krizových stavů
- Demontáž zařízení a likvidace

Při tvorbě scénářů, ale i při jejich vyhodnocování v rámci analýzy rizik, je výhodné používat grafická znázornění, umožňující pochopení komplexních scénářů. Jedním z vhodných způsobů jsou tzv. stromy poruch (Fault Trees), kdy analýzy pomocí logických schémat poruch umožní nejen vizualizovat scénář havárie, ale také pomocí Booleovské algebry vypočítat pravděpodobnost či frekvenci události a racionálně

provádět preventivní opatření. Z tohoto důvodu je analýza stromem poruch (FTA, Fault Tree Analysis) široce využívána v letectví, jaderné, i chemickém procesním průmyslu při řízení rizik [21], [22], [105]. FTA je proto i předmětem normy ČSN EN 61025 (010676) „Analýza stromu poruchových stavů“.

Tak jako identifikace nebezpečí odpovídá na otázku „co může neštěstí způsobit“, scénáře nám ukazují, „jak se to může přihodit“. Zůstávají však na čistě kvalitativní úrovni a pro kvantifikaci možných problémů musíme přejít k charakterizaci rizik.

Charakterizace a kvantifikace rizik

Cílem tohoto kroku je charakterizovat riziko, tj. určit šanci, s jakou sledovaný cílový subjekt (typicky zaměstnanec, okolní obyvatelstvo, životní prostředí, majetek apod.) utrpí poškození a jaká bude závažnost tohoto poškození. Charakterizace rizika pak slouží jako podklad pro rozhodovací proces o přijatelnosti rizika a často nahrazuje termín „analýza rizik“, zvláště pak ve frekventovaných případech, kdy některé veličiny ve výpočtech nelze exaktně zjistit a analytik se uchyluje ke kvalifikovanému odhadu, nebo když je analýza prováděna semikvantitativně. Postupné kroky charakterizace rizik jsou tři:

1. Stanovení intenzity havarijního jevu, např. velikosti tlakové vlny nebo množství uniklé toxické látky a modelování šíření tohoto jevu po okolí.
2. Odhad účinků na základě znalostí vztahů mezi dávkou a účinkem. Vztah mezi dávkou a účinkem reprezentuje poškození cílového systému (lidský organismus, zařízení, životní prostředí,...) následkem havarijních projevů a je vyjádřením funkce zranitelnosti cílového systému. V odborné literatuře zabývající se prevencí závažných havárií je uvedeno několik modelů nebo spíše principů, jak stanovovat poškození lidského organismu. Například u průmyslových výbuchů se v praxi používají dva základní přístupy a to „Principy založené na prahových hodnotách přetlaku“ a „Probitové funkce“ [35]. Přístupem nebo také modelem se v tomto případě rozumí zjednodušený popis vztahu mezi přetlakem (příp. jiným parametrem tlakového projevu – obecně dávkou) a negativním účinkem výbuchu na lidský organismus, popřípadě jiný cílový systém.
3. Stanovení nejistoty vzniku havárie. V češtině často používaný termín „pravděpodobnost“ může být zavádějící, protože může zahrnovat jak skutečnou pravděpodobnost, tedy bezrozměrnou veličinu udávající poměr mezi počtem případů vedoucích k havárii ke všem případům (např. pravděpodobnost havárie raketoplánů Space Shuttle při jednom letu se ukázala být kolem 0,018), tak frekvenci, tedy reciprokou hodnotu očekávané průměrné doby mezi dvěma haváriemi (závisí na počtu letů; u stejného typu raketoplánu činila 0,092/rok). Záměna mezi frekvencí a pravděpodobností vede k mylným závěrům a je jednou z nejčastějších chyb při charakterizaci rizika. Bohužel, ani v bezpečnostních zprávách českých podniků v rámci prevence závažných havárií není tato záměna neobvyklá.

U analýzy rizik je velmi důležité uvést úroveň nejistoty, která je vlastní konečnému odhadu. Je potřeba si uvědomit, že vzhledem k tomu, že charakterizace rizik vychází z integrace dat z předchozích kroků, je potřeba do finální nejistoty zahrnout všechny nejistoty, které s sebou přináší jednotlivé dílčí kroky.

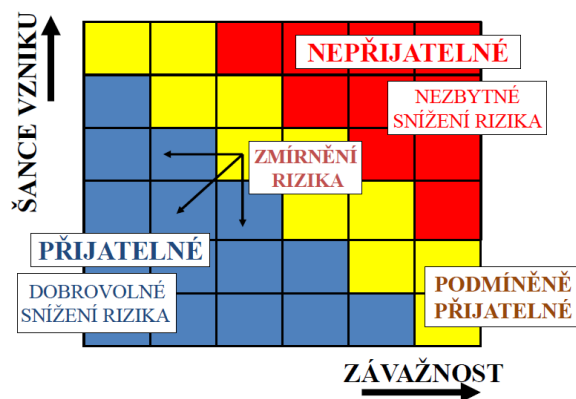
Riziko je chápáno jako komplexní funkce zahrnující dopad a jeho nejistotu (pravděpodobnost, frekvenci). To umožňuje nejen vizualizovat rizika v dvojrozměrném prostoru, ale také je srovnávat a prioritizovat, v konečném důsledku tedy i alokovat prostředky na jejich řešení. Prioritizace zahrnuje i vyřazení těch scénářů, které nebude analytik dále hodnotit. Jsou to především všechny scénáře vedoucí k marginálním dopadům, dále pak scénáře krajně nepravděpodobné, ale vedoucí jen ke středně závažným událostem. Není však správné takto vyřazovat i nepravděpodobné události s extrémně velkým dopadem, protože u tak závažných událostí je již často opouštěna probabilistická metoda hodnocení založená na kombinaci pravděpodobnosti a dopadu a je využíván deterministický princip [57], založený pouze na velikosti dopadu. Příkladem, kdy nesprávné vyhodnocení málo frekventované události vedlo ke katastrofě, je havárie raketoplánu Columbia, kde v rámci analýzy rizik byl vynechán scénář poškození velkého kusu ochranné tepelné izolace upadlou pěnou jako nerealistický, ve skutečnosti však nastal [6].

Zhodnocení rizik

Hodnocení rizik je proces, při němž je víceméně objektivně vyjádřeným rizikům ve formě závažnosti a pravděpodobnosti havárií přiřazována hodnota s ohledem na hodnotový systém organizace, která rozhoduje o řízení rizik. Je to tedy přechod mezi čistě technickou a organizační částí řízení rizik. Hodnocení rizik nemůže provést analytik ani technik, ale finální rozhodnutí je vždy v rukou manažerů nebo politiků, bez ohledu na jejich častý odpor. Přechod mezi analýzou (charakterizací) a hodnocením rizika je založen na vnímání a akceptovatelnosti rizik.

Proces analýzy rizik je zakončen odhadem a vyjádřením rizika. Obecně existuje více způsobů jak riziko pro účely dalšího hodnocení vyjadřovat [55]. K následnému hodnocení je třeba rizika vzájemně porovnat. K tomu slouží primárně vyjádření pomocí takzvané matice rizik, ve které jsou jednotlivá rizika umístěna podle předpokládané úrovně závažnosti a podle pravděpodobnosti. Příklad matice [28] je na obrázku 8 V rámci matice jsou rizika rozdělena do tří kategorií – rizika přijatelná, rizika podmíněně přijatelná a rizika nepřijatelná; v některých zjednodušených

případech pouze na dvě. Do matice se na základě analýzy rizik umístí všechny hodnocené scénáře formou bodů.



Obrázek 15 Matice rizik a jejich akceptovatelnosti

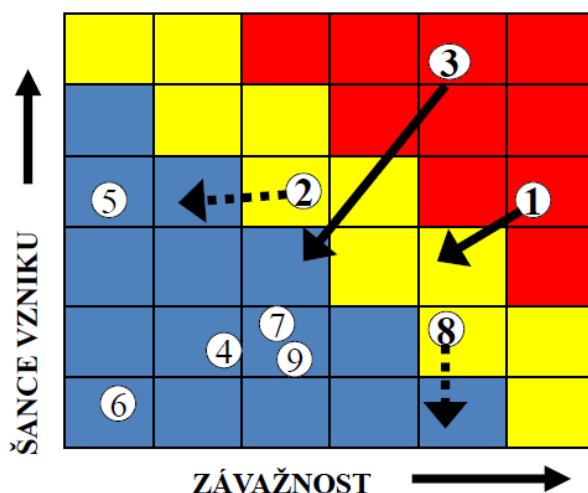
Právě zařazení do kategorií přijatelnosti vytváří rozdíl mezi analýzou (charakterizací) a hodnocením rizik. Umístění jednotlivých scénářů formou bodů do matice bez vymezení přijatelnosti reprezentuje analýzu rizik, s vymezením přijatelnosti pak jejich hodnocení; vzdálenost od hranice s další kategorií přijatelnosti pak lze chápat jako další míru přijatelnosti či nepřijatelnosti a tudíž využít k přiřazení priorit jednotlivým scénářům.

Přijatelná rizika není nezbytné dále řešit, přestože je vždy vhodné snižovat jakákoli rizika. Tolerovatelné riziko je riziko, se kterým je společnost ochotná žít pro zabezpečení blahobytu a v důvěře, že toto riziko je správně řízeno, kontrolováno a dále redukováno, když je to možné. Rizika zhodnocená jako nepřijatelná je nutné co nejdříve eliminovat, jelikož společnost není ochotna nést jejich následky s očekávanou frekvencí.

Stanovení cílů ošetření rizik

Stanovení cílů je klíčovou fází samotného managementu rizik a vychází z manažerské praxe. Cíle je možné stanovovat na základě provedeného vyhodnocení rizik, ale také s ohledem na možnosti realizace těchto cílů, a to jak možnosti finanční, tak i technické, personální a časové. Dostatečné, realistické a proveditelné stanovení cílů je základním předpokladem pro zvládnutí řízení rizik. Základním nástrojem je opět matice rizik, v níž je přiřazena priorita velkým rizikům a cíle jsou obecně stanoveny jako celková úroveň všech rizik. Příkladem může být cíl

„všechna rizika v přijatelné úrovni“, „okamžité snížení nejhorších dvou rizik a následně postupné všech ostatních o jednu úroveň přijatelnosti“ nebo i jinak formulované cíle, tato formulace však musí být jasná a být součástí politiky bezpečnosti. Příklad stanovení cílů s využitím matice rizik je na obrázku 16.



Obrázek 16 Stanovení cílů ošetření rizik. Čísla representují pořadí rizik při analýze (identifikaci scénáře) a jejich velikost nemá vztah k velikosti rizika.

Snižování rizik spočívá ve snižování dopadu (riziko 2, pravděpodobnosti či frekvence scénáře (riziko 8) nebo v kombinaci obojího (rizika 1 a 3). Možnost aplikace opatření na snížení rizika se hodnotí i po stránce jejich efektivnosti, a proto se obvykle aplikuje analýza poměru vynaložených nákladů k výslednému přínosu (Cost-Benefit Analysis). Zvláštní případ jsou scénáře s velkou neurčitostí výsledků nebo s obtížně stanovitelným přínosem, kdy ke snižování rizika lze přistoupit z hlediska principu ALARA (As Low As Reasonably Achievable), tj. snižování rizika na tak nízké, jak je to racionálně dosažitelné, resp. principu ALARP (As Low As Reasonable Practicable), tj. snižování rizika na tak nízkou úroveň, jak je to racionálně proveditelné, tedy kdy by už byly náklady na další snížení rizika neúměrné k přínosu získaném realizací těchto opatření. Obě tyto metody mají původ v jaderné energetice [104].

Stanovení prostředků prevence

Stanovení prostředků prevence vychází buď z obrázku 4 (MADS-MOSAR [73]) nebo z detailního rozboru scénářů. První formu řešení lze chápat jako makroskopický přístup, druhý pak jako zaměřený na detailní řešení.

Makroskopický pohled obsahuje jeden z následujících přístupů:

- a) snížení velikosti zdroje rizik, například snížením množství skladovaného množství nebezpečné látky nebo v případě, že nelze zásoby snížit, jejím rozdělením do většího počtu menších, vzájemně trvale nepropojených zásobníků; tato filosofie byla po havárii zásobníků zkapalněného plynu v PEMEX LPG terminálu v San Juan Ixhuatepec v Mexico City v roce 1984 (detaily v kapitole 3.2.5) kodifikována i do světově uznávaného pravidla, že nebudou nově konstruovány LPG zásobníky o tak velkém objemu jako v Mexico City – 500 tun
- b) změna zdroje rizik za menší výměnou nebezpečné látky za méně nebezpečnou, například nahrazení LPG kapalnými palivy
- c) lokalizace zdroje rizik dostatečně daleko od zasažitelných cílů; tento přístup je velmi vhodný i při řešení tzv. domino efektu
- d) zvýšení odolnosti (snížení zranitelnosti) cíle; tato technika je zvláště vhodná pro konstrukce, budovy a technologie a spadají do ní například požární stěny před citlivými objekty

Přístup zaměřený na detailní řešení („mikroskopický“ podle metodiky MADS-MOSAR [73]) vychází z detailního popisu scénáře havárie a je založený na přerušení tohoto scénáře, ať už ve fázi iniciace havárie nebo při jejím šíření. Ve schématu MADS-MOSAR odpovídá přerušení iniciace havárie nebo přerušení přenosu nebezpečí mezi zdrojem nebezpečí a cílem. S výhodou lze využít výsledky analýzy HAZOP nebo FMEA a zvláště pak FTA, kdy je možné zároveň i odhadnout efekt preventivního opatření se zřetelem na pravděpodobnost či frekvenci havárie. Přerušení scénáře spočívá ve vytvoření bariér, které rozvoj havárie zastaví nebo alespoň omezí. Existují různé typy bariér rozvoje havárie, které je vhodné kombinovat, a které byly detailně analyzovány v rámci evropského projektu EVG1–CT–2006–00036 ARAMIS – Accidental Risk Assessment Methodology for Industries in the Context of Seveso II Directive [84].

Pasivní bariéry jsou definovány jako fungující nepřetržitě, přičemž k dosažení jejich funkce nevyžadující žádnou lidskou činnost, zdroje energie a informační zdroje. Příkladem jsou ochranné valy, zachytňné jímky, rozdělení objektů na požární úseky.

Aktivní technické bariéry jsou tvořeny třemi subsystemy vzájemně propojeny v řetězci:

- systém detekce
- systém vyhodnocení a reakce na podnět z detekce (logický obvod, převod, mechanické zařízení, člověk, ...)
- systém nápravné činnosti (mechanická, nástrojová, lidská, ...)

Na rozdíl od pasivních bariér, které mají jen malou šanci selhat, aktivní tuto slabost mají, a proto se musí hodnotit i možnost jejich selhání.

Organizační opatření využívají činnosti člověka včetně jeho tvořivosti a fantazie. Paradoxně, člověk a jeho organizační opatření patří mezi nejméně spolehlivé systémy, avšak právě tvořivost a fantazie umožňují vyřešit i situace, na které pasivní ani aktivní bariéry nejsou konstruovány.

Stanovení prostředků prevence úzce souvisí s prostředky, které je možné v daném podniku a kontextu použít. Existují obecné postupy, především organizačního charakteru, jako zavádění bezpečnostní politiky a integrovaných postupů řízení za účelem zajištění větší bezpečnosti. Dalšími možnými prostředky jsou opatření na technologické úrovni. Pro snižování rizika se mohou použít opatření snižující následky událostí (např. nižší zádrže nebezpečných látek, používání méně nebezpečných látek) nebo snížení pravděpodobnosti událostí (např. záložní zařízení, obchvaty, instrumentace, alarmy).

Realizace prevence

Stanovené prostředky prevence je v další části nutné aplikovat do praxe. To většinou vyžaduje nejen jejich zavedení, ale i další kontrolu a neustálé zlepšování. Jde zde o přijetí předpisů týkající se organizace bezpečnosti, integrace přímých technologických a systematických opatření a podobně.

Aplikace prostředků prevence vede, nebo by alespoň měla vést, k zásadním změnám v rizicích příslušného zařízení, což znamená, že původně provedená analýza a hodnocení rizik přestávají platit. Po implementaci preventivních opatření je proto nezbytné analýzu rizik zopakovat, modifikovat scénáře o bezpečnostní bariéry a jiné změny a znovu provést analýzu a hodnocení rizik včetně kontroly, zda vytýčených cílů prevence bylo dosaženo. Také je nutné zhodnotit, zda bezpečnostní opatření sama o sobě nepřinášejí nová rizika, k čemuž obvykle dochází. Jedná se o princip dobře známý ze všech oblastí řízení rizik, jehož typickou ukázkou jsou bezpečnostní pásy nebo airbagy. Obě tyto zařízení významně snižují riziko smrti i zranění při havárii, bezpečnostní pás však může být příčinou nemožnosti úniku z hořícího auta po havárii a airbag aktivovaný bez připoutání bezpečnostním pásem může způsobit i smrtelná zranění.

Cyklus identifikace nebezpečí až realizace preventivních opatření je třeba opakovat do té doby, dokud nebude dosaženo požadované hodnoty bezpečnosti, tedy vytýčených cílů prevence.

Zbytková rizika

I přes přijetí preventivních opatření není nikdy možné eliminovat všechna rizika, nebo i snížit jednotlivá rizika na nulovou úroveň. Jedním z důvodů je i platnost ekonomického zákona růstu marginálních nákladů při dosahování stále vyšších úrovní bezpečnosti. Je tedy třeba se vyrovnat i s riziky, která se nedaří snížit nebo odstranit preventivními opatřeními. Takováto rizika, která zůstávají i po zavedení prevence, se nazývají zbytková rizika („residual risks“). Na rozdíl od prevence, kde je hlavním cílem, aby k havárii vůbec nedošlo, je cílem ošetření zbytkových rizik dosáhnout toho, aby i v případě vzniku havárie tato měla co nejmenší následky, tedy jedná se o uchránění hodnot. Základním opatřením je zavedení havarijní připravenosti – systematické přípravy na havárii, a to v případě prevence závažných havárií jak uvnitř podniku, tak vně podniku. Tento krok již vyžaduje vysoce organizovanou spolupráci nejen uvnitř zařízení, ale i vně v jeho okolí, jelikož připravovat by se měli všichni, kteří mohou být potenciální závažnou havárií zasaženi. Vnitřní havarijní plánování a připravenost jsou jednoznačně v kompetenci podniku samotného, vnější havarijní plánování mimo areál podniku je potom záležitostí veřejné správy a integrovaného záchranného systému.

Hodnocení rizik

Hodnocení rizik umožňuje přiřazení priorit, tedy rozhodnutí, zda budou rizika ošetřována, která to budou a do jaké míry je provozovatel či společnost chce zmírnit. Aby to bylo možné, musíme mít jednotná měřítko pro porovnávání jak dopadů, tak nejistoty vzniku havárie. Poměrně jednoduchá je situace u nejistoty, kde stačí zajistit, aby ve všech hodnocených scénářích byl výstup stejného charakteru, tedy frekvence či pravděpodobnost. Paradoxně, ačkoliv se častěji používá termín „pravděpodobnost“, ve většině případů je výstupem frekvence, obvykle s jednotkou reciproky rok. Frekvence je také vhodnější pro porovnávání, protože je možné ji vztáhnout k celému provozu a nejen k jednotlivé operaci. O porozumění problematice hodnocení rizik často vypovídá už číselná forma vyjádření nejistoty a dopadu.

Uvádění výsledků na velký počet platných cifer ukazuje na formální přístup a nepochopení úrovně neurčitosti dat a o záměně reality za manipulaci s čísly. Na jednom z jednání Komise kompetentních autorit EU k direktivě SEVESO II bylo například konstatováno, že průměrná frekvence závažných havárií v EU je o nejméně dva řády vyšší, než by vyplývalo z bezpečnostních zpráv podniků.

Pokud se týče závažnosti dopadů, situace je obtížnější, protože je nutné porovnat zdánlivě neporovnatelné hodnoty, tedy lidské zdraví a kvalitu života, finanční ztráty, životní prostředí a funkčnost provozu. Provádět takovéto srovnání je však nezbytné, protože jinak není možné stanovit priority. Zásadním úkolem pro tým zabývající se managementem rizik je tedy stanovení vzájemně harmonizovaných stupnic pro dopady a samozřejmě i pro frekvence. Obvykle není možné toto stanovení provést najednou, ale je předmětem komunikace. Jako účelné se jeví pracovat semikvantitativně, tedy v úrovních, a stupnice stanovit v logaritmickém měřítku. To umožní zvládnout hodnocení několika řádů událostí. Počet úrovní by neměl být menší než tři a větší než šest, protože při příliš velkém počtu již není prakticky možné provést srovnání. V praxi se občas vyskytují metody analýzy rizik, z nichž jako výstup jsou hodnoty dělené až na tisíc stupňů, v realitě však se jedná spíše o marketingový tah se symbolickými operátory než o skutečné hodnocení. Běžnému lidskému hodnocení se totiž vymyká možnost porovnat riziko na úrovni 754 a 753, a jak bylo ukázáno výše, od analýzy rizik lze jen těžko očekávat přesnost větší než jeden řád.

Při stanovování systému hodnocení tedy hodnotitelé připraví několik stupnic pro různé typy dopadů (minimálně: zdraví, peníze, životní prostředí) v rozmezí několika řádů a postupně je harmonizují tak, aby došlo ke shodě v tom, že událostí různých typů, ale stejné úrovně jsou vnímány jako srovnatelné s ohledem na zájmy a preference podniku nebo jiného hodnotícího subjektu. To umožní, aby všechna rizika bylo možné vynést do jediné matice a tu pak použít ke stanovení priorit.

Druhým krokem, vyžadujícím rozhodnutí vrcholového managementu nebo dosažení konsenzu, je stanovení akceptovatelnosti. I zde je vidět rozdíl mezi analýzou a hodnocením rizik, protože analýza je v podstatě symetrická, ale hodnocení (přijatelnost) nemusí být. Může se vyskytovat buď fenomén nazývaný „averze k rizikům“, kdy rizika vedoucí k velmi velkým neštěstím jsou neakceptovatelná i při velmi nízkých pravděpodobnostech, nebo naopak fatalismus, kdy málo pravděpodobné události jsou zanedbávány s tím, že „nám se to snad nestane“.

Zajímavý je vztah české společnosti k akceptovatelnosti rizik závažných havárií. Nejprve, v rámci předchozího zákona č. 353/1999 Sb., bylo voláno po jednoznačném a obecném stanovení neakceptovatelné úrovně rizik. Ukázalo se však, že mechanická aplikace těchto kritérií by vedla k pro společnost drastickým konsekvencím, kdy odstranění formálně nepřijatelného rizika by vedlo ke ztrátě zaměstnanosti, poklesu životní úrovně a možná i k vysídlení komunity. Přijatelnost je dnes chápána v socioekonomickém kontextu a je zahrnut princip, že neposuzujeme pouze rizika, ale i benefity a pokud benefity jasně převažují a rizika nejsou příliš velká, lze je tolerovat. Nezbytná je však kvalitní, otevřená a čestná komunikace o nich.

Systém a metody řízení prevence závažných havárií v průmyslu

Z historických zkušeností a z vyšetřování v minulosti proběhlých havárií celkem jasně vyplývá, že základní příčiny většiny havárií nemají jako hlavní důvod tzv. primární příčinu, ale že se odvíjejí od tzv. kořenových příčin svázaných s řízením organizace. Ty tkví mimo jiné ve způsobu organizace a řízení příslušného zařízení. Úroveň bezpečnosti v provozu, energetiku nevyjímaje, do velké míry závisí na přístupu managementu k problematice organizace a řízení bezpečnosti. Pouze management je z pozice své funkce oprávněn nastavit pravidla organizace a řízení bezpečnosti v objektu a dbát na jejich důsledné dodržování. To také vedlo k tomu, že při přechodu od původní směrnice SEVESO I k SEVESO II a III byl opuštěn koncept čistě technické bezpečnosti a u podniků spadajících do gesce zákona o prevenci závažných havárií se striktně vyžaduje zavedení systému řízení bezpečnosti.

Organizace a řízení bezpečnosti v objektu by se dle směrnice SEVESO III nemělo omezit jen na existenci vágního prohlášení o vyhlášené politice bezpečnosti a proklamaci o vyhovující úrovni prevence vzniku závažné havárie. Provozovatel by měl být vždy schopen prokázat, že politika prevence havárií je věcně aktuální, dostatečně náročná, odpovídající riziku a že je trvale naplňována konkrétními opatřeními. Pokud se konkrétní opatření týkají organizace a řízení bezpečnosti, jedná se o preventivní opatření organizačního charakteru, tedy organizační opatření.

Management podniků, v nichž hrozí nebezpečí vzniku závažné havárie, by měl být schopen:

- formulovat politiku bezpečnosti zabezpečující vysokou úroveň ochrany před riziky

- konkrétními opatřeními realizovat a trvale naplňovat stanovenou politiku prevence, tj. zajistit zavedení všech vhodných opatření, systémů, postupů, které jsou nezbytné k efektivnímu provádění politiky prevence.

Management bezpečnosti v podniku

Při managementu a zacházení s riziky závažných havárií identifikovaných v rámci analýzy je třeba hledat odpovědi na následující otázky:

- Co lze udělat a jaké možnosti jsou k dispozici?
- Jaké jsou s tím spojené kompromisy ve smyslu celkových nákladů, přínosů a rizik?
- Jaké jsou dopady současných rozhodnutí na budoucí možnosti?

V jednotlivých podnicích v rámci energetiky nelze odpovídat na tyto otázky jednotlivě pro všechny identifikované hrozby, rizika je třeba řídit globálně, na úrovni celého podniku. K tomu slouží zavádění bezpečnostní politiky, a zachovávání bezpečnostní kultury v podniku. Této oblasti se věnuje velké množství manažersky orientované literatury. Specificky pro oblast prevence závažných havárií může být management bezpečnosti určen například podle [42], [43] šesti základními oblastmi:

- a) Bezpečnostní politika
Bezpečnostní politika formálně vyjadřuje cíle, principy, strategie a návody, které je třeba následovat pro zdraví a bezpečnost při práci. Bezpečnostní politika zároveň specifikuje funkce a zodpovědnosti každého člena organizace v této oblasti. Jejím zaměřením je vytvořit příznivé klima, které zajistí, že jednotlivci ze všech úrovní podniku se zapojují a přispívají. Navíc, takové politiky je nutné založit na neustálém zlepšování a na učení se ze zkušeností. [42], [43]
- b) Motivace zaměstnanců
Podněty pro zapojení zaměstnanců v oblasti aktivit týkajících se zdraví a bezpečnosti, by měli podporovat bezpečné chování a zahrnovat osoby do rozhodovacích procesů. Toho lze docílit například systémem odměn a trestů, nebo konzultací s jednotlivci o jejich pohodě na pracovišti. Jeho cílem je předat zaměstnancům, že jejich přínos pro bezpečné prostředí v

rámci podniku je organizací oceňován, a tím i upravovat názory, hodnoty a praxe pracovníků s cílem dosáhnout bezpečného chování. [42], [43]

c) Cvičení

Jde o trénink a rozvoj kompetencí zaměstnanců. Bezpečnostní trénink se zaměřuje na vybavení zaměstnanců kapacitou a schopnostmi potřebnými k tomu aby prováděli své úkoly správně. Informuje je o rizicích na pracovišti, a o postupech, které jsou schopné jim předcházet, napravovat je nebo minimalizovat. Zároveň cílí na změnu postojů, takže manažeři i zaměstnanci jsou zapojováni a akceptují, že bezpečnost je základním prvkem toho dělat práci správně. Zároveň by měli podniky zavést systém kontinuální re-edukace a opakovaného tréninku, který umožní stávajícím zaměstnancům uchovávat znalosti o bezpečnosti aktuální. [42], [43]

d) Komunikace

Jedná se o komunikaci a přenos informací o možných rizicích na pracovišti, a jak s nimi nejlépe bojovat. Dobrý komunikační systém v podniku by měl obsahovat sérii prvků, jak formálních tak neformálních, které zajišťují adekvátní proudění informací, jak z hora dolů, tak z dola nahoru, a stejně tak i do stran. To by mělo podpořit motivaci a stimulovat zapojení všech členů organizace. [42], [43]

e) Plánování

Principem je plánování a rozlišování mezi preventivním plánováním a havarijním plánováním. Preventivní plánování identifikuje možná nebezpečí v procesu, analyzuje riziko toho, že dojde k havárii a navrhuje předběžná opatření k zabránění havárie a ztrátám. Může být použita široká škála metod pro analýzu rizika k ověření bezpečnosti procesů - kvantitativní analýza rizika, HAZOP, analýza What-if, Analýza stromem poruch atd. Podle prioritního listu, který je vytvořen na základě použití těchto technik by měli být přijata preventivní a ochranná opatření. Havarijní plán potom zahrnuje organizování lidských a materiálních zdrojů potřebných pro okamžitou a efektivní odezvu v případě jakékoli havárie, tak aby byli její potenciální následky redukovány na co nejmenší možnou

míru. To vyžaduje osvojení opatření týkající se první pomoci, hašení a evakuace pracovníků i dalších. [42], [43]

f) Kontrola

Kontrola a přehled aktivit prováděných v organizaci by měli umožnit neustálé zlepšování. Měly by být rozlišovány dva typy kontrol: vnitřní kontrola a techniky benchmarkingu. Vnitřní kontrola je prováděna ve smyslu analýzy operací a pracovních podmínek (bezpečnostní inspekce a audity) a prostřednictvím identifikace, vyšetřování a zaznamenávání událostí - havárií, incidentů a skoronehod - ke kterým dochází v rámci podniku. Benchmarking je proces učení založený na hledání nejlepšího manažerského systému na trhu, který by měl firmě sloužit jako referenční a pomoci jí lépe pracovat. Benchmarking umožňuje společně srovnávat svoji četnost havárií s jinými organizacemi v rámci stejného odvětví, které používají podobný výrobní proces, stejně tak jako srovnává jejich manažerské techniky a praxe (například kontrolní procedury, techniky pro vyšetřování havárií, ergonomický design prací nebo tréninkové programy) s dalšími organizacemi z jakéhokoli sektoru, s tím že identifikuje silné i slabé stránky. [42], [43]

Literatura I

- [1] ABBASI, T., a ABBASI, S. A. The boiling liquid expanding vapour explosion (BLEVE): Mechanism, consequence assessment, management. *Journal of Hazardous Materials* [online]. 2007, roč. 141, č. 3, s. 489–519 [cit. 3. 3. 2014]. ISSN 03043894. Dostupné z: doi:10.1016/j.jhazmat.2006.09.056
- [2] ABBASI, T. a ABBASI, S.A. Dust explosions—Cases, causes, consequences, and control. *Journal of Hazardous Materials* [online]. 2007, roč. 140, č. 1-2, s. 7–44 [cit. 3. 3. 2014]. ISSN 03043894. Dostupné z: doi:10.1016/j.jhazmat.2006.11.007
- [3] BABRAUSKAS, V. Estimating large pool fire burning rates. *Fire Technology*. 1983, roč. 19, č. 4, s. 251–261.
- [4] BAGSTER, D. F. a SCHUBACH, S. A. The prediction of jet-fire dimensions. *Journal of Loss Prevention in the Process Industries*. 1996, roč. 9, č. 3, s. 241–245.
- [5] BAKER, Q. et al. Vapor cloud explosion analysis. *Process Safety Progress*. 1996, roč. 15, č. 2, s. 106–109.
- [6] BANKE, J. Top 10 Questions About NASA's Columbia Shuttle Tragedy. *Space.com* [online]. 2003 [cit. 3. 3. 2014]. Dostupné z: <http://www.space.com/19403-nasa-space-shuttle-columbia-disaster-questions.html>
- [7] BAUDIŠOVÁ, B. et al. *Vybrané přístupy k definování smyslu zóny havarijního plánování*. In Aktuálně otázky bezpečnosti práce : New Trends In Safety and Health. Štrbské pleso : Technická univerzita v Košiciach, 2011. ISBN 978-80-553-076-0. 2011.
- [8] BEŇOVÁ, E. *Hodnocení bezpečnostních rizik souvisejících s únikem metanu z podzemních prostor*. Ostrava, 2012. Disertační práce. Vysoká škola báňská - Technická univerzita Ostrava.
- [9] BJERKETVEDT, D., BAKKE, J. R., a VAN WINGERDEN, K. Gas explosion handbook. *Journal of hazardous materials*. 1997, roč. 52, č. 1, s. 1–150.
- [10] BLÁŽKOVÁ, K., a KOŤÁTKO, A. *Hodnocení úniků nebezpečných látek do životního prostředí pro účely stanovování zóny havarijního plánování*. In Hodnocení a zvládání: Mezinárodní konference mladých

- vědeckých pracovníků. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2011. ISBN 978-80-248-2486-4. In: . 2011.
- [11] BULL, D. C., a RENWICK, P. A critical review of post Piper-Alpha developments in explosion science for the offshore industry. In: *Major hazards offshore. Conference*. 2000, s. 3–1.
- [12] BURGHERR, P., a HIRSCHBERG, S. Severe accident risks in fossil energy chains: A comparative analysis. *Energy* [online]. 2008, roč. 33, č. 4, s. 538–553 [cit. 3. 3. 2014]. ISSN 03605442. Dostupné z: doi:10.1016/j.energy.2007.10.015
- [13] BURGHERR, P., ECKLE, P., a HIRSCHBERG, S. Comparative assessment of severe accident risks in the coal, oil and natural gas chains. *Reliability Engineering & System Safety* [online]. 2012, roč. 105, s. 97–103 [cit. 3. 3. 2014]. ISSN 09518320. Dostupné z: doi:10.1016/j.ress.2012.03.020
- [14] CÁB, S. Nebezpečí výbuchu hořlavých prachů v průmyslu. *BOZP info* [online]. 2013. Dostupné z: http://www.bozpinfo.cz/win/knihovna-bozp/citarna/tema-bozpinfo/vybuch_prach130207.html
- [15] CAMERON, I. T., a RAMAN, R. *Process systems risk management*. B.m.: Academic Press, 2005.
- [16] CASAL, J. Fire accidents. In: *Evaluation of the effects and consequences of major accidents in industrial plants*. Elsevier, 2007.
- [17] CASAL, J. Vapour cloud explosions. In: *Evaluation of the effects and consequences of major accidents in industrial plants*. Elsevier, 2007.
- [18] CASAL, J. BLEVEs and vessel explosions. In: *Evaluation of the effects and consequences of major accidents in industrial plants*. Elsevier, 2007.
- [19] CASAL, J. Source term. In: *Evaluation of the effects and consequences of major accidents in industrial plants*. Elsevier, 2007.
- [20] CASAL, J. Atmospheric dispersion of toxic or flammable clouds. In: *Evaluation of the effects and consequences of major accidents in industrial plants*. B.m.: Elsevier. 2007
- [21] CENTER FOR CHEMICAL PROCESS SAFETY. *Guidelines for Chemical Process Quantitative Risk Analysis*. B.m.: American Institute of Chemical Engineers, 1999. ISBN 978-0-8169-0720-5.
- [22] CENTER FOR CHEMICAL PROCESS SAFETY. *Guidelines for Hazard Evaluation Procedures*. 3. vyd. B.m.: Wiley, 2008. ISBN 978-0-471-97815-2.
- [23] COHEN, E. A., a GOOCH, J. *Vojenské neúspěchy*. Praha: Naše vojsko, 2010. ISBN 978-80-206-1126-0.
- [24] CROWL, D. A. *Understanding explosions*. B.m.: John Wiley & Sons, 2010.
- [25] CUMBER, P. S. a SPEARPOINT, M. A computational flame length methodology for propane jet fires. *Fire Safety Journal* [online]. 2006, roč. 41, č. 3, s. 215–228 [cit. 3. 3. 2014]. ISSN 03797112. Dostupné z: doi:10.1016/j.firesaf.2006.01.003
- [26] ČT24: Výbuch na Transsibiřské magistrále odpovídal atomové bombě svržené na Hirošimu. 3. 6. 2009 03:25, autor:. [online]. [cit. 3. 3. 2014]. Dostupný z WWW: <
<http://www.ceskatelevize.cz/ct24/kalendarium/56731-vybuch-na-transsibirske-magistrale-odpovidal-atomove-bombe-svrzene-na-hirosimu/>>
- [27] DAMEC, J. *Protivýbuchová prevence*. Ostrava: Sdružení požárního a bezpečnostního inženýrství v Ostravě, 1998. ISBN 80-86111-21-0.
- [28] DANIHELKA, P. *Analysis and Management of Risks of Dangerous Chemicals in Industry*. Ostrava: VŠB - TU Ostrava, 2002. ISBN 80-248-0084-5.
- [29] DANIHELKA, P. Risk mitigation approaches to preventing and responding to tailings storage facility failure. In: *Proceedings of the Conference „Tailings“*. 2011. Operational Excellence Series.
- [30] DANIHELKA, P., a ČERVENÁKOVÁ, E. Tailing dams risk analysis and management. In: *UNECE Workshop on the Safety of Tailing Facility Management*. 2007.
- [31] DANIHELKA, P., NEVRLÝ, V., DOBEŠ, P., a BITALA, P. Požáry a znečištění ovzduší. *Ochrana ovzduší*. 2010, č. 3, s. 23 – 27.
- [32] DANIHELKA, P., a SOLDÁN, P. Jsou hasební vody potenciálním ohrožením vodního prostředí? *Vodní hospodářství*. 2012, roč. 62, č. 12.
- [33] DAYCOCK, J. H., REW, P. J. Thermal radiation criteria for vulnerable populations. HSE Books, 2000.
- [34] DLABKA, J. Basics of Evaluation of Thermal Radiation Effects on Humans in Industrial Fires. Sborník vědeckých prací Vysoké školy báňské - TU Ostrava. 2012, roč. 6, č. 2, bezpečnostní inženýrství, s. 44–51. ISSN 1801-1764.
- [35] DLABKA, J., BAUDIŠOVÁ, B., a BEŇOVÁ, E. Hodnocení následků výbuchu na člověka v rámci problematiky prevence závažných havárií. *Spektrum*. 2013, roč. 13, č. 1. ISSN 1211-6920.
- [36] DLABKA, J. et al. Základní deskripce fyzikálně-chemických parametrů tryskových požárů. *Spektrum*. 2012, roč. 12, č. 1, s. 70–73. ISSN 1211-6920.
- [37] DOBEŠ, P. et al. Ecotoxicity of waste water from industrial fires fighting. *Geophysical Research Abstracts*. Volume 14, 2012,
- [38] EISENBERG, N., LYNCH, A., CORNELIUS J., a BREEDING, R. J. Vulnerability model. A simulation system for assessing damage resulting from marine spills. *Enviro control inc rockville md*, 1975.
- [39] ELSAYED, N. M., a ATKINS, J. L. Explosion and blast-related injuries: effects of explosion and blast from military operations and acts of terrorism. Academic Press, 2010.
- [40] ERMAK, D. L. User's manual for SLAB: An atmospheric dispersion model for denser-than-air releases. B.m.: Lawrence Livermore Laboratory, 1990.

- [41] FAY, J. Model of large pool fires. *Journal of Hazardous Materials* [online]. 2006, roč. 136, č. 2, s. 219–232 [cit. 3. 3. 2014]. ISSN 03043894. Dostupné z: doi:10.1016/j.jhazmat.2005.11.095
- [42] FERNÁNDEZ-MUÑOZ, B., MONTES-PEÓN, J. M., a VÁZQUEZ-ORDÁS, C. J. Safety culture: Analysis of the causal relationships between its key dimensions. *Journal of Safety Research* [online]. 2007, roč. 38, č. 6, s. 627–641 [cit. 3. 3. 2014]. ISSN 00224375. Dostupné z: doi:10.1016/j.jsr.2007.09.001
- [43] FERNÁNDEZ-MUÑOZ, B., MONTES-PEÓN, J. M., a VÁZQUEZ-ORDÁS, C. J. Safety management system: Development and validation of a multidimensional scale. *Journal of Loss Prevention in the Process Industries* [online]. 2007, roč. 20, č. 1, s. 52–68 [cit. 3. 3. 2014]. ISSN 09504230. Dostupné z: doi:10.1016/j.jlp.2006.10.002
- [44] FREEMAN, M. W. *Tank Farms in Kuwait following Hostilities and their Implications*. Lodon: Department for Communities and Local Government, 2006.
- [45] FRIEDMAN, R. *Principles of fire protection chemistry and physics*. Sudbury: Jones & Bartlett, 2009. ISBN 978-0-7637-6070.
- [46] FRITZSCHE, A. F. The health risks of energy production. *Risk Analysis*. 1989, roč. 9, č. 4, s. 565–577.
- [47] GEXCON AS, *FLACS v9. 1 User's Manual*. [online] Bergen, Norway: Gexcon AS, March 2009 [cit. 3. 3. 2014]. Dostupné z: <http://www2.gexcon.com/download/flacs-v9-manual.pdf>
- [48] GÓMEZ-MARES, M., MUÑOZ, M., a CASAL, J. Radiant heat from propane jet fires. *Experimental Thermal and Fluid Science* [online]. 2010, roč. 34, č. 3, s. 323–329 [cit. 3. 3. 2014]. ISSN 08941777. Dostupné z: doi:10.1016/j.expthermflsci.2009.10.024
- [49] GUGAN, K. *Unconfined vapour cloud explosions*. B.m.: Institution of Chemical Engineers, 1979.
- [50] HANNA, S. R., Briggs, G. A., a Hosker, Jr., R. P. 1982. Handbook on Atmospheric Diffusion. Report DOE/IC-11223, U.S. Dept of Energy, Technical Information Center. 102 pp.
- [51] HAVENS, J. a SPICER, T. Development of an Atmospheric Dispersion Model for Heavier-than-Air Gas Mixtures, Vol I. Report CG-D-22-85, U.S. Coast Guard. 1985. 158 pp.
- [52] HIRSCHBERG, S., BURGHERR, P., SPIEKERMAN, G., a DONES, R. Severe accidents in the energy sector: comparative perspective. *Journal of Hazardous Materials* [online]. 2004, 7., roč. 111, č. 1-3, s. 57–65 [cit. 3. 3. 2014]. ISSN 03043894. Dostupné z: doi:10.1016/j.jhazmat.2004.02.009
- [53] HRÁDEK, F., a KURÍK, P. *Hydrologie. 1. vyd. Praha: Česká zemědělská univerzita v Praze, 2004. 280 s.* B.m.: ISBN 80-213-0950-4. 2004.
- [54] HYMES, I., BOYDELL, W., a PRESCOTT, B. *Thermal radiation: physiological and pathological effects*. B.m.: Institution of Chemical Engineers, 1996.
- [55] JONKMAN, S. N., VAN GELDER, P. H. A. J. M., a VRIJLING, J. K. An overview of quantitative risk measures for loss of life and economic damage. *Journal of Hazardous Materials* [online]. 2003, roč. 99, č. 1, s. 1–30 [cit. 3. 3. 2014]. ISSN 03043894. Dostupné z: doi:10.1016/S0304-3894(02)00283-2
- [56] KHAN, F. I., a ABBASI, S. A. Techniques and methodologies for risk analysis in chemical process industries. *Journal of Loss Prevention in the Process Industries*. 1998, roč. 11, č. 4, s. 261–277.
- [57] KIRCHSTEIGER, Ch. On the use of probabilistic and deterministic methods in risk analysis. *Journal of Loss Prevention in the Process Industries*. 1999, roč. 12, č. 5, s. 399–419.
- [58] KÖPPKE, K. E. *Discussion document* [online]. Dreden, Germany: OECD Workshop on Natech Risk Management, 2012. Dostupné z: <http://www.oecd.org/env/ehs/chemical-accidents/50337868.pdf>
- [59] LOWESMITH, B. J., HANKINSON, G., ACTON, M. R., a CHAMBERLAIN, G. An Overview of the Nature of Hydrocarbon Jet Fire Hazards in the Oil and Gas Industry and a Simplified Approach to Assessing the Hazards. *Process Safety and Environmental Protection* [online]. 2007, roč. 85, č. 3, s. 207–220 [cit. 3. 3. 2014]. ISSN 09575820. Dostupné z: doi:10.1205/psep.06038
- [60] MANNAN, S. *Lees' Loss prevention in the process industries: Hazard identification, assessment and control*. B.m.: Butterworth-Heinemann, 2004.
- [61] MCGRATTAN, K. B., BAUM, H. R., a HAMINS, A. Thermal radiation from large pool fires. *NISTIR-6546, NIST, Gaithersburg, Md., USA* [online]. 2000 [cit. 3. 3. 2014]. Dostupné z: <http://gisceu.net/PDF/U802.pdf>
- [62] MIKAELIS, P. *Guide méthodologique UFIP pour réalisation des études de danger en raffineries, stockages et dépôts de produits liquides et liquéfiés. Section 2: Modeles normalises des quantification deterministe*. UFIP ENV-MHS-98.09.25. 1998.
- [63] MINISTERSTVO VNITRA. *Statistická ročenka 2013 Česká republika*. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru České republiky, 2014.
- [64] MINISTERSTVO ZEMĚDĚLSTVÍ. *Zemědělská výroba. eAgri Zemědělství* [online]. 2013. Dostupné z: <http://eagri.cz/public/web/mze/zemedelstvi/>
- [65] MÖLLER, N., a HANSSON, S. O. Principles of engineering safety: Risk and uncertainty reduction. *Reliability Engineering & System Safety* [online]. 2008, roč. 93, č. 6, s. 798–805 [cit. 3. 3. 2014]. ISSN 09518320. Dostupné z: doi:10.1016/j.ress.2007.03.031
- [66] MUNOZ, M., ARNALDOS, J., CASAL, J., a PLANAS, E. Analysis of the geometric and radiative characteristics of hydrocarbon pool fires. *Combustion and Flame* [online]. 2004, roč. 139, č. 3, s. 263–277 [cit. 3. 3. 2014]. ISSN 00102180. Dostupné z: doi:10.1016/j.combustflame.2004.09.001
- [67] MŽP ČR. *Metodologie pro identifikaci a vyhodnocení kumulativních a synergických jevů* [online]. B.m.: Praha. 2001. Dostupné z: [http://www.env.cz/AIS/web-pub.nsf/\\$pid/MZPKHF6OS6AA](http://www.env.cz/AIS/web-pub.nsf/$pid/MZPKHF6OS6AA)

- [68] NEVRILÝ, V. *Strategie a metody modelování požáru nádrže kapalných uhlovodíků*. Ostrava, 2009. Disertační práce. Vysoká škola báňská - Technická univerzita Ostrava.
- [69] NEVRILÝ, V. et al. Predicting the formation and the dispersion of toxic combustion products from the fires of dangerous substances. In: *EGU General Assembly Conference Abstracts*. 2012, s. 13351.
- [70] OECD. *Report of the Special Session on Environmental Consequences of Chemical Accidents*. 7. Paris, France: OECD. 2000. *Series on Chemical Accidents*.
- [71] PALAZZI, E., FAVERI, M. D., FUMAROLA, D., a FERRAILOLO, G. Diffusion from a steady source of short duration. *Atmospheric Environment*, 1982. Vol. 16, No. 12, pp. 2785-2790.
- [72] PEARCE, F. After Bhopal, Who Remembered Ixhuatepec? *New Scientist*. 1985, roč. 107, s. 22–3.
- [73] PERILHON, P. Méthode d'analyse de risques MOSAR. In: *Ecole d'été „Gestion Scientifique du risque ”* [online]. 1999. Dostupné z: <http://www.v1.agora21.org/ari/perilhon1.html>
- [74] PERILHON, P., a LAURENT, A. Method MADS-MOSAR: A general tool for risk analysis. In: *Risques industriels et risques urbains: Vers une même approche?: 14. Entretiens Jacques Cartier*. 2001.
- [75] PERSSON, H., a LZONNERMARK. *Tank fires: review of fire incidents 1951-2003: BRANDFORSK Project 513-021*. Borås: SP Sveriges Provnings- och Forskningsinstitut, 2004. ISBN 9178489873 9789178489879.
- [76] PIERORAZIO, A. J., THOMAS, J. K., BAKER, Q. A., a KETCHUM, D. E. An update to the Baker-Strehlow-Tang vapor cloud explosion prediction methodology flame speed table. *Process Safety Progress* [online]. 2005, roč. 24, č. 1, s. 59–65 [cit. 3. 3. 2014]. ISSN 1066-8527, 1547-5913. Dostupné z: doi:10.1002/prs.10048
- [77] POKORNÝ, J. et al. *Urgentní medicína*. Praha: Galén, 2004. ISBN 80-7262-259-5.
- [78] POWELL, T. The Buncefield Investigation: third progress report. *Report prepared for the Buncefield Major Incident Investigation by the Health and Safety Executive (HSE) and the Environment Agency (EA), 10th May*. 2006.
- [79] PŘICHYSTALOVÁ, R. Analýza přechodu klasifikace nebezpečných látek na GHS z pohledu zákona 59/2006 Sb. 2009.
- [80] PŘICHYSTALOVÁ, R., a BAUDIŠOVÁ, B. Nový přístup v rámci direktivy SEVESO z pohledu CLP. In *Aktuálne otázky bezpečnosti práce: New Trends In Safety and Health*. Štrbské pleso: Technická univerzita v Košiciach, 2011. ISBN 978-80-553-076-0.
- [81] RAJ, P. K. Large hydrocarbon fuel pool fires: Physical characteristics and thermal emission variations with height. *Journal of Hazardous Materials* [online]. 2007, roč. 140, č. 1-2, s. 280–292 [cit. 3. 3. 2014]. ISSN 03043894. Dostupné z: doi:10.1016/j.jhazmat.2006.08.057
- [82] ROBERTS, T., GOSSE, A., a HAWKSWORTH, S. Thermal radiation from fireballs on failure of liquefied petroleum gas storage vessels. *Transaction of Institution of Chemical Engineers*. 2000, roč. 78.
- [83] SADEE, C., SAMUELS, D. E., a O'BRIEN, T. P. The characteristics of the explosion of cyclohexane at the Nypro (UK) Flixborough plant on 1st June 1974. *Journal of Occupational Accidents*. 1977, roč. 1, č. 3, s. 203–235.
- [84] SALVI, O., a DEBRAY, B. A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive. *Journal of Hazardous Materials* [online]. 2006, roč. 130, č. 3, s. 187–199 [cit. 3. 3. 2014]. ISSN 03043894. Dostupné z: doi:10.1016/j.jhazmat.2005.07.034
- [85] SHALUF, I. M., a ABDULLAH, S. A. Floating roof storage tank boilover. *Journal of Loss Prevention in the Process Industries* [online]. 2011, roč. 24, č. 1, s. 1–7 [cit. 3. 3. 2014]. ISSN 09504230. Dostupné z: doi:10.1016/j.jlp.2010.06.007
- [86] SCHILLER, R. Inferno at Tocoa. *Industrial fire world* [online]. 2009, roč. 24, č. 3. Dostupné z: http://www.fireworld.com/ifw_articles/boilover_0409.php
- [87] SKŘEHOT, P. et al. *Prevence nehod a havárií: 1. díl: Nebezpečné látky a materiály*. B.m.: Praha: Pink Pig sro, 2009. ISBN 978-80-86973-73-9.
- [88] SKŘEHOT, P. et al. *Prevence nehod a havárií: 2. díl: Mimořádné události a prevence nežádoucích následků*. B.m.: Praha: Pink Pig sro, 2009. ISBN 978-80-86973-73-9.
- [89] SKŘÍNSKÝ, J. Application of emergency planning criteria for the control of major accident hazards - Calculation of the consequences of fire accidents. In: *Proceedings of the European Safety and Reliability Conference ESREL*. Netherlands (Amsterdam): CRC Press Book, 2013. ISBN 978-1-138-00123-7. In: . 2013.
- [90] SKŘÍNSKÝ, J. et al. Description of Physical-Chemical Parameters of Pool-fire. *Časopis výzkumu a aplikací v profesionální bezpečnosti*. 2013, roč. 6, 3-4. Dostupné z: <http://www.bozpinfo.cz/josra/josra-03-04-2013/pool-fire.html>. ISSN 1803-3687. 2013.
- [91] SKŘÍNSKÝ, J. et al. The experiences with the software for jet fire thermal radiation modelling. *Časopis výzkumu a aplikací v profesionální bezpečnosti*. 2013, roč. 6, 3-4. Dostupné z: <http://www.bozpinfo.cz/josra/josra-03-04-2013/jet-fire.html>. ISSN 1803-3687. 2013.
- [92] SKŘÍNSKÝ, J. et al. Validation possibilities of the BLEVE thermal effects. *Časopis výzkumu a aplikací v profesionální bezpečnosti*. 2013, roč. 6, č. 2. Dostupné z: <http://www.bozpinfo.cz/josra/josra-02-2013/bleve.html>. ISSN 1803-3687. 2013.
- [93] SLUKA, V. Implementace směrnice 2012/18/EU (Seveso III) a analýza a hodnocení rizik v České republice. [online]. 2013, roč. 6, č. 3-4. ISSN 1803-3687. Dostupné z: <http://www.bozpinfo.cz/josra/josra->

- 03-04-2013/implementace-sevesolll-v-cr.html
- [94] SPICER, T., a HAVENS, J. User's Guide for the DEGADIS 2.1 Dense Gas Dispersion Model Cincinnati OH: Report EPA-450/4-89-019, U.S. Environ. Protection Agcy. 1989.
 - [95] STUČHLÁ, K. *Hodnocení dopadů závažných havárií na životní prostředí*. Ostrava, 2006. Disertační práce. Vysoká škola báňská - Technická univerzita Ostrava.
 - [96] ŠRÁČEK, O., DATEL, J., MLS, J. et al. *Kontaminační hydrogeologie*. B.m.: Karolinum, 2002.
 - [97] TANG, M. J., a BAKER, Q. A. A new set of blast curves from vapor cloud explosion. *Process Safety Progress*. 1999, roč. 18, č. 4, s. 235–240.
 - [98] TEPLÝ, Z. *Požáry otevřených technologických zařízení v chemickém a petrochemickém průmyslu: Konspekty odborné přípravy jednotek požární ochrany II*. Ostrava: Sdružení požárního a bezpečnostního inženýrství v Ostravě, 2001. ISBN ISBN 80-86111-89-X.
 - [99] TIXIER, J., DUSSEY, G., SALVI, O., a GASTON, D. Review of 62 risk analysis methodologies of industrial plants. *Journal of Loss Prevention in the process industries*. 2002, roč. 15, č. 4, s. 291–303.
 - [100] TNO. Safety Software EFFECTS Version 7 User and Reference Manual. *TNO Built Environment & Geosciences, Department of Industrial and External Safety, Utrecht, the Netherlands*. 2007.
 - [101] TNO. *Methods for the calculation of physical effects due to releases of hazardous materials (liquids and gases) - Yellow Book*. The Hague: Committee for the Prevention of Disasters, 1997. CPR 14E.
 - [102] TNO. *Guidelines for Quantitative Risk Assessment, Purple Book*. CPR 18E. 1999.
 - [103] TNO. *Methods for the determination of possible damage to people and objects resulting from releases of hazardous materials „Green book”*. CPR E 16. 2005.
 - [104] U.S. DEPARTMENT OF ENERGY. *Applying the ALARA process for radiation protection of the public and environmental compliance with 10 CFR part 834 and DOE 5400.5 ALARA program requirements*. 1997.
 - [105] U.S. DEPARTMENT OF LABOR OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION. *Process Safety Management Guidelines for Compliance*. B.m.: U.S. Government Printing Office, 1994.
 - [106] US EPA. Technical Guidance for Hazards Analysis [online]. 1987 [cit. 3. 3. 2014]. Dostupné z: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.398.6488&rep=rep1&type=pdf>
 - [107] US EPA. *Risk Management Program Guidance for Offsite Consequence Analysis*. B.m.: US Environmental Protection Agency, Office of Solid Waste and Emergency Response, Chemical Emergency Preparedness and Prevention Office, 1999. 9.
 - [108] US EPA. *ALOHA user's manual*. 2006.
 - [109] WHO. *General scientific principles of chemical safety*. B.m.: World Health Organization Geneva, 2000.
 - [110] *Úmluva o účincích průmyslových havárií přesahujících hranice států*. Helsinky, Finsko. 1992
 - [111] HSE: Jet Fires. *Health and Safety Executive* [online]. 2010. [cit. 3. 3. 2014]. Dostupné z: <http://www.hse.gov.uk/offshore/strategy/jet.htm>
 - [112] TNI 01 0350. *Management rizik: Slovník (Pokyn 73)*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2010
 - [113] *Směrnice Evropského parlamentu a Rady 2012/18/EU ze dne 4. 7. 2012 o kontrole nebezpečí závažných havárií s přítomností nebezpečných látek a o změně a následném zrušení směrnice Rady 96/82/ES*. Dostupný na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:197:0001:0037:CS:PDF>.

Komunikace¹

Začátkem je vhodné nastínit, co je to vůbec komunikace o rizicích. Jedna z možných definic uvádí, že se jedná se o praktickou disciplínu založenou na vědeckých základech, která se soustřeďuje na jakoukoliv smysluplnou výměnu informací ohledně zdraví nebo rizik mezi zainteresovanými stranami (Covello, 2004), v našem případě zaměstnanci, vedením, klienty atp. Nicméně pro pochopení charakteru celého oboru (oblasti) je důležité zasazení do širšího kontextu. Ať už se bude jednat o historický vývoj, vztah k ostatním disciplínám nebo příslušnost k širšímu pojetí vědy o bezpečnosti.

Výše zmíněná definice je konsensem pohledů mnoha odborníků a zástupců odborných institucí. Stejnou vypovídací hodnotu však mohou mít definice samostatných výzkumníků. Začátkem je vhodné nastínit, co je to vůbec komunikace o rizicích. Jedna z možných definic uvádí, že se jedná se o praktickou disciplínu založenou na vědeckých základech, která se soustřeďuje na jakoukoliv smysluplnou výměnu informací ohledně zdraví nebo rizik mezi zainteresovanými stranami. (Covello, 2004). Nicméně pro pochopení charakteru celého oboru (oblasti) je důležité zasazení do širšího kontextu. Ať už se bude jednat o historický vývoj, vztah k ostatním disciplínám nebo příslušnost k širšímu pojetí vědy o bezpečnosti.

Problémem oboru komunikace o rizicích je jeho zdánlivá jasnost a známost. Každý má pocit, že si umí pod označením „komunikace o rizicích“ konkrétně představit, o co se jedná. „Mluvení o riziku“, „sdělování rizika“, „vzdělávání v oblasti rizik“, atd. Tento automatický odhad je navíc umocněn tím, že komunikace je proces, který každý člověk nejen zná, ale i každodenně používá, a riziko je pojem, který je poměrně zřejmý i člověku, který není přímo spojen s průmyslem nebo s nebezpečnými technologiemi.

Často se tak může stát, že lidé pokládají své zkušenosti a poznatky za rovnocenné výsledkům odborných studií, aniž by k tomuto oboru a jeho metodologii měli příslušnou teoretickou základnu. Paradoxně se tak dopouštějí zkreslení a odhadů, kterým se snaží komunikace o rizicích předcházet. Sdílení poznatků, zkušeností a pozorování je klíčové, ale pro komplexní pochopení a obraz je potřeba využívat metody vědecké práce. Přírodu člověk také pozoruje a zažívá osobně, přesto nelze odvodit vazby v ekosystému pouze na základě několika

¹ Autor děkuje spoluřešitelům projektu BV MVČR - VG20132015131, KOMRISK - ZEFEKTIVNĚNÍ KOMUNIKACE O RIZICÍCH PRO ZVÝŠENÍ BEZPEČNOSTI OBYVATEL V RÁMCI NOVELIZACE ZÁKONA O PREVENCI ZÁVAŽNÝCH HAVÁRIÍ, za významný přínos k této a k následující kapitole.

necílených pozorování. V tomto je oblast komunikace o rizicích zrádná a vyžaduje odmyšlení si osobních představ a vybudování si jejího obrazu od počátku.

Podle OECD je komunikace o rizicích: „Komunikací směrem k pracovníkům nebo veřejnosti o průmyslových, zdravotních, environmentálních, sociálních, katastrofických rizicích nebo hrozbách, které mohou mít potencionální dopad na vystavenou populaci, komunitu nebo jednotlivce.“ (OECD, 2002)

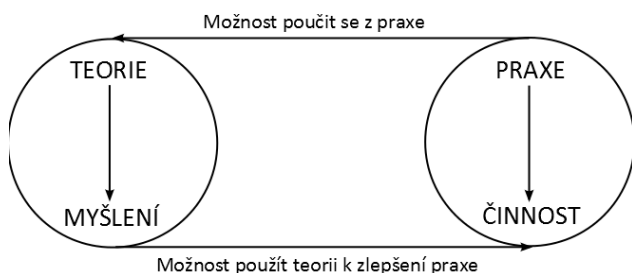
Teorie nebo praxe?

Způsob, kterým poznáváme svět, výrazně ovlivňuje naše vnímání a myšlení, a to nejen na osobní, ale především na profesní úrovni. Důležitost vymezení vzájemného vztahu „teorie“ a „praxe“ vyvstává na povrch během každé snahy definovat přesněji a jednoznačněji to, co je komunikace o rizicích. V závislosti na zvoleném pohledu či postoji se také výrazně mění zvolené metody, kterými lze poznávat proces komunikace o rizicích.

Komunikace o rizicích má totiž výrazně dvojí povahu. Na jedné straně se jedná o praktickou disciplínu, ale na straně druhé je založena na teoretických základech. Kombinací teoretických a praktických poznatků lze dosáhnout zefektivňování komunikace o rizicích. Je zde ovšem také největší riziko bádání v oblasti komunikace o rizicích.

Teorie a praxe jsou dva odlišné světy, které používají odlišné metody, jazyk a přístupy. Je proto skutečnou výzvou, aby tyto dva světy mohly a uměly mezi sebou navzájem komunikovat a posouvat se kupředu. To je mimochodem zajímavý paradox, když samotná komunikace o komunikaci je obtížnou disciplínou a zkoumané procesy jsou ty samé procesy, které vedou ke sdělování poznatků o těchto procesech.

Jedním z nejčastějších předsudků je vnímání teorie a praxe samostatně, bez vzájemné návaznosti. Ve skutečnosti však teorie slouží ke zlepšení praxe a praxe nám poskytuje možnost se poučit a zlepšit teorii. Viz obrázek č. 17.



Obrázek 17 Vztah teorie a praxe (Manák, 2011)

Srovnání přírodních věd a humanitních věd je pro oblast komunikace o rizicích v rámci prevence závažných havárií klíčové. Na jedné straně stojí analýzy založené na přírodních vědách, ale samotný proces komunikace informací, reakce na obsah zpráv, změny v chování, účel těchto analýz, předpokládané přijetí opatření atd. jsou cílem věd humanitních, ať už se jedná o sociologii, psychologii nebo filosofii.

Management rizika a komunikace o rizicích jsou součástí tzv. vědy o bezpečnosti, o které se na akademickém poli v současné době živě diskutuje s cílem určit, zda se jedná o samostatný obor a zda existuje společný objekt zkoumání. Je třeba zdůraznit fakt, že jde o multidisciplinární obor, ale také skutečnost, že se jedná převážně o poznatky a metody sociálních věd jako je filosofie (k čemu slouží analýzy rizik), sociologie (jak lidé budou reagovat na přijatá opatření), politologie (jaká rozhodnutí je dobré udělat), ekonomie (jaká rozhodnutí je výhodné udělat) nebo psychologie (jak lidé konstruují svůj svět a na základě čeho se rozhodují).

Funkce a cíle komunikace o rizicích

Stejně jako v případě oblasti komunikace obecně, i komunikaci o rizicích lze nejlépe definovat podle jejích funkcí. Podle (Renn, 2008) existují čtyři kategorie všeobecně platných funkcí. Jedná se o tyto:

1. Osvětová funkce. Cílem této funkce je zaručit, že příjemci zprávy jsou schopni pochopit její obsah a efektivně tak zvýšit své obecné znalosti o komunikovaných rizicích.
2. Funkce důvěryhodnosti. Cílem této funkce je vytvořit vztah důvěry mezi tvůrcem zprávy a jejím příjemcem.
3. Funkce podpory snižování rizika. Cílem této funkce je přesvědčit příjemce zprávy ke změně svého postoje nebo přístupu v závislosti na typu rizika. Například volba nošení ochranných oděvů, výběr kvalitnějšího jídla, apod.
4. Funkce kooperativního rozhodování. Cílem této funkce je vytvořit podmínky pro efektivní zapojení zainteresovaných stran v otázce rizik tak, aby se obě zasažené strany mohly účastnit procesu řešení konfliktu.

Renn (Renn, 2008; Renn, 1991) dále blíže specifikuje, ke kterým cílům by měla komunikace o rizicích vést. Tyto cíle jsou zvoleny tak, aby vznikla tzv. komunikační aréna, kde se jednotlivé zainteresované strany mohou navzájem obohacovat a učit. Jedná se o tyto cíle:

1. Dosáhnout porozumění mezi příjemcem a odesílatelem zprávy, zajištění prostředí, které toto podporuje.
2. Přesvědčit příjemce zprávy pro změnu svého postoje a chování vzhledem k podstatě rizika.
3. Poskytnout podmínky pro racionální debatu týkající se rizik tak, aby se všechny zainteresované skupiny mohly podílet na efektivním a demokratickém řešení možného konfliktu.

4. Vytvoření vztahu důvěry mezi institucemi a širokou veřejností.

Prvním nutným prvkem pro efektivní komunikační proces jsou tedy dobře definované cíle. Na obecné úrovni sice lze sestavit proces, který tyto cíle nemusí mít explicitně definovány, a i přesto tento proces může být úspěšný. Je to dáno především skutečností, že samotná oblast komunikace o rizicích nedává jinou možnost než komunikovat rizika. Důraz je zde kladen především na souběh jednotlivých cílů a jejich kompletnost. Bez atmosféry důvěry nelze přesvědčit příjemce pro změnu svého postoje, atd., stejně tak nelze atmosféru důvěry eticky vybudovat, pokud jedním z cílů bude zatajit některé informace.

Je potřeba si uvědomit, že v západním světě dochází k ideologickému střetu mezi morálkou (etikou) a ekonomickým utilitarismem (užitek vyjadřovaný penězi). Přestože morálně a eticky je lidský život nevyčíslitelný, pro zpracování analýz např. v pojišťovnictví, bezpečnosti práce nebo v rámci prevence závažných havárií je lidský život vyčíslován penězi a stejně tak jsou pro prevenci a záchranu alokovány zdroje, které nezaručují 100% bezpečí všem obyvatelům.

Vývoj komunikace o rizicích

Komunikace a její vznik jsou stále jistou záhadou. Lidská komunikace je však výjimečná použitím symbolů a především jazyka. Ať už se přikloníme k teorii, že se jazyk v průběhu evoluce vyvíjí od jednoduchého ke komplexnímu, nebo k teorii, že jazyk a schopnost komunikovat člověk získává ze svého genetického kódu (Chomsky, 1965), tak je nutno přiznat, že se v současné době o komunikaci stále mnoho nevíme.

Lidé se komunikaci věnují od pradávna. Věnoval se jí Aristoteles nebo například Tomáš Akvinský. Z našeho pohledu je však nejzajímavější a nejdůležitější 20. století, kdy se věda o bezpečnosti začala formovat do podoby, ve které ji známe teď. Jedná se o období po válce, v 50. letech, kdy se poprvé začala objevovat témata přijatelnosti, kvantifikace a hodnocení rizik. V této době se začal také poprvé řešit vztah mezi člověkem a životním prostředím a objevují se první náznaky o udržitelném rozvoji.

Teprve v letech 1960 až 1970 bylo obecně přijímáno hodnocení a posuzování rizika na základě nově vznikajících analýz. V 70. letech se také překotně začal rozvíjet výzkum rozhodovacích procesů a faktorů, které ovlivňují vnímání rizika. Do roku 1970 bylo také převažujícím okruhem zájmu nebezpečí (hazard). Nebezpečí bylo vnímáno z hlediska přírodního, technologického, ale také sociálního.

Nová etapa začala v 80. letech, kdy se okruhem zájmu stala namísto nebezpečí zranitelnost. V této době se objevují první snahy a zmínky o participaci. Především se ale jedná o vrchol rozvoje oblasti percepce (vnímání) rizika. V této době se badatelé snažili popsat kulturu vědeckými metodami a snažili se odlišit mezi jednáním člověka jako součásti přírody a jednáním člověka spojeného s naučenými vzorci ze strany společnosti (Kulturní teorie). V oblasti rozvoje se v této době prosazují zásady decentralizace, osvobození trhu a začíná se výrazněji rozvíjet občanský sektor (NGOs).

Zlatou érou z dnešního pohledu je období kolem roku 1990, kdy začaly být poznatky předchozích let v oblasti percepce přenášeny do praxe a vznikl samostatný obor komunikace o rizicích zaměřený na informace, zprávy, média a proces dialogu. V této době pokračuje prosazování udržitelného rozvoje a dobré governance (správy).

V současném století zacházíme se starými koncepty, ale setkáváme se s mnoha novými. Tam, kde byl v minulosti kladen důraz na snižování zranitelnosti, se dnes snažíme budovat odolnost (resilienci), idea udržitelného rozvoje je stále klíčová, participativní přístupy nelze nadále přehlížet a dochází k jasnému přechodu (kvalitativnímu) k zahrnutí psychosociálních aspektů v rámci hodnocení rizik. Od roku 2000 také zřetelně operují obory percepce rizika a komunikace o rizicích v rámci studií managementu a governance. Na počátku komunikace o rizicích

převažovala jednosměrná komunikace. Cílem komunikace v této době bylo poskytování informací směrem k lidem tak, aby se rozdíly co nejvíce vyrovnaly. Dlouhodobý odklon lidí od předpokládaného výsledku byl připisován na vrub ignoranci a hlouposti lidí.

Později bylo dokázáno, že zvýšení rozsahu informací nevede k větší informovanosti pracovníků, a proto se pozornost přesunula na změnu chování a vnímání jinak než prostřednictvím poskytování informací. V této době již byl opuštěn jednosměrný model a badatelé se snažili zkoumat způsoby, jakými lidé pracují s informacemi. Cílem této etapy bylo přesvědčovat a měnit chování.

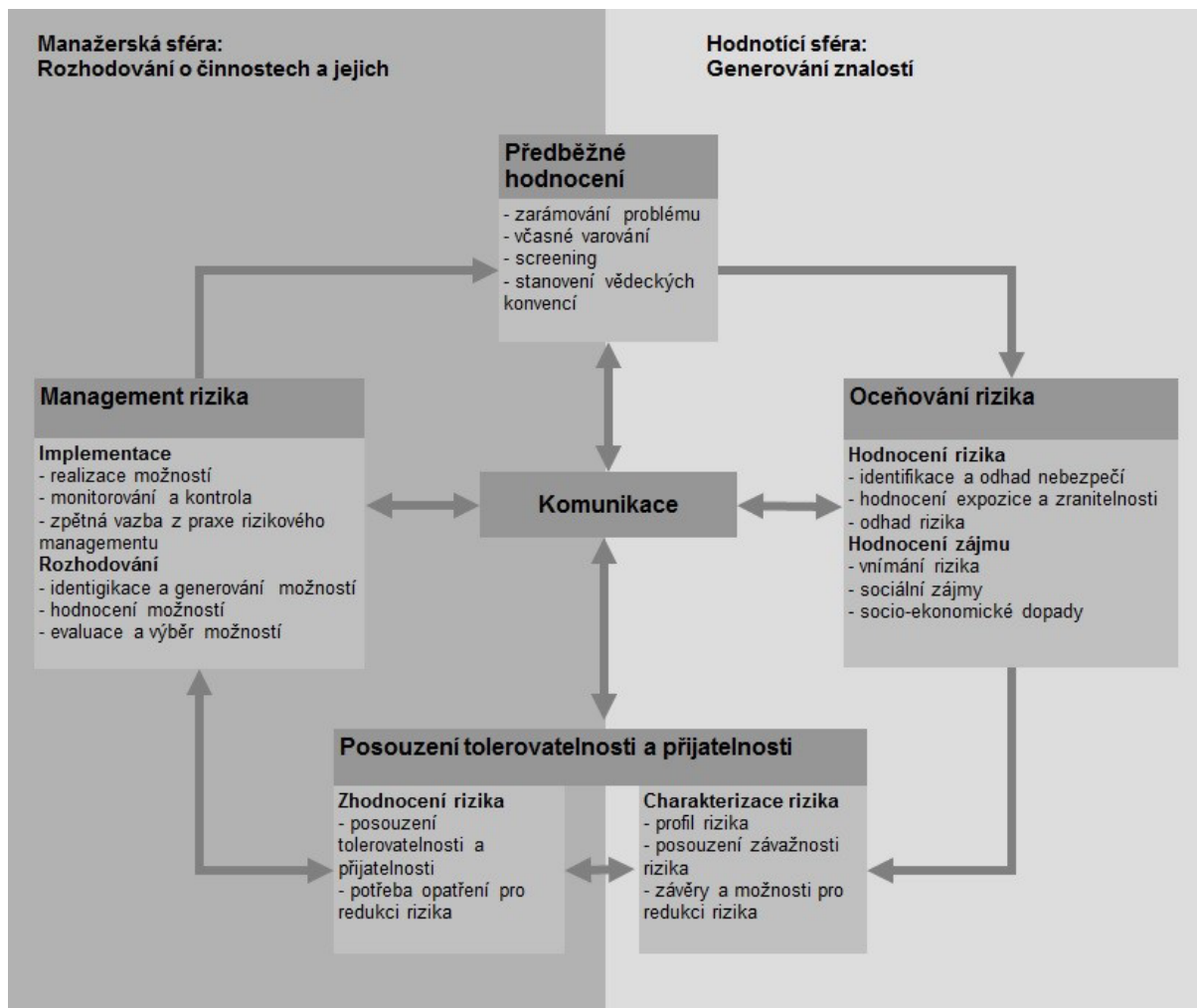
Zatím poslední etapou je obousměrná komunikace, která stále pracuje s informacemi, ale snaží se měnit chování. Změnou je přijetí předpokladu, že všichni účastníci procesu mají právo se vyjádřit a mohou se od sebe navzájem učit (deliberace). Prostředkem k dosažení těchto cílů jsou často participativní (vzájemné) nástroje jako jsou například kulaté stoly, besedy s občany nebo workshopy.

Zásadním rozdílem mezi jednosměrnou komunikací a obousměrnou komunikací je souvislost. Jednosměrná komunikace je jednorázovou akcí ze směru odesílatele k příjemci se zaměřením na zprávu a její vizuální a obsahové zpracování. Oproti tomu obousměrná komunikace je dvoustranná souvislá interakce zaměřená na řešení problémů, hledání konsensu a na snahu přizpůsobit proces cílové skupině.

Riziko a jeho řízení

Jak bylo zmíněno výše, je nutné nakládat s dostupnými zdroji tak, aby byla zaručena co nejefektivnější možná ochrana lidem. K tomuto cíli slouží systém managementu rizik, jehož je komunikace o rizicích nedílnou součástí. V současné době je koncept managementu (řízení) rizik překonaný a je nahrazován tzv. governancí (správou) rizik. Tam, kde management rizik byl inkluzivní a krokový, je governance rizik otevřena všem zainteresovaným stranám a jednotlivé dílčí kroky jsou na sobě chronologicky závislé, ale zároveň umožňují mnohem flexibilnější propojení a obsahují systém zpětné vazby.

V rámci tohoto přístupu je komunikace o rizicích samostatným prvkem, který je však vlastní každému jinému kroku během celého procesu governance rizik. Viz následující obrázek:



Obrázek 18 Governance rizik (IRGC, 2007)

Komunikace o rizicích je tedy nástrojem k prosazování mnoha vyšších cílů, ať už se jedná o ochranu morálních zásad, prosazování principu udržitelného rozvoje nebo jako součást procesů řízení rizika.

Nakládání s rizikem však není jednotnou oblastí. Existuje mnoho přístupů s odlišnými nástroji.

Pro jednotlivé oblasti platí stejná proměnná, kterou je snaha zvládat rizika. Nicméně nástroje a cíle jsou často odlišné, nehledě na to, že je za riziko považováno vždy něco trochu jiného. Pro oblast PZH je platná oblast strojírenského managementu rizika (prevence havárie) a management přírodních rizik (prevence ztrát), protože snaha zvládnout nakládání s nebezpečnými látkami za co nejnižšího rizika tvoří velkou část systému prevence závažných havárií (prevence havárií). Nicméně nelze zapomínat na prevenci ztrát, které jsou do jisté míry shodné s nástroji a postupy v rámci prevence přírodních katastrof. Obecným cílem je totiž sebezvědomý občan schopný sebezáchran. Informace týkající se rizika se liší, ale principiálně se jedná o týž systém.

Vraťme se však ještě k vlastnímu riziku jako samostatnému jevu. Existuje riziko samo o sobě nebo se jedná o sociální konstrukt? Vzhledem k vysoké komplexitě komunikace o rizicích je nutno riziko vnímat a pracovat s ním v nejvyšší možné šíři. Možná trochu analogicky s předchozím seznamem přístupů k řízení rizika existuje vícero pohledů na riziko. Viz též obrázek

č. 4. V rámci komunikace o rizicích není účelné soustředit se na jednotlivé pohledy samostatně, ale je nutno pracovat se všemi, tzn. integrálně.

O něco odlišnější možnost pohledu na rizika je z hlediska jejich poznatelnosti a komplexity. Jde tedy o to, že určitý typ rizika zasahuje do určité oblasti lidského života a čím je riziko obtížněji uchopitelné, tím zasahuje do života více, a je potřeba pokročilejších prostředků k efektivní komunikaci o rizicích.

Prvním případem ze čtyř jsou lineární rizika. Jedná se o typ rizika, která jsou známa, a je dobře známo, jaké důsledky z těchto rizik vyplývají, a zároveň jsme si vědomi toho, jak s těmito riziky zacházet. Tento typ rizika v podstatě nevyvolává odezvu u obyvatelstva a cílem efektivní komunikace rizik této úrovně je poskytovat co nejpřesnější obraz a fakta, stejně tak jako popisovat přístupy, jak se vyrovnat se zbylými nejistotami z těchto rizik vyplývajících. Přestože je podstatou této úrovně komunikace snaha především o zjednodušený přenos informací, je i zde nutno vytvořit obousměrnou komunikaci pro zajištění toho, že je komunikovaná informace pochopena. (Renn, 1991; Renn, 2008)

Dalším typem jsou vysoce komplexní rizika, u kterých je velmi obtížné rozlišit a identifikovat vzájemné kauzální vztahy. Zároveň je v tomto případě obtížné identifikovat faktory způsobující rizika a k jejich nalezení je potřeba většího množství informací. Adekvátní reakcí na tento typ rizik je jednak debata, ale v mnoha případech je nutno uchýlit se k odlišnému přístupu. Druhým typem prostředku komunikace vysoce komplexních rizik je komunikace o úrovni kompetence institucí pro zacházení s riziky. (Renn, 2008)

Při tomto typu rizika je důležité komunikovat o rozložení rizik a výhod, stejně jako o důvěryhodnosti institucí. Komunikace se tedy točí okolo faktu, zda jsou instituce schopny dostát svým mandátům, tedy zda splňují očekávání společnosti. Nutno podotknout, že tento způsob komunikace je ve vícestranné společnosti velice obtížný. Zdrojem konfliktu jsou v tomto případě zkušenosti, důvěryhodnost a chování institucí. Informační transfer ve většině případů nedostačuje a je proto nutné vytvořit/podpořit vzájemný dialog mezi stakeholdery a širokou veřejností. (Renn, 2008)

Třetím typem jsou rizika s vysokou mírou nejistoty. Jedná se o velmi komplexní vztahy, u kterých věda v současné době (za současného stavu poznání) není schopná přinášet jednoznačné výsledky.

Příkladem takového rizika je například vliv některých nebezpečných látek na zdraví člověka.

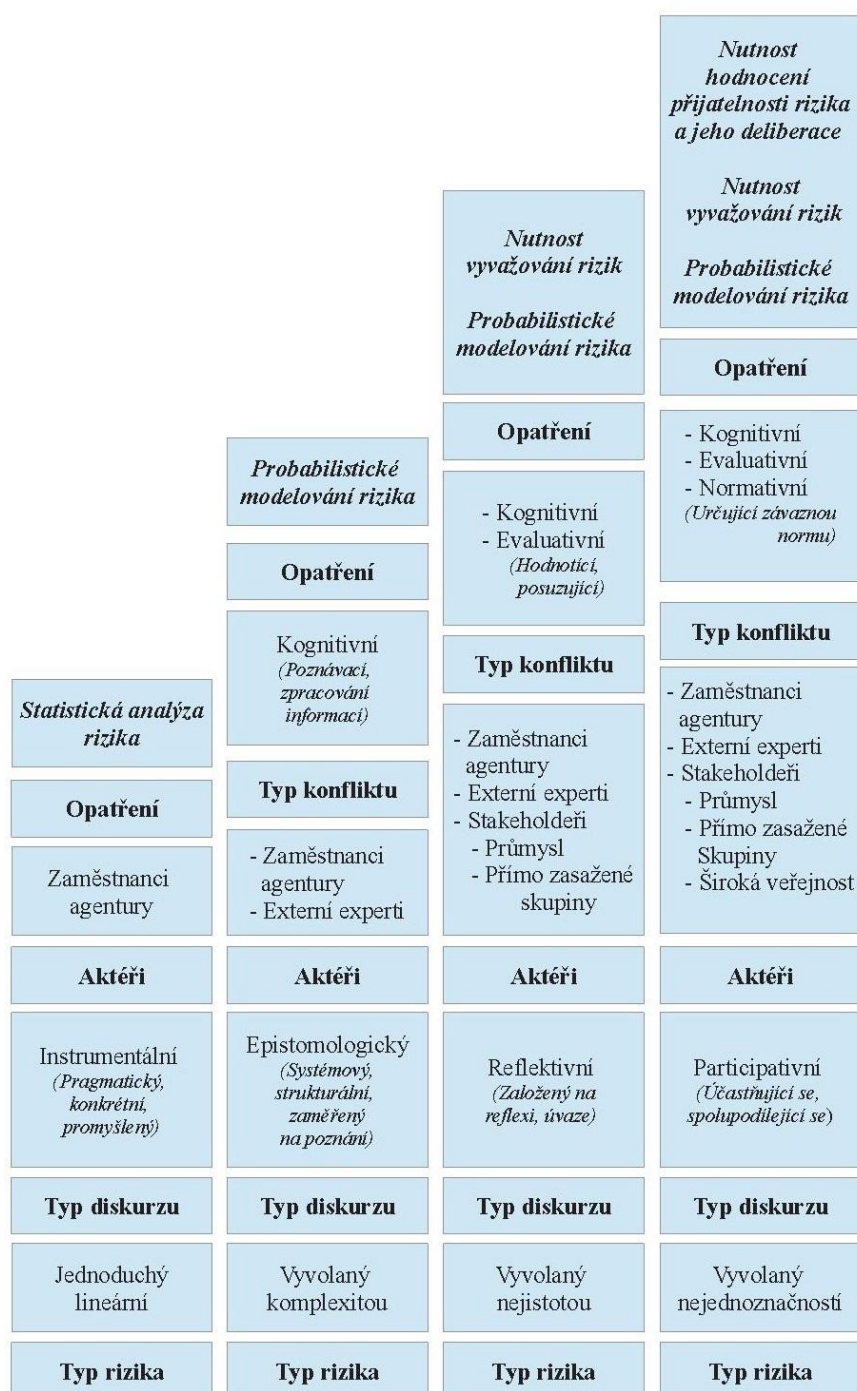
Přestože se daří mapovat možná rizika, je stále nad dosaženými výsledky vedena diskuze, a to z důvodu, že jsme si vědomi nedostatečnosti našeho poznání lidského těla k tomu, abychom mohli s vysokou pravděpodobností vyloučit negativní důsledky z dlouhodobého užívání dané látky.

Vědecká komunita tak musí počítat se strachem z neznáma, strachem z nejistot. Při tomto typu rizika je velice důležité, aby odpovědné instituce monitorovaly důsledky rizik a rychle reagovaly v případech, kdy jsou výsledky viditelné a negativní. Adekvátním způsobem reakce na tento typ rizika je vhodně a efektivně vedený dialog se stakeholdery a širokou veřejností. V ojedinělých případech použití participativních metod komunikace (workshopy, kulaté stoly, veřejné besedy, apod.). (Renn, 1998)

Posledním typem jsou rizika s potenciálem pro dvojznačnost a kontroverzi. Tato rizika mohou nést nejistoty, ale také nemusí. V každém případě se jedná o kontroverzní a emoce vyvolávající rizika. Příkladem může být nedobrovolné vystavení pozemním elektromagnetickým polím v okolí silnoproudých vysílačů nebo účinky větrných elektráren. Zde se nejedná o to, nakolik jsou rizika reálná, nakolik jsou zmapovaná, ale jedná se především o rizika, která vyvolávají silné emoční

reakce na straně veřejnosti, ať už se jedná o podloženou reakci nebo reakci nezakládající se na pravdě. V tomto případě jde o konflikt zasahující hodnoty a normy, životní styl, apod. U tohoto typu rizika je nejefektivnějším způsobem komunikace snaha o nalezení fundamentálního konsensu. Obecně se jedná o nejobtížnější formu komunikace a k jejímu uskutečnění slouží zangažovanost stakeholderů, mediace, občanské panely, otevřená jednání, apod. Cílem je nalézat taková řešení, která jsou přijatelná pro všechny zúčastněné. (Renn, 1998)

Schéma vhodných nástrojů komunikace o rizicích s ohledem na komplexitu rizika je znázorněn na obrázku č. 19.



Obrázek 19 Schéma závislosti aspektů komunikace o rizicích na typu rizika (Renn, 2008)

Posledním subjektem v tomto modelu komunikace jsou příjemci, kteří reinterpetují zprávu poslanou z primárního zdroje přes zdroj sekundární. Příjemce je koncovým a cílovým subjektem přenášené zprávy. Velmi důležitý je zde proces zpětné vazby, kdy jedině prostřednictvím tohoto procesu je možno posoudit, zda informace splnila svůj účel (zvýšila znalost příjemce, zvýšila míru důvěry směrem k instituci, dopomohla k behaviorální změně nebo pomohla vytvořit prostředí pro efektivní zapojení do rozhodovacích procesů). Pokud svou funkci nesplnila, pak je nutno proces opakovat s větší důrazem na specifičnost audience a s cílem identifikovat překážky v komunikaci. (Renn, 2008; Renn, 1991)

Toto je obecně velmi obtížná část procesu komunikace o rizicích, protože příjemce přijatou zprávu „dekóduje“ na základě vlastních zkušeností, postojů, kultury, apod. Podrobněji se tomuto fenoménu věnuje Kasperson et al. (Kasperson et al., 1988)

Kultura bezpečnosti

Co je to kultura bezpečnosti?

Kultura bezpečnosti má za cíl zapojení zaměstnanců a vedení. Jde o přístup zdola nahoru. Je založená na skutečném závazku vedení a odborné podpoře odborníků, aby bezpečnost a zdraví byly reálné hodnoty v každodenním životě podniku. Programy zaměřené na zvyšování kultury bezpečnosti jsou založené na chování a osobních postřezích zaměstnanců, kteří provádějí rutinní pracovní úkoly, stanovují nápravná opatření způsobem pozitivního koučování a mentoringu a poskytují včasnou zpětnou vazbu o nesprávném chování souvisejícím s bezpečností. Zaměstnanci nacházejí smysl v pravidlech BOZP, jsou zapojeni do jejich budování i jejich hájení a komunikace.

Pojem "kultura bezpečnosti" byl poprvé použit v jaderné energetice ve zprávě publikované IAEA (MAAE) v roce 1986 a byl rozpracován v dalších publikacích. Používá se ve spojení s bezpečností jaderných elektráren, avšak interpretace tohoto pojmu zůstala velmi volnou a principy definující kulturu bezpečnosti je možno použít pro hodnocení úrovně bezpečnosti i mimo jadernou energetiku. V prostředí rozvinutých firem je kultura bezpečnosti chápána jako nedílná součást firemní kultury.

Kultura bezpečnosti je definována jako soubor charakteristik a osobních postojů v organizaci a myšlení lidí, který zajišťuje, že problémům bezpečnosti je věnována nejvyšší priorita, odpovídající jejich významnosti.

Kulturu bezpečnosti popisují následující principy:

1. Každý je osobně odpovědný za bezpečnost.
2. Vedoucí demonstrují svoje postoje k bezpečnosti.
3. Nastoluje se atmosféra vzájemné důvěry.
4. Při rozhodování se zohledňuje „bezpečnost na prvním místě“.
5. Technologii respektujeme jako specifickou.
6. Podporuje se zvědavý přístup.
7. Učí se z chyb („jsme učící se organizace“).
8. Úroveň bezpečnosti se trvale ověřuje.

Úroveň kultury bezpečnosti je veličina, kterou není možno přímo a exaktně změřit, přesto má zásadní vliv na chování pracovníků, styl řízení i úroveň technologie. Proto by měly být periodicky prováděny průzkumy kultury bezpečnosti, které umožní definovat slabé a silné stránky v jednotlivých oblastech bezpečnosti a na tato zjištění reagovat. Porovnání časové řady průzkumů umožní vyhodnotit účinnost korektivních opatření.

Pro naplnění této odpovědnosti se vyžaduje závazek vytvořit a rozvíjet odpovídající podmínky a dostatečné lidské i finanční zdroje, účinné řídicí struktury a kontrolní mechanismy.

Types of Safety Cultures



Credit: Prof Patrick Hudson

Příklady z jaderné energetiky, kdy nedostatky vedly k závažným důsledkům pro bezpečnost nebo provoz²

Během nedávné doby doznala řada společností provozujících jaderné elektrárny a jaderné komponenty poměrně závažných změn. Účinnost řízení při provádění změn se liší od společnosti ke společnosti. Mezní případy, podle toho, jak jsou změny řízeny, mohou vést elektrárnu buď k vynikajícímu provozu, nebo k destrukci toho, co bylo kdysi efektivní organizací.

Jaderná energetika **čelí již určitou dobu nedostatku kvalifikovaných vedoucích pracovníků, kteří jsou si vědomi k jakým následkům může vést nezvládnutí vysoké koncentrace energie obsažené v jaderném palivu.** Havárie v Three Mile Island, Černobylu, zanedbání základních principů bezpečnosti v Ontario Hydro, Millstone, David Bessie, Pakši, ukazuje, kam vede vyhovívání tlakům na zvyšování zisku tím nejjednodušším způsobem, tj. nevhodnou „intensifikací“, nebo snižováním počtu kvalifikovaných pracovníků v jaderných elektrárnách. Je otázka, jak této tendenci čelit. Asi lze těžko očekávat, že akcionář bude

² Informace převzaty z <http://www.dukovany.cz/provozni-kultura-jaderne-bezpecnosti.html>

někým, kdo si bude přát něco jiného než dobrou dividendu a rovněž je nemožné od něho očekávat nezbytnou míru jaderně-energetické kvalifikace. Je jej ale snad možné upozornit na to, že může o svou dividendu přijít, bude-li uvažovat pouze z hlediska krátkodobých spekulativních ekonomických zájmů. Jak ukazují reálné příklady, nevhodné postupy vedení společnosti mohou vést k vyřazení bloku z provozu dočasně, nebo natrvalo a má pak pro akcionáře mnohonásobně větší negativní ekonomické dopady i když nemusí jít přímo o havárii. Ztráta provozní licence postačuje. Je užitečné si některé příklady připomenout a zamyslet se:

Společnost Ontario Hydro Nuclear (OHN) byla nucena v roce 1997 odstavit sedm ze svých devatenácti bloků z důvodů dlouhodobých problémů v metodách řízení i provozu zařízení. (Dva z těchto bloků dosud nebyly opětovně uvedeny do provozu). Rozhodnutí o odstavení bylo iniciováno potřebou naprosté změny přístupu ke kultuře provozu. Během výstavby a spouštění byla OHN mimořádně úspěšná, ale postupně se soustředila pouze na provozování a údržbu bloků (kterou omezovala). Výroba byla upřednostňována před bezpečností, což vyústilo v nekonzervativní rozhodování a nedostatek vhodného klimatu pro vytvoření dobré provozní kultury. Když bloky zestárly a zkušený personál byl nahrazován novým, začaly problémy. Vrcholové vedení společnosti i kanadský dozor nad jadernou bezpečností toleroval snížení úrovně bezpečnosti provozování, ačkoli externí i interní zprávy poukazovaly na značné provozně-bezpečnostní problémy. Sílily i požadavky vlastních zaměstnanců na zlepšení přístupu k bezpečnosti. Vrcholové vedení Ontario Hydro sledovalo především zisk a vytvářelo tlak na pokračování provozu za ne zcela standardních podmínek. Řada pokusů o vyřešení problémů - aplikace různých nápravných programů - byla neúspěšná. Byly zahajovány další a další změny v organizaci a řízení, aniž by bylo analyzováno, proč nebyly předcházející kroky úspěšné. Na situaci se podílela i absence účinného sledování vhodných ukazatelů a nedostatek účinného dozoru nad jadernou bezpečností ze strany vedoucích pracovníků. Příčinami degradace byla postupná ztráta kvalifikace personálu, „mazácký“ přístup nových, nezkušených, nedostatky v řízení, přehlížení chyb na všech úrovních organizace od představenstva směrem dolů. Kanadský jaderný dozor - Atomic Energy Control Board (AECB), na nedostatky upozorňoval a požadoval v mnoha oblastech nápravu. Požadoval prokázat výsledky nápravných opatření, ale viděl jen sérii neúspěšných pokusů. Několik krátkodobých zlepšení neukazovalo na celkový trend. Až do roku 1994 nebyl dosažen skutečný trvalý pokrok. Z důvodu nedostatku přidělených zdrojů a chyb vedení společnosti nebyly rozpoznány potenciální důsledky. Informace sice byly podávány představenstvu společnosti, avšak bez velkého výsledku. Nedostatek technické kvalifikace jim

neumožnila pochopit hloubku problému. Proces ozdravování byl pak dlouhodobý a velmi drahý, vedení společnosti muselo být vyměněno, společnost se však dosud z následků plně nevzpamatovala.

Případ Ontario Hydro je pro odbornou veřejnost poměrně znám [L6], případ Millstone je čerstvější (počátek v roce 1996) a zaslouží si detailnější připomenutí:

Dne 4. března 1996 vyšel v novinách Time Magazine, článek “**Nuclear Warriors**”, který popisoval (na základě svědectví dvou zaměstnanců) rutinní porušování bezpečnostních pravidel při překládkách paliva. Cílem bylo zkracovat čas potřebný pro výměnu paliva. Přestože bazén skladování paliva byl dimenzován na určitý zbytkový výkon, bylo rutinní praxí, že do něho byla při překládkách dočasně přeložena celá aktivní zóna, aniž se počkalo na pokles jejího zbytkového výkonu. Doba potřebná k uvedení vodní náplně bazénu do varu po případném výpadku chlazení byla pouze minuta. Zkrácení času jedné překládky přinášelo ekonomický efekt okolo 0,5 milionu US dolarů, za což byli vedoucí pozitivně hodnoceni a honorováni. Článek rovněž kritizoval jaderný dozor USA (NRC) za to, že přivíral nad porušováním předpisů oči, ačkoli si ho byl vědom. Článek popsal problémy, s nimiž se zaměstnanci setkávali, a které požadovali řešit od vedení elektrárny i od NRC. Obavy zaměstnanců byly vyjadřovány o mnoho let dříve, než NRC vydala pokyn na zastavení všech tří bloků. Provozovatel dodatečně potvrdil všechny obavy svou vlastní analýzou. Problémy zahrnovaly například i neefektivní vedení, nedostatky vědomí bezpečnostní kultury provozu, nedostatečné finanční zdroje poskytované vedením společnosti provozovaným blokům. Ačkoliv elektrárna vydala program na zlepšení činnosti, v němž byly nedostatky pojmenovány, NRC dostávala v letech 1985 až 1995 od zaměstnanců znepokojující informace, jejichž počet rostl rok od roku. Informace uváděly bezpečnostní problémy a chyby ve zvycích vedoucích pracovníků porušovat bezpečnostní kritéria tlakem na rychlejší plnění úloh.

Kořenová příčina byla v nedostatečné provozní kultuře společnosti. Střední a vrcholoví vedoucí pracovníci trvale podporovali porušování bezpečnostních pravidel s cílem snížit náklady, protože nedokázali odolat přáním ekonomického vedení společnosti. Vlastník – společnost Northeast Utilities - na článek v Time zareagoval propuštěním, přeložením, či předčasným pensionováním veškerých vrcholových a mnohých středních vedoucích pracovníků. Řada pracovníků NRC musela rovněž odejít. Společnost přiznala vinu za závažné porušování dvaceti pěti pravidel proti jaderné bezpečnosti a životnímu prostředí v období 1994 až 1996 a zaplatila pokutu 10 milionů dolarů, z nichž 5 milionů bylo přímo za porušování pravidel jaderné bezpečnosti. Šlo o vůbec největší pokutu, kterou NRC do té doby

provozovateli jaderné elektrárny udělila. Výše uvedený případ byl pouze jedním z mnoha. Ukázalo se například, že elektrárna nemá v pořádku ani provozní a projektovou dokumentaci, kterou bylo nutné dát do pořádku. Důsledkem ale bylo, že všechny tři bloky musely být odstaveny, blok číslo 1 natrvalo (bylo oceněno, že nápravná opatření by u něho byla příliš drahá), bloky 2 a 3 na cca dva a půl roku. Nápravné operace si vyžádaly přes miliardu dolarů, akcie společnosti Northeast Utilities spadly z 25 dolarů na cca 7 dolarů za akcii.

Nejdůležitějším úkolem bylo změnit kulturní návyky personálu, pokažené předcházejícím vedením, obnovit důvěru NRC, veřejnosti a mnohých pracovníků elektrárny. Byl zjištěn i nesoulad mezi provozní a projektovou dokumentací a projektovými předpoklady.

Na základě skutečností zjištěných na elektrárně Millstone odeslala NRC jaderným elektrárnám USA dopis (datován ve Washingtonu D.C. Oct. 9, 1996) s požadavkem informovat, jak je u nich zajištěn soulad mezi projektovými předpoklady, provozní dokumentací a skutečným stavem na elektrárnách. Společné hledání řešení vedlo provozovatele jaderných elektráren Spojených států k vytvoření kontrolního nástroje, který byl nazván Configuration Management.

NRC požadovala od společnosti Northeast Nuclear Energy, majiteli a držiteli licence pro JE Millstone před opětovným spuštěním bloků, nezávislou verifikaci plnění požadavků na zavedení vhodného systému řízení dokumentace a popsání „design bases“ [7]. NRC byla znepokojena i chybami držitele licence při řízení provozu a postupů při řešení bezpečnostních problémů navrhovaných zaměstnanci a proto byl v roce 1996 vydán požadavek, aby držitel povolení zpracoval podrobný plán na prověrku stavu všech otázek spojených s bezpečností navrhovaných samotnými zaměstnanci.

Prvotním problémem JE Millstone byl úpadek kvalifikace a chyby vedoucích pracovníků od presidenta společnosti a generálního ředitele až po výkonné techniky. Efektivní nápravné akce byly přijímány s nechtí, sebehodnocení prováděno formálně dokonce i poté, kdy byly nedostatky popsány zvenčí a identifikovány dozorným orgánem. Podíl na tom měla mimořádně špatná komunikace uvnitř organizace, která způsobila ztrátu důvěry mezi vedoucími pracovníky, zaměstnanci a pracovníky dozoru [8].

Millstone nebyla první jadernou elektrárnou, odstavenou z důvodů prohřešků proti bezpečnosti při řízení provozu. V roce 1987 vydala NRC příkaz k odstavení elektrárny Peach Bottom Atomic Power, kde operátoři spali, nevěnovali se svým povinnostem, nedodržovali předpisy, a vedení situaci přehlíželo, nebo přijímalo nedostatečná opatření. V sebehodnocení [9] pak sami došli k závěru, že provinění se proti některým kulturním návykům, které jsou podmínkou dobré úrovně provozu, vedly oprávněně k zákazu provozování.

V polovině osmdesátých let rozhodla Tennessee Valley Authority (TVA) odstavit jejich 5 reaktorů poté, když se zvýšil počet problémů souvisejících s bezpečností a které rovněž vedly k nízkému ratingu hodnocení provozu ze strany NRC. Ve zprávě, kterou vydala poradní komise [10] však bylo uvedeno, že ani TVA, ani NRC z počátku nerozpoznaly závažnost problémů TVA. Problémy managementu TVA byly označeny jako „hluboce zakořeněné“ ve své „zvláštní formě řízení“ a „zesílené podnikovou volností při uplatňování zodpovědnosti i škodlivých následků stropů federálních platů“.

Na schůzi v roce 1994 diskutovala NRC se svou poradní Komisí i nevěrohodné způsoby provádění sebehodnocení elektrárenských společností. Zvláštním diskutovaným případem byla elektrárna Cooper Nuclear Power Station. Tato elektrárna se silně odchýlila od klasických požadavků na respekt k jaderné bezpečnosti při řízení. Během diskuse mezi Komisí a pracovníky NRC byl předložen důkaz, že některé problémy elektrárny se vyvíjely po léta, ukazatele, registrující degradaci nebyly brány dostatečně vážně a včas, aby bylo možné problémům čelit. I zde byl zaznamenán „klasický scénář“ elektráren, které zahájily provoz velmi dobře, ale po nějaké době začaly selhávat [viz též 11]. Tato degradace probíhala po dlouhou dobu před tím, než dozorný orgán začal věnovat elektrárně pozornost a žádal rozsáhlá opatření, která měla vést k nápravě. Nebylo to jednoduché. Přístup elektrárny probíhal v několika stádiích:

- * období zapírání, nebo dokonce arogance, kdy byl provozovatel přesvědčen, že problém neexistuje a dozorný orgán se mýlí,
- * zjištění, že problém existuje a musí být seriosně projednán a
- * složitý proces nápravy, kdy se provozovatel snaží dostat z problémů

Z různých případů se zdá, že „ fáze zapírání“ má řadu forem. U OHN to byl nedostatek prozíravosti a základních znalostí řídicích pracovníků na úrovni hlavní správy, kteří problém ani nechápali, takže se divili výhradám. (Dvě nezávislé analýzy provedené počátkem devadesátých let v OHN zjistily řadu závažných nedostatků, ale vedly jen k málo efektivním nápravným akcím. V případě Millstone, dozorný orgán ze zprávy „Millstone Independent Review Group Regarding Millstone Station and NRC Handling of Employee Concerns and Allegations“ zjistil, že existuje „nezdravá pracovní atmosféra“, netolerující nekonformní názory a považuje diskusi o provozně-bezpečnostních otázkách „za nevíтанou“ [7], což je velmi eufemistické vyjádření stavu.

Tyto případy by měly varovat vedení elektrárenských společností a přesvědčit je o potřebě vidět bezpečnost při řízení jako součást vyvážených potřeb provozu spolu s technikou, ekonomikou a lidským faktorem.

V souvislosti s nehodou na jednom z bloků bylo ve Švédsku odstaveno v roce 1992 pět reaktorů kvůli nedostatkům zjištěným v dokumentaci “design basis”. Během odstávky 1. bloku Oskarshamn proběhla na reaktoru rozsáhlá inspekce. Na několika místech byly zjištěny vady, takže nakonec bylo rozhodnuto obnovit veškeré vnitřní části reaktoru. Následně byly zjištěny slabiny projektu a řízení jakosti, které způsobily odklad znovuvvedení bloků do provozu o dva roky. Žádost na znovuvvedení do provozu měla v příloze zprávu o události s titulem: “Odchyłky od oznámené úrovně bezpečnosti” Touto zprávou podepřel provozovatel požadavek, aby dozorný orgán souhlasil s obnovením provozu. Jednotlivé nedostatky nebyly neobvyklé, ale v sumě tvořily tolik odchylek, že stály za pozornost. Elektrárna předložila dvě zprávy o opatřeních na zlepšení: jednu o technických zlepšeních a druhou o zlepšení organizace a řízení [12, 13]. Dozorný orgán vzal na vědomí, že elektrárna je schopna vnitřní analýzy a popisu vztahů mezi potřebami řízení a techniky [14]. Švédský jaderný dozor (SKI) už delší dobu zdůrazňoval lidské aspekty, zejména vliv řízení. SKI sledoval rozbor poruch s hlediska vzájemného ovlivňování Personálu, Techniky a Organizace (hlediska PTO), což mu umožnilo požadovat od vedení elektráren nápravy příčin opakovaných problémů spojených s lidským faktorem.

V elektrárně Barsebäck Kraft AB (BKAB), dozorný orgán vyhodnotil opakované události spojené s PTO v letech 1990 až 1993. Vyhodnocení bylo ukázáno elektrárně s požadavkem na okamžitá nápravná opatření. Elektrárna připustila, že efekty týkající se lidských vlivů nebyly dostatečně analyzovány. Dozorný orgán (SKI) pak měl elektrárnu pod “zvláštním dohledem” a veškeré úsilí na zlepšení pečlivě “monitoroval” [15] až do roku 1997. SKI nebyl v tomto případě schopen předejít změnám organizace, které nebyly dostatečně předem dost analyzovány, ale měl alespoň schopnost požadovat následná nápravná opatření a dohlédnout na jejich realizaci.

Společným problémem dozorných orgánů v jednotlivých zemích je najít kritéria, podle nichž by bylo možné posoudit postupnou degradaci přístupu k bezpečnosti. Nelze se obejít bez hloubkových šetření na elektrárně. Dozorné orgány i elektrárenské společnosti se zpočátku soustřeďovaly na technické otázky, a události spojené s řízením a lidským faktorem přisuzovaly většinou různým jiným - technickým důvodům. Kromě Švédska bylo věnováno otázkám PTO v měnícím se společenském a ekonomickém prostředí jen nevelké úsilí dozorných orgánů. A navíc: dozorné orgány obecně nevěnují takovou pozornost organizačním změnám a jejich vlivu na bezpečnost, jako změnám technickým. Je to logické: posoudit technickou změnu je snazší. Avšak přísnější požadavky dozoru na předkládání analýz možných bezpečnostních následků organizačních změn a následovné pečlivé prověření těchto

změn dozorem mohou předejít některým problémům, které se u elektráren projevíly. Zkušenost Kanady a USA ukazuje, že dozorný orgán sice zjistil slabiny již během počáteční fáze organizačních změn, neměl ale schopnost efektivního vlivu požadovat zlepšení od vedení společnosti. Opakované změny organizace a přístupu k řízení, zavádění nových, často neúspěšných změn bez příslušných rozborů, byly dozornými orgány odsouhlasovány místo toho, aby byly podrobeny kritickému pohledu. V řadě případů dozor dostatečně neuplatnil “páky” na vrcholové vedení společností a spolupůsobil tak při zhoršování stavu.

Co je to vlastně provozní kultura jaderných zařízení?

Ve světě se v mnohých elektrárnách už kultura provozu (kultura bezpečnosti) stala součástí každodenního života, jinde si zatím hledá teprve cestu k pochopení.

Kultura provozu jaderných zařízení je souhrn chování zaměstnanců provozovatelské společnosti a stavu zařízení i všech podmínek pro jeho efektivní a bezpečný provoz. **Patří sem i celková pracovní atmosféra v elektrárenské společnosti.** Vedle společných ekonomických cílů je postavena na hlubokém poznání potřeb jaderné energie, na znalosti techniky, projektu a stavu zařízení, na uvědomování si úskalí při rozhodování. Je to i trvalé budování důvěry mezi vedením společnosti a zaměstnanci, podpora diskusím o bezpečnostních rizicích - a hlavně - uvažování o provozu z hlediska dlouhodobé perspektivy, neboť provoz jaderného bloku má převýšit několik generací. **Soustředění se pouze na krátkodobý ekonomický efekt je důkazem nevhodné kvalifikace vedoucích pracovníků.**

Vše záleží především na míře tohoto pochopení vedoucích osobností jednotlivých jaderných elektráren, protože kulturu bezpečnosti nelze v elektrárně navodit zdola.

Stav kultury provozu a bezpečnostní kultury lze formálně rozdělit do tří stupňů, z nichž každý představuje různé povědomí vlivů lidského chování a přístupů na bezpečnost. Každá elektrárna by měla mít snahu sama si odpovědět na otázku, kam patří, aby zjistila své slabiny a mohla je odstranit.

Stav 1. Bezpečnost založená pouze na Pravidlech a Směrnících

V tomto stavu vidí organizace bezpečnost jako vnější požadavek a nikoli jako hledisko, jehož plnění pomáhá k úspěchu. Bezpečnost je viděna většinou jako technická záležitost, pouhé

plnění směrnic a pravidel je považováno za dostatečné. U elektrárny, spoléhající se přednostně na pravidla lze pozorovat následující rysy :

- Problémy nejsou předvídány, organizace reaguje na každý případ tak, jak přijde;
- Komunikace a spolupráce mezi útvary a specialisty je slabá;
- Útvary a specialisté se chovají jako poloautonomní jednotky a existuje malá snaha o společně dosažené rozhodování;
- Rozhodování útvarů a specialistů se soustřeďuje na potřebu vyhovění pravidlům;
- Pracovníci, kteří udělají chybu jsou jednoduše obviněni z porušení předpisů;
- Konflikty nejsou řešeny, útvary a specialisté mezi sebou „bojují“;
- Role managementu je vnímána jako vydávání pravidel, vytváření tlaku na zaměstnance a očekávání výsledků;
- Neexistuje naslouchání, nebo poučení se uvnitř nebo vně organizace, které by vedlo k osvojení si zdrženlivých postojů při kritice;
- Bezpečnost je viděna jako vyžadovaná otrava;
- Státní dozorné orgány, zákazníci, dodavatelé a smluvní partneři jsou považováni za protivníky, s nimiž je nutné jednat obezřetně;
- Krátkodobá výhoda (obvykle zisk) je brána za důležitou;
- Pracovníci jsou vnímáni jako část zařízení – jsou popisováni a hodnoceni pouze podle toho, co dělají;
- Existují obezřetné vztahy mezi managementem a zaměstnanci;
- Existuje malé povědomí o potřebách průběhu práce;
- Pracovníci jsou odměňováni za poslušnost a výsledky bez ohledu na dlouhodobé následky.

Stav 2. Dobré bezpečnostní výsledky jsou cílem organizace

Organizace v tomto stádiu má vedení, které chápe otázky bezpečnosti jako důležité dokonce při absenci tlaku ze strany dozorných orgánů. Přestože vzrůstá vědomí o otázkách chování, chybí tento aspekt v řídicích metodách tvořících technická a procedurální řešení. O bezpečnostních výsledcích je jednáno stejně jako o jiných aspektech podnikání v termínech cílů a jejich plnění. Organizace začíná pozorovat důvody výsledků, tendence vývoje a cítí potřebu hledat inspiraci u jiných organizací.

- Elektrárna se soustřeďuje na denní úkoly, existuje jen minimum strategie;
- Vedení povzbuzuje přímou komunikaci mezi týmy a útvary;

- Vedoucí pracovníci jako tým začínají koordinovat rozhodování na úrovni útvarů a specialistů;
- Rozhodování se soustřeďuje často na náklady a funkceschopnost;
- Reakcí vedoucích na chyby je zavedení většího počtu kontrol, předpisů a přeškolování. Je zde méně obviňování;
- Konflikt je vnímán jako rušivý a je mu bráněno ve jménu týmové práce;
- Na roli vedení je pohlíženo jako na aplikaci technického vedení, vedení podle cílů;
- Organizace je ochotna učit se od jiných společností, zvláště v technických otázkách a dobré praxi;
- Na bezpečnost, náklady a produktivitu je nahlíženo odděleně;
- Vztahy organizace k dozorným orgánům, zákazníkům, dodavatelům a obchodním partnerům jsou spíše zdrženlivé, než těsné. Jde o opatrný přístup tam, kde by měla být pěstována důvěra;
- Je považováno za důležité dosáhnout, nebo překonat krátkodobé úkoly spojené se ziskem. Pracovníci jsou odměňováni za překročení zadání bez ohledu na dlouhodobé výsledky a následky;
- Vztahy mezi zaměstnanci a vedením jsou vztahy protivníků s malou důvěrou nebo malým projevem úcty;
- Existuje vzrůstající vědomí vlivu otázek kultury na jednotlivých pracovních místech. Není ale pochopeno, proč dodatečné kontroly nepřinášejí požadované výsledky v otázkách bezpečnosti.

Stav 3. Bezpečnostní výsledky lze vždy zlepšit

Organizace ve stavu 3 si osvojila myšlenku trvalého zlepšování a aplikovala tuto koncepci i na zajišťování bezpečnosti. Úroveň chování a přístupu k úkolům je vysoká a přijímaná opatření směřují ke zlepšení chování zaměstnanců. Pokrok je uskutečňován krok za krokem a nikdy není přerušen. Organizace se ptá, jak by mohla pomoci jiným společnostem.

- Organizace se začíná chovat strategicky se soustředěním se na dlouhodobou perspektivu a vědomým jednáním v současnosti. Problémy jsou předvíhány a jejich případy projednávány dříve, než se přihodí;
- Pracovníci chápou potřebu spolupráce mezi útvary a specialisty. Mají v tom podporu vedení, uznání a prostředky, které pro takovou spolupráci potřebují;
- Pracovníci si uvědomují pracovní procesy a procesy v organizaci a pomáhají vedoucím je řídit;

- Rozhodování je činěno s plnou znalostí vlivu na bezpečnost;
- Neexistuje konflikt mezi bezpečnostními a výrobními úkoly, otázky bezpečnosti nejsou v kontradikci s výrobními cíli;
- Téměř každá chyba je vnímána jako proměnlivost pracovního procesu. Je důležitější pochopit co se stalo, než někoho obvinít. Takové pochopení je použito k úpravě postupů;
- Existence konfliktu je vnímána jako cesta k nalézání vzájemně výhodného řešení;
- Role vedení je spatřována ve vedení lidí k zlepšování provozních výsledků.
- Učení se od jiných vně i uvnitř organizace je ceněno. Je věnován čas na osvojení si takových znalostí, které ke zlepšení výsledků vedou,
- Je rozvíjena spolupráce mezi organizací, dozorem, dodavateli a zákazníky.
- Krátkodobé výsledky jsou měřeny a analyzovány tak, aby změny vedly ke zlepšování dlouhodobých výsledků.
- Pracovníci jsou respektováni a hodnoceni za své přispění k dosažení cílů. Organizace neoceňuje jen ty, kteří „vyrábí“, ale i ty, kteří poskytují podporu práci jiných. Lidé jsou hodnoceni též za zlepšování procesů stejně jako za výsledky.
- Vztah mezi vedením a zaměstnanci je dán vzájemnou úctou a podporou.
- Pracovníci jsou si vědomi vlivu kulturních hodnot a tato hlediska berou v úvahu při klíčových rozhodováních.

Že je stupeň 3 jen sen, který předpokládá ideální, takřka nereálné pracovníky? Je to asi trochu pravda, ale ten sen by měl být asymptotou, k níž bychom měli mít snahu se blížit.

POUČENÍ ZE SLABIN PŘI ŘÍZENÍ BEZPEČNOSTI A BEZPEČNOSTNÍ KULTURY

-

SPOLEČNÉ SYMPTOMY

- * Tlak vedení společnosti na vysokou výrobu, vysoký zisk a snižování nákladů za každou cenu (honba za krátkodobými ekonomickými efekty),
- * Výrobní společnost (i dozorný orgán) je soustředěna spíše na technické otázky, než na otázky související s organizací, řízením a lidmi
- * Trvalé (časté) změny organizace a vedení (módní heslo z pouček pro mladé manažery: „jedinou naší trvalou jistotou je změna“)
- * Nedostatek efektivního dohledu ze strany vedení společnosti

- * Organizační izolace (odloučení)
- * Opakování chyb

SPOLEČNÉ PŘÍČINY

- * Nedostatky ve vedení společnosti, nedostatečná prozíravost (rozhled, znalost a schopnost) řídit jedinečné vztahy mezi technikou, ekonomikou, lidskými otázkami a bezpečností v měnících se podmínkách
 - * Přehlížení „varovných signálů“
 - * Nedostatky kritérií pro včasné zásahy dozorných orgánů pro snížení následků zhoršování řízení v oblasti bezpečnosti
 - * Neschopnost některých dozorných orgánů působit na představitele výrobní organizace (až po představenstvo) pokud jsou shledány nedostatky řízení
 - * Nástup nedostatečně kvalifikovaných pracovníků na místa uvolněná po odchodu zkušených
1. Všechny události mají zřetelné kořeny v kultuře organizace
 2. Kořeny příčin vznikaly mnoho let před nehodami, či ztrátou licence a nebyly detekovány
 3. Některé dozorné orgány nevěnovaly v povolovacím řízení dostatek zájmu o oblast organizace a kultury bezpečnosti

Literatura

1. Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident. IAEA Safety Series No.75-INSAG-1, 1986.
2. Safety Culture. IAEA Safety Series NO.75-INSAG-4, 1991.
3. The Convention on Nuclear Safety, June 1994.
4. Kupcis, Alan, Presentation to EDF, January 1998
5. Report to Management IIPA/SSFI Evaluation Findings and Recommendations. Prepared for A.Kupcis and C.Andoginini, July 1997.
6. Shutdown of Ontario Hydro Reactors: The Regulatory Perspective. AECSB, August 1997.
7. NRC Order requiring independent third-party oversight of Northeast Nuclear Energy Company's implementation of resolution of the Millstone Station employee's safety concerns issues. October 24, 1996. Docket Nos. 50-245, 336, 423.
8. NRC, Selected issues related to recovery of Millstone Nuclear Power Station, Unit 3. SECY-98-090-APLA-98.
9. Peach Bottom Commitment to Excellence Plan, Appendix A: Problem Root Cause Assessment of Peach Bottom Shutdown. Report prepared for Philadelphia Electric Company by Management Analysis Company (MAC), June 1987.
10. Report of the Advisory Committee on the Tennessee Valley Authority to the Southern

States Energy Board, 1987.

11. Murley, T. 'Early signs of deteriorating Safety Performance'. Report prepared for Committee on Nuclear Regulatory Activities, OECD/NEA, December 1997

12. O1- Säkerhetsredovisning inför ?terstart 1995, Ärende 1-95.073.

13. O1- Beskrivning av organization och kompetenssituation, 95-08493.

14. SKI Gransknings-PM, Ref.nr. 8.11-950988.

15. Särskild Tillsyn av BKAB - Verksamhetsinriktad Inspektion. Beslut 1997-02-05, Ref.No. 6.04-960832.

16. INSAG draft ' Safety management' by Dr. R.H. Taylor, April 1998

17. Kultura bezpečnosti souvisí s hospodárností (F.Hezoucký, příspěvek na konferenci pořádané k dvacátému výročí spuštění 1. bloku JE Dukovany, Třebíč 2005 a na konferenci v Bratislavě)

18. The Millstone story (presentation on the IAEA workshop in Richmond, June 2006)

Analýza pojmu RESILIENCE v různých vědních oblastech

Resilience začala být skloňovaným pojmem kolem 16. - 17. století především v průmyslu, jako vlastnost materiálu ([Dictionary, 2016](#)). Naznačuje schopnost a ochotu se přizpůsobit v reálném čase novým hrozbám. První zmínky o resilienci byly v souvislosti s pružností, vzhledem k zemětřesení, tedy jaký materiál je vhodný k postavení odolné budovy. ***Obecně můžeme resilience považovat jako schopnost systému absorbovat rušení, a ještě udržet jeho základní funkci a strukturu.***

Resilience je v současné době velmi diskutovaným tématem, existuje mnoho definic, mnoho přístupů k určování a současně také vědní disciplíny, které se resilienci zabývají, se snaží ji implementovat do svých oborů.

Z pohledu literatury se dá rozčlenit do tří základních oblastí a jejich podoblastí, které jsou nejčastěji uváděny v literatuře, a jsou zmíněny níže ([Birkie,2014](#); [Eid, 2015](#); [Fekete, 2011](#), [Gross, 2015](#), [Ouyang, 2012](#)):

1. **Resilience v psychologii** - mentální schopnost rychle zotavit se z deprese, onemocnění nebo neštěstí (např. po autonehodě)
2. **Resilience struktur** (technická resilience, biomateriál, např. v inženýrství ...) - v oblasti inženýrství to znamená fyzikální vlastnost materiálu, kdy může obnovit svůj tvar po natažení nebo deformování (elasticita)
3. **Resilience systému** (socio-ekologická, biologická, kritická infrastruktura) - schopnost systému zotavit se z katastrofálního selhání, biologové a geografové zkoumají vztahy mezi člověkem a prostředím, aby lépe porozuměli vývoji organismů a populace v závislosti na vývoji prostředí.

add 3) **Ekologická resilience** - je chápána jako rychlost, při které se systém vrátí do ustáleného stavu po negativní události. Ekosystémy se stále vyvíjí, jsou dynamické a vyvíjí se v reakci na vnější prostředí, které se dějí v průběhu času.

add 3) **Sociálně – ekologická resilience** – se skládá z bio-geo-fyzikálních jednotek a jejich přidružených sociálních subjektů a institucí. Sociálně – ekologické systémy jsou složité a adaptivní systémy, jak uvádí např. [Holling](#). Existuje několik definic tohoto systému, např. tento systém je soubor kritických zdrojů (přírodních, socioekonomických a kulturních), jejíž tok a využívání je regulováno pomocí ekologických a sociálních systémů.

Berkes ([Berkes, 2003](#)) a kolegové rozlišili čtyři sady prvků, které mohou být použity k popisu socio - ekologického systému:

- Ekosystémy
- Znalost místního prostředí
- Lidé a technologie
- Instituce a vlastnická práva

Pojem **odolnost** je slibným nástrojem pro analýzu adaptivní změny směrem k udržitelnosti, protože poskytuje způsob, jak analyzovat a manipulovat stabilitou tváří v tvář změnám. Co se týče adaptivního cyklu, ten interpretuje dynamiku složitých ekosystémů v reakci na narušení a změnu. Adaptivní cyklus je jedním z pěti heuristik používaných k pochopení sociálně-ekologického chování systému. Další čtyři heuristiky jsou: odolnost, panarchy, transformabilita a přizpůsobivost. ([Berkes, 2003](#))

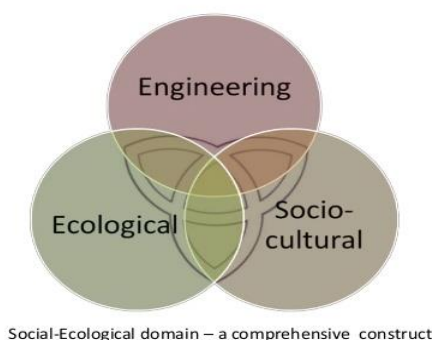
add 3) **Ekonomická (hospodářská) resilience** – ekonomická resilience je schopnost místního hospodářství zachovat funkce, zaměstnanosti a prosperity v zrcadle rozrušení způsobené šokem ztráty určitého druhu místního průmyslu nebo zaměstnavatele.

add 3) **Resilience kritické infrastruktury** (např. ICT) - resilience je schopnost sítě poskytovat a udržovat přijatelnou úroveň služby tváří v tvář různým poruchám a snaží se dosáhnout normálního provozu po mimořádné události.

add 3) **Resilience průmyslová a bezpečnost organizace** – odolnost strojírenství hledá způsoby, jak posílit schopnost organizace vytvářet procesy, které jsou robustní a přitom pružné.

Průnik jednotlivých oblastí je patrný z obrázku 20, kdy lze pozorovat, že jednotlivé výše zmíněné oblasti se navzájem ovlivňují.

Social-Ecological System Resilience



Obrázek 20: Průnik jednotlivých oblastí (<http://www.slideshare.net/kgtidball/srijb-resilience-talk-share-version>)

První zmínky resilience byly v souvislosti s ekologickými a později sociálně ekologickými systémy, které jsou podrobně rozebrány níže. Z tohoto důvodu se další část zabývá zejména sociálně – ekologickým systémem, protože poskytuje potřebné znalosti ohledně pochopení resilience a její výstupy mohou sloužit k ucelenému pohledu na problematiku resilience, kterou lze aplikovat na ostatní systémy. Nicméně princip resilience je stejný, ať jej používáme v jakémkoliv oboru.

Ekologický a sociálně-ekologický systém

Prvním, kdo zmínil resilienci a její potřebu v souvislosti s ekologickým systémem byl ekolog C. S. Holling v roce 1973, a po té následovaly další literatury. Později se začalo používat spojení **socio - ekologický systém**.

Holling ve své knize *Odolnost a stabilita ekologických systémů* prozkoumává ekologickou teorii a chování přírodních systémů, které mohou vést k užitečným postřehům pro praxi v sociálním systému. V práci uvádí celou řadu příkladů chování ekologických systémů, které je možno aplikovat na sociální systém, který je dále propojen s dalšími systémy. Je zde rozebrána stabilita a nestabilita ekologického systému, například u predátora a kořisti čím je způsobena a aplikovatelnost na reálné systémy.

Odolnost systému zde demonstruje na příkladu špatné rybolovné činnosti. Kdy se na jezeře Michigan lovalo několik tun pstruhů ročně, po několik let úlovky výrazně stoupaly a poté se rybolov zhroutil z důvodu úplného selhání přirozené reprodukce. Jedním z důvodů byla *Mořská mihule*, která se rozšířila do jezer po vybudování Wellandského kanálu. Rybolov pokračoval dál, ačkoliv pstruzi se nestihli reprodukovat a lovíli se čím dál mladší populace pstruhů, přispělo ještě k rychlejšímu úpadku rybolovu. Předpokladem tedy pro zhroucení rybolovu bylo nevhodné nastavení sklizně ryb, ačkoliv dlouhou dobu nebyly vidět příznaky. Holling došel k závěru, že rybolovné činnosti postupně snižují resilienci systému ve vodě, takže dochází k vyhnutelné situaci a to zhroucení populace určitého druhu, kdy na to navazuje zhroucení dalších druhů.

Z výše uvedených příkladů, kterých je v práci uvedena celá řada Holling rozlišuje dva typy chování. První typ nazývá **stabilita**, která představuje schopnost systému k návratu do rovnovážného stavu po dočasném narušení, čím rychleji se vrací, tím méně kolísá, a proto je více stabilní. Další typ označuje za **resilienci**, která je měřítkem přetrvávání systému a jeho schopnost absorbovat změny a rušení a stále se udržuje ve stejném stavu se stejnými vztahy mezi populacemi.

Holling ve své knize tvrdí, že chování ekosystému je ovlivněno náhodnými událostmi, které potvrzují tzv. existenci domén přitažlivosti. Vyplývá zde důležitý fakt a to, že **nestabilita** ve smyslu výrazného kolísání, může vést k **resilienci** a schopnosti přetrvávat. A právě Holling poukazuje na zcela odlišný pohled na svět, pokud se soustředíme na doménu přitažlivosti, spíše než na rovnovážný stav.

V rámci této práce v souvislosti s ekologickým systémem Holling navrhl výše zmíněné dvě odlišné vlastnosti, které tento systém definují. **Resilience** podle něj určuje přetrvání vztahu v rámci systému a je to míra schopnosti těchto systémů absorbovat změny stavových proměnných a dalších a stále přetrvávají. V této definici je **odolnost**

vlastnost systému a přetrvání nebo pravděpodobnost zániku může být výsledek. **Stabilita** je na druhé straně schopnost systému návratu do rovnovážného stavu po dočasné poruše.

Tyto definice mají myšlenku, že systém může být **resilientní** a stále značně kolísat, tedy má **nízkou stabilitu**. Pohled na resilienci a stabilitu chování ekologických systémů, může přinést velmi odlišné přístupy k řízení zdrojů ve světě. Pohled stability zdůrazňuje rovnováhu, zachování předvídatelného světa, nadměrnou produkci ze strany přírody a s co nejmenším kolísáním systému. Pohled resilience zdůrazňuje doménu přitažlivosti a potřebu vytrvalosti. Z toho vyplývá, že zde není předpoklad dostatečné znalosti, ale uznání nevědosti. Nepředpokládá se, že budoucí události budou očekávány, ale že budou neočekávané. **Rámec odolnosti** tento pohled bere v potaz, neboť nevyžaduje přesnou předpověď budoucnosti, ale kapacitu vymyslet systémy, které jsou schopné absorbovat a přizpůsobit se budoucím událostem v jakékoliv neočekávané formě.

Článek (Holling, 2001) z roku 2001 usiluje o pochopení složitosti ekonomického, ekologického a sociálního systému. Uvádí, že hierarchie a adaptivní cykly jsou čtyři. Adaptivní systém se dokáže proměnit, ačkoliv jeho podstata zůstane zachována a dokáže se učit ze zkušeností, tvoří základ ekosystému a sociálně-ekologických systémů. Dohromady tvoří **panarchy**. Tento pojem je užíván v souvislosti s těmito systémy velmi často a je chápán jako opak hierarchie, je to chápáno jako forma systému, která zahrnuje všechny ostatní. **Panarchy** je termín používán k popisu konceptu, který vysvětluje vyvíjející se povahy komplexních adaptivních systémů. **Panarchy** je struktura, v níž přírodní systémy a lidé, stejně jako v kombinaci člověk - příroda a sociálně ekologické systémy jsou vzájemně propojeny v nekončícím adaptivním cyklu, restrukturalizace a obnovy.

Adaptivní cyklus má tři vlastnosti, které tento cyklus utváří:

- Vlastní potenciál systému, který je schopný změny, jeho potenciál možné budoucí změny, známo taky jako „bohatství“ systému
- Vnitřní řiditelnost systému: to znamená míra propojenosti mezi interním ovládáním procesů a flexibilita
- Adaptivní kapacita: to znamená resilience systému, míra náchylnosti k neočekávaným nebo nepředvídatelným šokům.

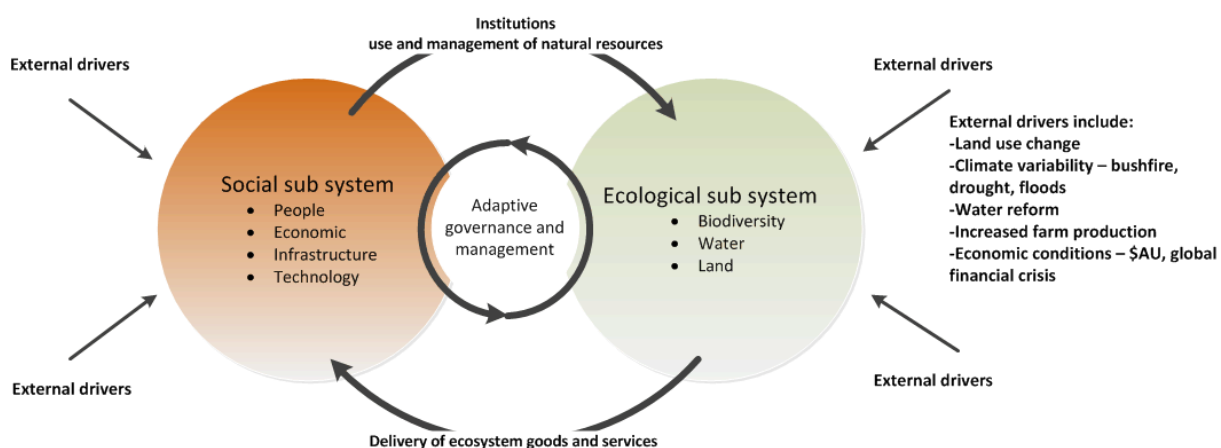
Z výše uvedených prací jasně vyplývá, že ekologický systém a sociální systém jsou navzájem závislé a ovlivňují se. Historie vztahů mezi ekologickými a společenskými

vědami sahá až do 17. století, kdy bylo oddělení těchto dvou věd základním principem *Západní akademické organizace*. Mnoho nedávných studií ekosystémů a společnosti ukázal, že existují vzájemné interakce mezi lidmi, biologickou rozmanitostí a ekosystémem a že jsou tyto systémy komplexní a souhrnně se nazývající **sociálně - ekologický systém**.

Právě tady vyvstává **potřeba sociálně - ekologické resilience**, kterou první zmiňoval Holling.

Holling ve svých pozdějších pracích zdůrazňuje, že základní charakteristika moderní koncepce resilience je multi-stabilní stav nelineární formy reakce, která vytváří více rovnováhy. Takto **multi-stabilní stav**, nebo lépe nazváno **režim**, představuje základní pochopení rovnováhy jako stav dynamické stability a řešení dynamiky sociálně ekologických systémů. Socio-ekologická **odolnost** je definována jako schopnost systému absorbovat poruchy a reorganizovat se, zatímco podstoupí změnu tak, aby i nadále udržel v podstatě stejnou funkci, strukturu, identitu a zpětné vazby (Walker et al., 2004).

Primární myšlenka adaptačního cyklu přichází opět z ekologie (Holling, 2001), která říká, že adaptace je založena na reorganizaci, kolapsu a obnově systému a na komponentech. Na obrázku 21 je zobrazen model sociálního systému a ekologického systému.



Obrázek 21: Model sociálně - ekologického systému

<http://weconnect.gbcma.vic.gov.au/node/138/revisions/1962/view>

Výzkumné projekty nebo centra RESILIENCE v jednotlivých oblastech

Po stručném vymezení základních oblastí a podoblastí resilience jsou níže uvedeny příklady jednotlivých organizací, které se zabývají resiliencí ve svém oboru a to resilience v psychologii, socio-ekologii a inženýrství.

Psychologie

[A simulation to teach about cumulative risk and resilience in adolescent development](#)

– Tato publikace se zabývá dospíváním dětí, jaký je průběh jejich života, úspěchy, vzdělání, přátelství a další aspekty života. Těžiště knihy spočívá v hledání rizik v tomto období dospívání a hledání pomoci. (<http://www.wright-house.com/psychology/risk/Introduction.html>)

[The Resiliency Center](#) - internetová americká stránka zaměřující se na reálné životní situace a jak resilience může mít vliv na individuální rozvoj a dává doporučení. Zaměřuje se na lidskou resilienci po celém světě, která vede ke zvládnutí uměn v současném světě. (<http://resiliencycenter.com/>)

[Resilience Research Centre in Canada \(Dalhousie University\)](#) - toto centrum vytváří různé projekty směřované na resilienci dětí s důrazem na rizika, kterým čelí děti v současné době. To znamená, jak jsou děti schopny se orientovat v současných službách, jako je například soudnictví, duševní zdraví, vzdělávání atd. Jsou zde zkoumány aspekty resilience mládeže napříč různými kulturami počínaje tímto výzkumem v Kanadě, kdy dalšími partnery je Nový Zéland, Jižní Afrika, Kolumbie a Čína. (<http://www.resilienceresearch.org/>)

[National Resilience Resource Centre LCC](#)- centrum, které se zabývá psychickou odolností dětí ve škole. (<http://www.nationalresilienceresource.com/Research.html>)

Ekologie

[The Resilience Alliance](#) - výzkumná síť, která se zaměřuje na sociálně-ekologickou resilienci. Byla založena v roce 1999. Resilience Alliance je mezinárodní

multidisciplinární výzkumný ústav, který zkoumá dynamiku sociálně-ekologických systémů. Členové RA spolupracují napříč obory s cílem správného chápání a aplikování resilience, schopnosti adaptace a transformace společnosti a ekosystému s cílem vyrovnat se se změnami a podporovat lidskou pohodu. (<http://www.resalliance.org/>)

Stockholm Resilience Centre - tento program nabízí PhD kurzy, semináře a workshopů pro zdokonalení znalostí studentů v socio-ekologických systémech. Jeden z výzkumů je také zaměřen na městské sociálně ekonomické systémy. Výzkum se snaží být součástí vytváření lepšího pochopení výzev, kterým města čelí a vytvářet řešení. (<http://www.stockholmresilience.org/education.html>)

Inženýrství

Centre for research on Risks and Crises - centrum výzkumu rizik a krizí, je otevřenou organizací lidí a míst, která se zaměřuje na bezpečnost ve složitých systémech. Centrum vzniklo v roce 2008, jedná se o interdisciplinární laboratoře, které jsou součástí Mines ParisTech (francouzská škola) a ARMINES (soukromá nezisková výzkumná a technologická organizace pod záštitou francouzského ministerstva). S dalšími výzkumnými středisky se věnují sociologii, ekonomice a průmyslu. Výzkum CRC leží na křižovatce mezilidských, společenských a technických věd. Práce v centru, která se zabývá modelováním a strojírenstvím, si klade za cíl formalizovat a sjednotit znalosti s cílem umožnit jednotlivcům, organizacím (zejména podnikům) a správním orgánům, omezit jejich zranitelnost a zvýšit jejich resilienci tváří v tvář mimořádně znepokojujícím nebo škodlivým událostem (časté technické katastrofy, pracovní úrazy a nemoci, přírodní a ekologické nebezpečí, škodlivé činy, terorismus, rizikové vztahující se k projektu, operační riziko, atd.) (<http://www.resilience-engineering.org/>)

100 Resilient Cities - tento projekt sponzorovaný Rockefellerovou nadací se zaměřuje na pomoc městům po celém světě, být více resilientní a čelit novým výzvám a rizikům jak psychickým, sociálním tak ekonomickým a technickým, které jsou specifické pro jejich území. Pro uvedení příkladu měst zahrnutých do projektu Amman, Athény, Bangkok, Cali, Chicago a další (<http://www.unisdr.org/campaign/resilientcities/home/toolkitblkitem/?id=4>).

UNISDR (The United Nations Office for Disaster Risk Reduction)- důvodem proč se tolik organizací a center po celém světě zabývá resiliencí, je zvyšování expozice osob, majetku a životního prostředí podstatně rychleji než se snižuje jejich zranitelnost, čímž se vytváří nové riziko a narůstají ztráty. UNISDR je organizace, která vznikla v roce 1999 jako specializovaný sekretariát s cílem usnadnit provádění mezinárodní strategie pro omezování katastrof. V rámci UNISDR existuje několik rámců pro snižování rizik a katastrof pro budování resilience komunit vůči katastrofám. ([UNISDR, 2016](#))

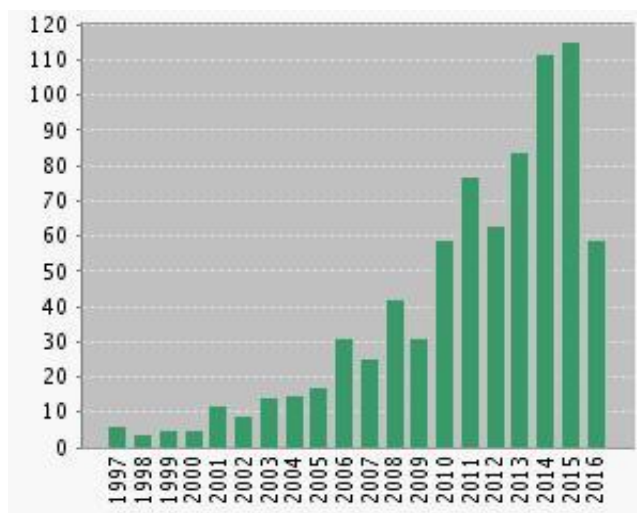
CEE V ILLINOIS Oddělení občanských a environmentální techniky - Program týkající se resilience, který byl zahájen na podzim roku 2011, se zabývá rozvíjením přístupů k systému infrastruktury se zaměřením na resilienci a udržitelnost na příklad: strukturální, geotechnickou a vodní interakci v městském prostředí. Program si klade za cíl připravit nové generace stavebních inženýrů, kteří jsou připraveni k řešení naléhavých společenských problémů a zároveň rozvíjet potřebnou infrastrukturu.

(<http://cee.illinois.edu/areas/sustainable-and-resilient-infrastructure-systems-program#brief2>)

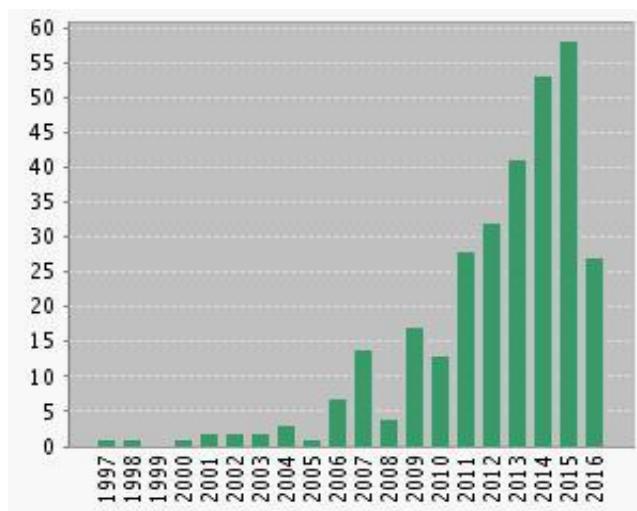
Počet výskytu pojmu RESILIENCE v jednotlivých oblastech

Publikace na Web of Science za posledních 20 let, ve kterých je využíván pojem resilience v jednotlivých oblastech.

- resilience v psychologii
- socio - ekologické systémy
- resilience v technické oblasti: kritická infrastruktura



Obrázek 22: Publikování resilience v oblasti psychologie



Obrázek 23: Publikace v socio-ekologické oblasti