Manažérstvo životného prostredia 2013 ♦ Management of Environment´2013
Zborník z XIII. medzinárodnej vedeckej konferencie, 18. - 19. apríl 2013, Bratislava
Proceedings of the 13rd International Conference, Bratislava, April 18-19, 2013
■ Žilina: Strix. Edícia ESE-14, 1. vyd., ISBN 978-80-89281-90-9 ■ Rusko, M. [Ed.] ■

PŘÍČINY NEHOD A HAVÁRIÍ A ZPŮSOBY ŘÍZENÍ BEZPEČNOSTI TECHNOLOGICKÝCH SYSTÉMŮ S OHLEDEM NA DOPADY HAVÁRIÍ

Dana PROCHÁZKOVÁ

THE CAUSES OF ACCIDENTS AND CRASHES AND THE METHODS OF MANAGEMENT OF SAFETY OF TECHNOLOGY SYSTEMS WITH RESPECT ON THE CRASHES IMPACTS

ABSTRAKT
ČLÁNEK ANALYZUJE POZNATKY O NEHODÁCH SKORONEHODÁCH A HAVÁRIÍCH, UKAZUJE JEJICH PŘÍČINY ZÁKLADNÍ I MNOHONÁSOBNÉ, KTERÉ MAJÍ PŮVOD V TECHNOLOGIÍCH, V LIDSKÉM FAKTORU A TÉŽ V NEPOZNANÝCH NEURČITOSTECH V CHOVÁNÍ SLOŽITÝCH SYSTÉMŮ. Z DŮVODU OCHRANY LIDÍ, MAJETKU A ŽIVOTNÍHO PROSTŘEDÍ SE ZABÝVÁ ŘÍZENÍM BEZPEČNOSTI TECHNOLOGICKÝCH SYSTÉMŮ A DOPORUČUJE, ABY DO PRAXE BYL ZAVEDEN SYSTÉM ŘÍZENÍ BEZPEČNOSTI, VE KTERÉM JSOU VČLENĚNA PREVENTIVNÍ, ZMÍRŇUJÍCÍ, REAKTIVNÍ I OBNOVOVACÍ OPATŘENÍ A ČINNOSTI S OHLEDEM NA DOPADY MOŽNÝCH HAVÁRIÍ.

***Klíčová slova**: bezpečí, bezpečnost, havárie, příčiny havárií, systém řízení bezpečnosti*

ABSTRACT
THE PAPER ANALYSES THE FINDINGS ON INCIDENTS, NEAR MISSES AND ACCIDENTS, IT SHOWS THEIR CAUSES, PRIMARY AND MULTIPLE, THAT HAVE GENESIS IN TECHNOLOGIES, HUMAN FACTOR AND ALSO IN UNKNOWN EPISTEMIC (KNOWLEDGE) UNCERTAINTIES IN BEHAVIOUR OF COMPLEX SYSTEMS. FROM THE VIEWPOINT OF PROTECTION OF HUMANS, PROPERTY AND ENVIRONMENT IT DEALS WITH MANAGEMENT OF SAFETY OF TECHNOLOGICAL SYSTEMS AND IT RECOMMEND TO INCLUDE INTO PRACTICE THE SAFETY MANAGEMENT SYSTEM IN WHICH THERE ARE INCORPORATED PREVENTIVE, MITIGATING, REACTIVE AND RENOVATING MEASURES AND ACTIVITIES WITH REGARD TO IMPACTS OF POSSIBLE ACCIDENTS.

***Key words:** security, safety, accidents, accident causes, safety management system*

Úvod

Před průmyslovou revolucí byly nehody, havárie a neštěstí výsledkem živelních pohrom nebo několika, relativně dobře známých, jednoduchých technologických zařízení (např. vysokotlaké parní kotle). V 20. století vědecký a technologický pokrok zredukoval nebo eliminoval mnohá z tehdejších rizik; byla zahájena systematická práce s riziky zacílená na řízení a vypořádání rizik pro specifikovaná aktiva. Na druhou stranu věda a technologie přinesla nová nebezpečí. Příkladem může být přítomnost nebezpečných chemických látek produkovaných antropogenními technologiemi v ovzduší nebo využívání radioaktivního záření, které zvýšilo potenciál pro úmrtí a choroby z ozáření.
Mnohá z nových nebezpečí jsou záludnější, hůře odhalitelná a eliminovatelná, než v minulosti. Navíc neexistuje žádná předchozí zkušenost, které by mohlo být využito při překonávání nových nebezpečí. Mnoho zkušeností a poučení z předcházejících havárií je uloženo v zákonech, normách a v postupech dobré praxe. Ale odpovídající zákony a normy pro mnohé z nových inženýrských odvětví a technologií ještě nejsou vypracované. Mnohokrát se poučení získané za celá staletí ztratí, když se starší technologie nahradí novějšími; například, když se mechanické zařízení nahradí digitálními počítači.
I když redundance (znásobení součástkových komponent pro ochranu před selháním obvodů měřící nebo regulační funkce - zálohování) poskytuje ochranu před haváriemi zapříčiněnými selháním individuálních částí, není stejně efektivní vůči nebezpečím, která vygenerují interakce mezi komponenty ve stále komplexnějších a vzájemně interagujících inženýrských systémech dneška. Redundance mohou ve skutečnosti zvýšit složitost až do takové míry, při které už ony samotné jsou přispívajícími faktory k haváriím.
Mnohá z nových nebezpečí jsou svázaná se zvětšující se složitostí systémů, které se dnes budují. Složitost nejen vytváří nová nebezpečí, ale dělá je i hůře odhalitelnými. Dalšími novými nebezpečími jsou již jen heslovitě např.:

- vzrůstající expozice nebezpečí,
- zvyšování kumulace energií a dosahů nebezpečí,
- zvyšování automatizace,
- narůstající centralizace a výrobní kapacita,
- nárůst tempa technologických změn.

Příčiny havárií

Pod pojmem havárie rozumíme pohromu, tj. škodlivý jev, který vyvolá technologický systém nebo jeho část. Označuje se jím poškození určitého zařízení nebo systému, které působí selhání jejich funkcí a má nepřijatelné dopady na aktiva v jejich okolí. Příčiny havárií jsou rozmanité a většinou jde o kombinaci několika příčin. Rozdělujeme je zpravidla na primární (počáteční, základní, zdrojové) příčiny (Root Causes) a mnohonásobné. Při vyšetřování havárií obvykle hledáme příčiny primární. Existují různé kategorie primárních příčin. V nich jsou určitá klíčová slova, která charakterizují určitou množinu jevů / stavů / provedení / atd., tzv. „před-podmínek“ pro selhání [1]. Je skutečností, že příčiny většiny havárií nejsou jednoduché, ale obvykle jde o souběh celé řady příčin a popřípadě náhodných kombinací příčin. Postup pro určení mnohonásobných příčin vychází z cíle vyšetřování nehody, kterým je zabránit opakování nehody tím, že:

- identifikují a ocení příčiny (primární příčiny a přispívající příčiny),
- identifikují a ocení doporučená preventivní opatření, která redukují pravděpodobnost vzniku nehod a / nebo dopady nehod,
- zajistí efektivní provádění sledování všech doporučených opatření.

Velmi často je hlavní nebo vedlejší příčinou havárie lidský faktor [2]; který působí ve dvou rolích, a to provedení nesprávného úkonu anebo nesprávná organizace práce, tzv. organizační havárie, přičemž dopady druhého uvedeného faktoru jsou zpravidla krutější.

Souhrn poznatků o výsledcích šetření havárií

Na základě údajů shromážděných v publikaci [1], které byly po doplnění použity pro zpracování dále uvedeného souhrnu, popisy příčin havárií často zahrnují subjektivitu a filtrování zjištěných informací. Pouze ojediněle jsou příčiny havárií vnímané identicky vedením společnosti, inženýry, představiteli odborů, operátory, zaměstnanci v pojišťovnách, soudci, policisty, novináři, státem a oběťmi. Ukazuje se, že každá specifikace možných příčin havárií nevyhnutelně nese znaky střetu zájmů.
Některé podmínky mohou být považované za nebezpečné jednou skupinou, přičemž druhá skupina je má za perfektně bezpečné a nevýznamné. Ke střetům dochází často v situacích, při kterých jsou potřebná normativní, etická a politická posouzení. Navíc, rozhodnutí o příčině nehody mohou být ovlivněná hrozbou možných soudních sporů.
Opravdu, každý dotazovaný člověk může přisoudit k dané havárii či nehodě různou příčinu. Jedna studie ukázala, že dělníci, kteří byli spokojeni se svou prací a byli včleněni do podnikání, přisuzovali událostem hlavně osobní příčiny. Naopak, pracovníci, kteří nebyli spokojení, měli na podnikání jen malý podíl, uváděli daleko častěji neosobní příčiny, které dokazovaly, že za události odpovídá podnik. Dalším faktorem subjektivity může být pracovní postavení v organizaci. Čím nižší je hierarchické postavení, tím větší je tendence svádět události na faktory spojené s organizací a naopak, jednotlivci, kteří mají vysoké postavení v hierarchii, mají tendenci obviňovat dělníky. Uvedená skutečnost odporuje údajům z hlášení o „skoronehodách“, která dokazují, že příčinami vzniklých událostí jsou v převážné míře technické a organizační závady (často mající kořen v rozhodnutích špičkových řídících pracovníků). Je tedy zřejmé, že určení příčiny závisí na určitých charakteristikách oběti a na analýze postavení oběti (hierarchické postavení, míra zainteresovanosti a spokojenost s prací) na vztazích mezi obětí a analytikem a na stupni závažností havárie.
Identifikování příčiny nehody a z ní vyvinuté havárie může být ovlivněno i metodami sběru dat. Většinou jsou údaje o haváriích shromažďované ve formě textových popisů časového průběhu události s tendencí soustřeďovat se na běžné okolnosti bezprostředních jevů (které časově těsně předcházely vzniklé události). Na jedné straně, formuláře pro zaznamenání jevů, které jsou předem připravené jen na bezprostředně související jevy, většinou ani neumožňují zaznamenat i jiné související jevy. Na druhé straně, podrobněji vymezené formuláře mohou omezit kategorie podmínek, které mají být zvažované při vyšetřování příčin události.

Dalším problémem při identifikování příčin havárií je nepřiměřené zjednodušování. Mnohokrát se při nehodách zdůrazní pouze některé faktory jako příčina přesto, že všechny zjištěné faktory byly stejně nevyhnutelné pro vznik události. Např. při smyku auta za deště může působit mnoho faktorů, jako např.: mokrá vozovka, nedostatek zkušenosti řidiče, nevybavení auta protismykovým brzdovým systémem a pod. Ani jeden z těchto faktorů není dostatečnou příčinou smyku, ale jakýkoliv z nich je často uváděný jako jediná příčina smyku. Určitá podmínka / faktor může být vybraná jako příčina čistě proto, že se naplnila jako poslední před vznikem události, nebo se zdá být nejnápadnější, nebo analytik má svůj vlastní motiv pro její výběr. Mnoho odborníků zastává názor, že přestože často izolujeme jednu podmínku a nazveme ji příčinou, přičemž ostatní podmínky považujeme za přispívající, nemá takové odlišování žádný všeobecný základ.
Přílišné zjednodušování příčinných faktorů u havárií může být obzvlášť škodlivé pro ochranu před haváriemi v budoucnosti.

Společným typem přílišného zjednodušování je úřední, formálně zákonný přístup, kterým se nehody připisují jen selháním člověka, nebo technickým chybám, přičemž se ignorují organizační faktory a hledají se jednoduché zjevné příčiny.
Právníci a pojišťovací agenti často příliš zjednodušují příčiny havárií a obyčejně identifikují bezprostřední, resp. přímou příčinu nehody. Je jim jasné, že se na havárii podílelo více faktorů, ale z praktických důvodů, obzvlášť pro určení viny a odpovědnosti za škodu, identifikují podstatný faktor jako příčinu. Jejich cílem je určit, která ze zúčastněných stran má ze zákona odpovědnost zaplatit škody. Uvedený způsob určování míry zavinění může být ovlivněn platební schopností zúčastněných stran nebo politickými úvahami.

Všeobecně neexistuje žádné objektivní kritérium pro upřednostnění jednoho faktoru před druhým, z množiny možných faktorů, které se podílely na havárii. Právnický přístup ke kauzalitě má výhodu jen pro určení viny a odpovědnosti. Pro technický pokrok, u kterého cílem je porozumět a zabránit havárii, má právnický přístup pouze malý užitek. Může být dokonce přímo škodlivý, protože většina relevantních faktorů z hlediska prevence budoucích havárii může být u něj zcela ignorovaná.
Opatření proti nehodám a haváriím, které se zavádějí do praxe, by neměla být určovaná podle relativního významu příčinných faktorů. Naopak, priorita by měla být dána opatřením, která budou co nejefektivněji redukovat ztráty. Zjednodušené vysvětlení nehod často neposkytuje nevyhnutelné informace pro zabránění dalším nehodám v budoucnosti a kromě důvodů souvisejících s odpovědností, je vynakládání času na určení relativních příspěvků jednotlivých faktorů k daným událostem neproduktivní.
Nejčastěji vyskytujícím přílišným zjednodušením je podle zpráv o nehodách svalení viny na člověka (operátora, pilota, řidiče, dělníka). V každém systému, do kterého je včleněný člověk, může být hypoteticky příčina nehody vždy přiřazená člověku, ať už za jeho zásahy, nebo za nedostatečnou prevenci havárií. I v těchto případech, když je chyba člověka bezprostředně spojená s nehodou, ***je chybou považovat člověka za jedinou příčinu nehody systému a snažit se ho proto v budoucnosti z něho vyloučit, protože to má jen omezený účinek pro identifikaci toho, co má být změněno, aby se efektivně zvýšila bezpečnost.***
Všeobecně se selhání člověka udává jako příčina nehody: „Vinen je lidský činitel“. Analytici často zastaví rozbory při chybě člověka a nevěnují náležitou pozornost jiným nevyhnutelným okolnostem, které musely spolupůsobit, aby k chybě člověka došlo.
Protože objektivně můžeme o každé havárii říci, že ji způsobila chyba člověka, je uvedená fráze demotivující pro konstruktivní přístup k akcím potřebným pro zabránění opakovaným selháním člověka. Je velmi jednoduché říci někomu: „Buď opatrnější.“ Asi bude vhodnější přestat se zjišťováním, jestli chyba člověka byla příčinou nehody a místo toho začít zkoumat a aplikovat prevenci proti selháním člověka.

Obdobně přílišným zjednodušováním je i zaměření jen na technické chyby a bezprostřední fyzikální jevy. Tento typ převládajícího úzkého zaměření může vést k přehlédnutí některých nejdůležitějších faktorů nehody.
Velké technologické provozy a technické systémy jsou víc než množinou technických částí zařízení a součástek. Jsou odrazem organizační struktury, managementu, provozních předpisů a kultury konstrukčních organizací, které je vytvořily a také jsou zpravidla i odrazem společnosti, ve které byly vytvořené (viz [3]). Nehody jsou často svalované na chyby operátorů nebo zařízení, bez rozlišení průmyslových, organizačních a manažerských faktorů, které způsobily, že se tyto chyby a nedostatky staly nevyhnutelnými. Příčiny havárií mají často, ne-li skoro vždy, kořeny v organizaci - v její kultuře, managementu a struktuře. Všechny zmíněné faktory jsou kritické pro bezpečnost technických systémů.
Významnou podporu hypotéze o převážném vlivu vyjmenovaných organizačních příčin na vznik havárií dává přehled výsledků zjištění ze závažných průmyslových havárií z posledního období. Hlubší, nezávislé rozbory havárií, jednoznačně zvýrazňují organizační a manažerské nedostatky. V uváděných příčinách je jen málo identifikovaných technických příčin, ale většinou se jedná o problémy řízení, výcviku a organizačních nedostatků.
Ve většině velkých havárií z posledních 25 let byly technické informace o potřebné prevenci havárií dopředu známé a často i implementované. Při každé havárii se však ukázalo, že technické informace a řešení nebyly využity v důsledku nedostatků v organizaci, a v jejím řízení [3].
Všeobecně je nepravděpodobné, že kterákoliv jednotlivá podmínka / faktor může být rozhodující, nebo dokonce postačující pro způsobení havárie složitého systému. Ve většině systémů, které byly konstruované s náležitou péčí o jejich bezpečnost, budou nehody a havárie nebo selhání záviset na mnohonásobnosti příčinných faktorů a na složitých kombinacích podmínek technických, personálních, organizačních a sociálních.
Vysoká četnost havárií, které měly komplexní příčiny, vyplývá pravděpodobně ze skutečnosti, že konkurenční organizační struktury a inženýring eliminují jednodušší příčiny. Pozitivní je, že obrovská složitost nehodových procesů znamená, že je možné najít mnoho příležitostí zasáhnout včas, nebo je eliminovat. Proto průřezové zvažování všech podmínek vedoucích k nehodám je mnohem užitečnější, než zjednodušující vysvětlení.

Poučení z nehod a havárií

Studiem nehod provozovatelé mohou omezit nebezpečné nebo neproduktivní pracovní praktiky, a tím zvýšit kulturu bezpečnosti práce. Pozitivní zpětnou vazbu na vznik nehod mohou mít i audity řízení, audity bezpečnosti, audity nebezpečných dějů, chemických reakcí, zprávy o nehodách a skoro nehodách, a monitoring dodržování všech opatření [1]. Existují 3 kategorie nebo „úrovně“ doporučení, a to:

- Bezprostřední technická doporučení.
- Doporučení pro zabránění nebezpečí.
- Doporučení pro řízení zaměřená na primární příčiny nehod.

Bezprostřední technická doporučení jsou zaměřená na zabránění určitým nehodám. Např. u odběru vzorků kapalného chlóru ve výrobně chlóru existuje určité nebezpečí úniku chlóru a následná inhalace plynného chlóru obsluhou při vzorkování chlóru. Příslušná doporučení jsou:

- změna techniky vzorkování,
- výcvik (trénink) správného odběru,
- použití ochranných pomůcek.

Doporučení pro zabránění (odvrácení) nebezpečí jsou zaměřená na odvrácení nepřijatelných nehod anebo alespoň jejich nepřijatelných dopadů. Např. se provede zlepšení běžných, oddělujících opatření umístěných mezi obsluhu a vlastní nebezpečí, tj. modifikace vzorkovací aparatury, vzorkováním v jiném místě nebo in-line analyzátorem, který odstraňuje potřebu ručního vzorkování.
Doporučení pro řízení zaměřené na primární příčiny nehody. Analýzou situace se identifikují nutné změny v systému řízení bezpečnosti, je-li ustaven anebo v jiných řídicích systémech. Úsilí je zaměřeno nejen na prevenci dané nehody, ale i na zabránění jiným podobným nehodám. Opatření takto koncipovaná jsou více důsledná a déle přetrvávající. V případě vzorkování chlóru to může být:

- Zlepšení v metodách odběru vzorků (Sofistikovaně se odpoví na otázky: Kdo se účastní rozhodování? Jaká jsou kritéria pro stanovení místa odběru? Jaké jsou metody odběru a přístrojové vybavení? Kdo je oprávněn k odběru? Existuje periodický audit?), a odpovědi se zavedou do praxe.
- Zlepšení v systému řízení pro zaváděcí, hodnotící a monitorovací standardní výrobní postupy (Jsou postupy adekvátní, srozumitelné a jsou důsledně prováděny? Je tento pracovní úkol stále nezbytný?), a odpovědi se zavedou do praxe.
- Zavedení rutinního postupu, jako je např. analýza bezpečnosti práce, kterou jsou úkoly systematicky posuzovány z hlediska potenciálního nebezpečí.

Poučení z havárií a skoronehod by měla být použita při zvažování technických a organizačně - řídících opatření. Profesor Kletz, který zkoumal havárie, poukazuje na problém udržování a využívání znalostí v rámci dané organizace. S postupem času a změnami personálu jsou původní opatření provedená po proběhlé havárii zapomenuta nebo nejsou předána všem pracovníkům v dané organizaci. Z těchto důvodů navrhuje následující opatření ke zlepšení společné paměti organizace:

- připojení poznámky ke každému pokynu, předpisu nebo normě, proč je právě takový,
- popis staré i nedávné havárie v podnikovém tisku s poučeními, která z nich vyplývají, a jejich projednání na školeních o bezpečnosti pro všechny složky podniku,
- pravidelná kontrola dodržování vydaných opatření,
- odstranění existujících zařízení teprve po poznání, proč bylo instalováno. Rušení původního postupu po zjištění, proč byl přijat. Je to nutné, aby se neodstranilo něco, co má zabránit havárii nebo má zmírnit její dopady,
- zavedení lepšího informačního systému pro nalezení podrobností o haváriích a vydaných doporučeních po havárii.

V praxi se používá také pojem „organizační havárie“. Při zkoumání zavádění směrnice Seveso I byly na základě analýzy závažných havárií, které byly nahlášeny od zavedení směrnice, identifikovány oblasti pro nová ustanovení v nové směrnici. Jednou z těchto oblastí jsou přístupy k řízení (koncepce řízení) a systémy řízení. Z analýzy vyplynulo, že ***selhání systému řízení přispělo k příčinám více než 85% nahlášených havárií.*** Proto ***omezování rizik v rámci řízení bezpečnosti pokrývá několik okruhů:***

- bezpečnost procesů,
- ochrana zdraví a bezpečnost zaměstnanců (bezpečnost práce) a omezování vlivů na životní prostředí.

Analýza dopadů řízení na bezpečnost podniku může vycházet z modelu organizační havárie. Organizační havárie [2] se skládá ze tří základních prvků:

- organizační procesy,
- podmínky, které působí vznik chyb nebo porušení předpisů,
- chyby a/nebo porušení předpisů.

Systém řízení bezpečnosti

Komplexní ochranu chráněných zájmů zajistí pouze sofistikované typy řízení, a to řízení rizika anebo vyšší typ řízení, tj. řízení bezpečnosti [4]. Účelem a cílem řízení rizik je jejich snížení na přijatelnou úroveň. Jakmile na základě stanovení ohrožení je nebezpečí jednou identifikováno, musí být nejvyšší prioritou jeho eliminace, anebo jeho spolehlivé řízení. Systém řízení bezpečnosti (ŠMS – Safety Management System - někdy též systémové řízení bezpečnosti nebo jen krátce systémová bezpečnost) má cíl zvyšovat bezpečnost a provádí to také na základě snižování rizik na úroveň přijatelného rizika. Má široko akceptované priority jak zvládnout nebezpečí, kterými jsou:

- Eliminovat zdroje nebezpečí.
- Redukovat (omezit) možné dopady, tj. možná nebezpečí pro chráněné zájmy / rizika.
- Zvládnout rizika.
- Lokalizovat a zmírňovat škody.

Uvedené priority neznamenají, že stačí, aby byla jen jedna z nich aplikovaná při projektu zaměřeném na zvyšování bezpečnosti, nebo že jen nejvyšší priorita je nejžádanější. Pokud není možné kompletně eliminovat zdroj rizika, je dalším nejlepším výběrem ochrana před dopady spojenými s realizací rizika (tj. zmírňování dopadů pomocí specifických opatření), a to minimalizováním vzniku realizace rizika tak, že se příslušná bezpečnostní ochranná opatření (bezpečnostní systémy – Safety Systems) přímo zabudují jak do projektu zařízení, tak i do podmínek provozu projektovaného zařízení, tj. zajišťují bezpečnost. Dalšími v akceptovatelném pořádku priorit jsou zařízení na zvládnutí nebezpečí a na zmírnění jejich dopadů (systémy spojené s bezpečností – Safety Related Systems), které mají jen ochranné funkce. Jsou to např. pojistné ventily,

které chrání před nedovoleným přetlakem v případech, ve kterých se nedovolenému zvýšenému tlaku v zařízení nedá úplně zabránit.
Bezpečnostní systémy jsou konstruované jako pasivní anebo aktivní. Nejefektivnějšími bezpečnostními zařízeními jsou zařízení pasivní, která fungují na bázi fyzikálních principů (např. gravitace) a pro uvedení do činnosti nepotřebují žádný přidaný impuls. Příkladem pasivního bezpečnostního systému je železniční semafor, jehož rameno automaticky spadne do polohy „stop“ vždy, když se přeruší ovládací proud v přívodním kabelu.
Aktivní bezpečnostní zařízení / systémy jsou méně vhodné, protože pro jejich aktivaci pro zabránění havárie anebo zmírnění jejich dopadů jsou potřebné zvláštní iniciační impulsy. Jejich vytvoření zahrnuje detekci nebezpečí a rozpoznání odpovídající bezpečnostní procedury. Příkladem aktivního bezpečnostního systému může být detektor kouře propojený se sprchovým systémem. Současné technické poznání dovoluje používat hybridní bezpečnostní systémy, které se samostatně vypínají, když podmínky nejsou v rozsahu podmínek stanovených pro provoz aktivních systémů.
Systém řízení bezpečnosti musí být vždy vybaven opatřeními pro minimalizování škod v případech, že bezpečnostní opatření a bezpečnostní systémy selžou, anebo se vyskytne neidentifikované nebezpečí. Minimalizování škod může mít podobu varovné a výstražné signalizace, výcviku, pokynů a procedur pro chování v nebezpečných situacích, anebo izolace nebezpečných zařízení od osídlených center. Opatření před nehodami včetně nouzového plánování musí být vypracováno ještě před tím, než bude zařízení spuštěno do provozu. Při vzniku havárie by už na to nemuselo být dosti času.
Správné porozumění určité problémové oblasti vyžaduje pochopení její historie, vědeckého základu, kulturního a sociálního prostředí, ve kterém byla vyvinutá a ve kterém se využívá. Systém řízení bezpečnosti má svoje kořeny v inženýrství průmyslové bezpečnosti, která se datuje už od 19. století. Relativně nová disciplína zabývající se systémem řízení bezpečnosti (v inženýrském slangu systémovou bezpečností) je odpovědí na podmínky, které vznikly po 2. světové válce, když se vyvinuly její “rodičovské“ disciplíny, a to systémové inženýrství a systémová analýza, které se vyvinuly pro řešení nových a komplexních inženýrských problémů. Vědecká báze všech těchto nových proudů inženýrství spočívá v teorii systémů, jejíž vývoj začal v třicátých letech minulého století.
Systém řízení bezpečnosti (SMS – Safety Management System) využívá teorii systémů a systémové inženýrství pro prevenci předvídatelných havárií a pro minimalizování dopadů nepředvídatelných havárií. Zajímá se všeobecně o ztráty a škody a ne jen o smrtelné úrazy, anebo o zranění, např. o poškození majetku, nesplnění poslání (mise, účelu), anebo škody na životním prostředí. Klíčovým bodem je považovat ztráty za dostatečně vážné na to, aby na jejich prevenci byl věnovaný dostatek času, úsilí a prostředků. Velikost investic věnovaných na předcházení haváriím, anebo jejich dopadům je vždy závislá na sociálních, politických a ekonomických faktorech.
Prvotním zájmem systému řízení bezpečnosti je řízení rizik, jehož úkoly, zásady a cíle jsou v práci [4]. V r. 1968 vzniká nová disciplína „inženýrství řízení bezpečnosti systému (systémová bezpečnost)“ jako „organizované veřejné mínění“. Jedná se o plánovaný, osvojený a systematický přístup k identifikování, analyzování a kontrolování rizik během celého životního cyklu systému za účelem snížení pravděpodobnosti výskytu nehod a minimalizace jejich dopadů.
Program na zvyšování bezpečnosti pomocí systému řízení bezpečnosti [5,6] musí zabezpečovat přesně stanovený postup metodické kontroly bezpečnostních aspektů a hodnotit projekt zařízení ve smyslu identifikování možných zdrojů rizik a předepsání časově i nákladně efektivních nápravných zásahů. ***Cíle programu systémové bezpečnosti mají zajistit následující***:

- bezpečnost zařízení, která odpovídá jeho poslání,
- identifikaci, vyhodnocení, eliminaci anebo kontrolu možných rizik na akceptovatelné úrovni u všech zařízení přidružených k systému, podsystému a k jednotlivým částem,
- řízení dopadů od ohrožení, která představují všechny možné pohromy, která nemohou být eliminována, musí být zajištěno tak, aby chránilo personál, zařízení a majetek,
- použití nových materiálů, anebo výrobků a testovacích technik musí být prováděno tak, aby to bylo spojené jenom s minimálním rizikem,
- nápravná opatření požadovaná pro zlepšení bezpečnosti jsou minimalizována dočasným včleněním bezpečnostních faktorů během vzniku systému,
- historické údaje o bezpečnosti generované podobnými programy bezpečnosti jsou brány v úvahu a používány všude tam, kde je to vhodné.

Průmyslová odvětví si buď adaptovala program na zvyšování bezpečnosti pomocí systému řízení bezpečnosti z vojenství anebo NASA, anebo samostatně vyvinula své vlastní programy podle zkušeností, které byly získány z výstavby elektráren, z výroby složitých nebezpečných a drahých zařízení. Čekání na výskyt havárií a následné eliminování příčin se stalo neekonomickým a někdy až neakceptovatelným způsobem úprav a zdokonalování systémů.
Budování mnohých dnešních komplexních systémů si vyžaduje integraci částí (podsystémů a komponentů) zhotovených různými samostatnými dodavateli a organizacemi. I když každý z dodavatelů dodrží požadovanou kvalitu svých částí, kombinování podsystémů do systémů vnáší nové chyby a nebezpečí, které nejsou vidět, pokud se na tyto části díváme jako na oddělené objekty. V mnohých průmyslových odvětvích se potvrdilo, že zabudování bezpečnosti do zařízení nebo výrobků může zredukovat celkové náklady na jejich životní cyklus, a že dosažení akceptovatelné úrovně bezpečnosti vyžaduje přístupy systémové bezpečnosti.
Aktivity související se systémem řízení bezpečnosti začínají hned v nejranějších stádiích vývoje koncepce systému a pokračují přes všechny projekční činnosti, výstavbu, výrobu, testování, provoz a odstavení. Podstatný aspekt, který odlišuje přístup založený na systému řízení bezpečnosti (systémové bezpečnosti) od ostatních přístupů k bezpečnosti je prvořadý důraz na včasnou identifikaci a klasifikaci nebezpečí tak, aby mohly být přijaté nápravy pro jejich eliminování, anebo minimalizování ještě před konečným projektovým rozhodnutím.

I navzdory skutečnosti, že je systém řízení bezpečnosti relativně novou a ještě stále se vyvíjející disciplínou, má své základní ideje, které jsou zachovány ve všech jejich projevech a odlišují ji od ostatních přístupů k řízení bezpečnosti a řízení rizika. Používají se zásady, že systém řízení bezpečnosti:

- zdůrazňuje budování bezpečnosti a ne její přidávání do vytvářeného systému,
- se zabývá systémem jako celkem, a ne jen jeho podsystémy a komponentami,
- pojímá ohrožení a s ním spojená nebezpečí poněkud šíře než jen jako chyby zařízení,
- klade důraz raději na analýzu, než později na získanou zkušenost a dodatečně vytvořené standardy,
- upřednostňuje kvalitativní přístupy před kvantitativními,
- rozpoznává důležitost změn a konfliktů cílů v projektu systému a je více, než jen systémové inženýrství.

Nejdůležitějším aspektem systému řízení bezpečnosti v souvislostech s prevencí havárií jsou procedury řízení bezpečnosti.

Účinné řízení bezpečnosti spočívá ve stanovení politiky a v definování cílů bezpečnosti, tj. v:

- plánování úloh a procedur; definování odpovědnosti a určení kompetencí,
- dokumentování a v průběžném sledování ohrožení a z nich plynoucích nebezpečí včetně kontrol,
- udržování bezpečnostního informačního systému včetně zpětné vazby a forem hlášení poruch / havárií apod.

Systém řízení bezpečnosti je odpovědný za zajištění bezpečnosti systému jako celku včetně analýzy interface mezi komponentami. Aktivity na úrovni bezpečnosti komponentů, jako např. bezpečnost raketové odpalovací rampy, mohou být součástí všeobecné odpovědnosti za systém řízení bezpečnosti (systémovou bezpečnost), anebo mohou být částí inženýringu komponentů při velkých a komplexních projektech. Pro vymezené druhy pohrom, jakými mohou být požáry, radioaktivní záření anebo výbušné prostředí, může být požadované další členění odpovědnosti za bezpečnost. Při jakémkoli odstupňování rozčlenění úsilí o kvalitní systém řízení bezpečnosti mají odpovědnost za integraci jednotlivých bezpečnostních aktivit a informací inženýři systému řízení bezpečnosti0. Systém řízení bezpečnosti je obyčejně provázaný s odpovídajícími inženýrskými, anebo vědeckými disciplínami jako např. inženýrství spolehlivosti, zajištění kvality, lidský faktor apod.
Jaké procesy a úlohy systému řízení bezpečnosti se provedou v konkrétním projektu, závisí na jeho velikosti a úrovni rizika projektovaného systému. Všeobecně platí, že bezpečnost a spolehlivost spolu úzce souvisí. Přitom platí, že bezpečné zařízení nebo bezpečný systém musí být spolehlivý, ale spolehlivý systém ještě nemusí být bezpečný. Spolehlivostní inženýrství se přednostně zabývá chybami a redukováním četnosti jejich výskytu. Spolehlivost je definovaná jako charakteristika daného objektu, která je vyjádřená pomocí pravděpodobnosti, že tento objekt bude vykonávat specifikovaným způsobem funkce, které jsou na něm požadovány během stanoveného časového intervalu a za stanovených resp. předpokládaných podmínek.
Reprezentativními technikami spolehlivostního inženýrství zaměřeného na minimalizaci chyb komponentů (součástek) a tím i chyb komplexních systémů, které byly zapříčiněné chybami komponentů, jsou:

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

Uvedené techniky jsou prokazatelně efektivní pro zvýšení spolehlivosti, ale bezpečnost nevyhnutelně nezvyšují, ba dokonce za jistých okolností ji mohou redukovat. Analýzy rizik prováděné u systému řízení bezpečnosti (systémové bezpečnosti) se dívají na interakce a nezaměřují se jen na chyby anebo jistoty inženýrského řešení. Spolehlivostní inženýři často považují spolehlivost a bezpečnost za synonyma. To je pravda jen v některých speciálních případech. Všeobecně má bezpečnost širší význam. Běžně mají spolehlivost a bezpečnost mnoho společných vlastností.
Mnohé havárie však nastanou bez toho, že by selhala nějaká komponenta. Právě naopak, častokrát všechny komponenty při haváriích fungovaly podle očekávání a bezchybně. Taktéž se může stát, že komponenty mohou selhat (mít poruchu) bez toho, aby došlo k havárii. Havárie a nehody mohou být zapříčiněny provozem zařízení mimo povolené rozsahy hodnot parametrů nebo časových limitů, z kterých vycházely analýzy bezpečnosti či analýzy spolehlivosti. To znamená, že systém může mít vysokou spolehlivost a přece může dojít k havárii. Navíc, generalizované pravděpodobnosti a analýzy spolehlivosti se nemohou přímo aplikovat na specifické, anebo lokální podmínky. Nejdůležitější je, že havárie a nehody mnohdy nejsou výsledkem jednoduchých kombinací chyb (selhání) komponentů.
Bezpečnost je vlastnost, která vystupuje na úrovni systému, když jsou komponenty provozovány společně. Události vedoucí k havárii mohou být složitou kombinací chyby zařízení, nesprávné údržby, problémů informačního a řídicího systému, zásahů člověka a konstrukčních chyb. Analýzy spolehlivosti se zaobírají jen pravděpodobnostmi havárií a nehod souvisejících s chybami. To znamená, že nevyšetřují potenciální škody, které může způsobit správná činnost (provoz) jednotlivých komponentů.
Není tudíž možné, aby spolehlivostní inženýrství nahrazovalo systém řízení bezpečnosti (systémovou bezpečnost), může ji ale doplnit. Musí to však být provedeno s jasným vědomím, že konečným cílem je zvýšení odolnosti systému vůči nebezpečí spojeným s výskytem náhodných chyb. Je vždy lepší, když se zařízení (systém) navrhuje tak, že individuálně náhodné chyby nemohou způsobit havárii, i kdyby se vyskytly; je si však třeba uvědomit, že to není vždy možné.
Velké opatrnosti je třeba při aplikování technik odhadování spolehlivosti pro posuzování bezpečnosti. Pokud nejsou havárie nevyhnutelně zapříčiněné událostmi, které se dají vyjádřit pravděpodobnostmi, nelze pro ně všeobecně používat míry pravděpodobnosti rizika. Odhady pravděpodobnosti měří pravděpodobnost náhodných chyb a ne rizik a nehod anebo havárií.
Když se při analýzách systému řízení bezpečnosti (systémové bezpečnosti) najde projektová chyba, je daleko účinnější ji

odstranit, než někoho přesvědčovat pomocí vypočítaných pravděpodobností, že tato chyba nikdy nezpůsobí havárii. Nízké hodnoty pravděpodobnosti výskytu havárie nezaručují bezpečnost a bezpečnost nevyžaduje mnohdy ultra vysokou spolehlivost zařízení.
Hlavním nedostatkem pravděpodobnostních modelů nejčastěji není to, co zahrnují, ale to, co nezahrnují. Nízké hodnoty pravděpodobnosti jednoduše hovoří o tom, že systém neselže uvažovaným způsobem, ale naopak, selže s daleko vyšší pravděpodobností způsobem, o kterém uvažováno nebylo. Odlišování rizika nehody od chyb je podstatné pro to, abychom porozuměli rozdílu mezi bezpečností a spolehlivostí.
Z praktických důvodů musí být přístupy systému řízení bezpečnosti efektivní a cenově dostupné. Návratnosti nákladů na program systému řízení bezpečnosti se dosáhne tehdy, když se zabrání haváriím. Efektivnost programu na zvyšování bezpečnosti pomocí systému řízení bezpečnosti (systémové bezpečnosti) se prokazuje velmi těžko, protože měřit něco, co se nestalo, je těžké.
Jeden z nepřímých způsobů měření efektivnosti programu na zvyšování bezpečnosti pomocí systému řízení bezpečnosti, byť i ne celkem uspokojivý pro nedostatek porovnávaných faktorů, je porovnávání systémů, které měly program na zvyšování bezpečnosti pomocí systému řízení bezpečnosti s těmi, které ho neměly. Jinou cestou zjišťování efektivnosti programu na zvyšování bezpečnosti pomocí systému řízení bezpečnosti je vykazování nebezpečí, které bylo personálem systému řízení bezpečnosti korigováno ještě předtím, než došlo k havárii, anebo bylo jinak zjištěno.
Třetí cestou odhadování efektivnosti programů na zvyšování bezpečnosti pomocí systému řízení bezpečnosti je zkoumání případů, při kterých nebylo respektované doporučení systémové bezpečnosti a došlo k haváriím.

Závěr

Analýza poznatků o nehodách skoronehodách a haváriích ukazuje příčiny základní i mnohonásobné, které mají původ v technologiích, v lidském faktoru a též v nepoznaných neurčitostech v chování složitých systémů. Z důvodu ochrany lidí, majetku a životního prostředí se zabývá řízením bezpečnosti technologických systémů a doporučuje, aby do praxe byl zaveden systém řízení bezpečnosti, ve kterém jsou včleněna preventivní, zmírňující, reaktivní i obnovovací opatření a činnosti s ohledem na dopady možných havárií.
Je jasné, že pokud jde o riziko, dnešní složitá, technologicky orientovaná společnost požaduje, aby důvěra veřejnosti byla založená na znalostech expertů. V daném smyslu je odpovědnost za detekci a ochranu před nebezpečím přenesená z obyvatelstva na stát, management podniků, inženýry, bezpečnostní experty a na jiné odborníky. Není ale rozumné úplně se vzdát osobní odpovědnosti. V některých případech, jako např. při havárii v chemickém provozu nadnárodní firmy Union Carbide (USA) v Bhópálu (Indie, 1984) se obyvatelstvo při nouzovém plánování a účinném chování při havárii zcela spolehlo na instituce, což mělo tragické následky. Chemická továrna Bhopal Union Carbide byla provozována tak, že bylo jisté, že v ní musí dojít k vážné havárii. Také nouzové plánování, evakuační plán, trénink a pomůcky byly neadekvátní možnému nebezpečí. Okolní obyvatelstvo nebylo varované před možným i vzniklým nebezpečím a nikdo mu neoznámil ani jednoduchá opatření (např. dát si na obličej vlhký šátek), která by mohla tehdy zachránit lidem život. Katastrofické havárie tohoto druhu vyburcovaly veřejnost k větší zainteresovanosti v otázkách rizika.
Naopak, zájem veřejnosti u problémů, které minulé generace považovaly za zajištěné, jako např. nebezpečí související se zdravotnictvím, dopravou a průmyslem, vede ke státní regulaci a k vytváření veřejných sdružení pro kontrolu nebezpečí, která byla kdysi tolerovaná.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] PROCHÁZKOVÁ, Dana, J. BUMBA, V. SLUKA, B. ŠESTÁK, 2008: Nebezpečné chemické látky a chemické přípravky a průmyslové nehody. ISBN 978-80-7251-275-1, PA ČR, Praha, 420p.
[2] PROCHÁZKOVÁ, Dana, 2011: *Ochrana osob a majetku*. ČVUT, Praha, ISBN: 978-80-01-04843-6, 301p.
[3] OECD, 2002: Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response. OECD, Paris, 191p.
[4] PROCHÁZKOVÁ, Dana, 2011: *Analýza a řízení rizik*. ČVUT, Praha, ISBN: 978-80-01-04841-2, 405p.
[5] PROCHÁZKOVÁ, Dana, 2011: *Strategické řízení bezpečnosti území a organizace*. ISBN: 978-80-01-04844-3. ČVUT, Praha, 483p.
[6] PROCHÁZKOVÁ, Dana, 2012: *Bezpečnost kritické infrastruktury*. ČVUT, Praha, ISBN: 978-80-01-05103-0, 318p.

ADRESA AUTORA:

Dana PROCHÁZKOVÁ, doc., RNDr., DrSc., ČVUT v Praze, Fakulta dopravní, Konviktská 20, 110 00 Praha 1, Česká republika, e-mail: prochazkova@cvut.fd.cz

RECENZENT:

Vojtech KOLLÁR, prof. Ing., PhD., Vysoká škola ekonómie a manažmentu verejnej správy v Bratislave, Ústav verejnej správy, Furdekova 16, 851 04 Bratislava 5, Slovenská republika