AZIN CZ společnost s r. o.

ISATech s.r.o.
Industrial Safety Assessment Technicians

T-SOFT

Spolehlivost lidského činitele

VÚBP, v.v.i.

Výzkumný ústav bezpečnosti práce, v.v.i.

Praha 2008

Spolehlivost lidského činitele

Výzkumný ústav bezpečnosti práce, v .v.i.
Praha 2008

Tato souborná metodika je výstupem projektu „1H-PK/21: Metody a nástroje hodnocení a zvyšování spolehlivosti lidského činitele v provozu JE“, který byl řešen v rámci programu POKROK vyhlášeného Ministerstvem průmyslu a obchodu ČR.

Zpracovali: Ing. Miloš Paleček, CSc., RNDr. Stanislav Malý, Ph.D., Ing. Adam Gieci

Recenzenti: Ing. Aleš John, Ing. Mgr. Karel Matějka, MTh.

Vzor citace:
PALEČEK, Miloš; MALÝ, Stanislav; GIECI, Adam. Spolehlivost lidského činitele. 1. vyd. Praha : Výzkumný ústav bezpečnosti práce, 2008. 140 s. ISBN 978-80-86973-28-9.

Anotace: Jaderná zařízení vzbuzují jak respekt vyvolaný používanými špičkovými technologiemi a pracovními postupy, tak nedůvěru, ke které přispívá každá neprojektová situace kterékoli části provozu. Na těchto neprojektových situacích se podílí v podstatné míře obsluha. Projekt je zaměřen na rozbor standardních a nestandardních operačních postupů, ke kterým dochází při provozu jaderného zařízení a které mají vliv na jeho bezpečnost. Úloha lidského činitele bude posouzena z pohledu jeho chybování a nespolehlivosti. Bude navržen kriteriální aparát, který umožní priorizaci vlivů lidského činitele na bezpečnost jaderného zařízení. Pro navrženou a aplikovanou metodiku hodnocení lidského činitele budou zpracovány algoritmy. Ty budou základem pro zpracování softwaru umožňujícího využití PC při hodnocení lidského činitele na vzniku nebo nežádoucím rozvoji neprojektové situace.
Klíčová slova: spolehlivost, lidský činitel, selhání, prevence nehod, identifikace příčin selhání

Annotation: Nuclear power houses raise respect triggered by top technologies, working procedures and mistrust in each non-project situation of any operation segment. The operators give vast support to non-project situations. The project is focused on an analysis of the standard and non-standard procedures that are subject to nuclear operation and influencing safety. The task of human factor based on erroring and unreliability will be evaluated. A criterion model enabling to prioritise influence of human factor on nuclear operation will be put forward. Algorithms will be designed both for the proposed and applied methodology. The algorithms will be the base for software development that will make it possible to use a PC for assessment of human factor while a non-project situation is originating or on-going.
Keywords: reliability, human factor, failure, accident prevention, failure reason identification

ISBN 978-80-86973-28-9

OBSAH

ÚVOD

Lidský činitel (LČ) – člověk - představuje v pracovních systémech z hlediska spolehlivé činnosti systému nejméně spolehlivý a nejvíce zranitelný článek. Selhání LČ je příčinou velkého počtu neprojektových situací. Z oblasti jaderné energetiky lze uvést např.

- Windscale (VB) – přehřátí palivových článků s následným požárem v reaktoru zaviněný nepozorností obsluhy velínu (1957),
- Chalk River (Kanada) – únik aktivity způsobený nekázní obsluhy (1958),
- Pickering (Kanada) – únik chladiva způsobený chybou operátora a nedostatečnou kontrolou obsluhy (1974),
- Browns Ferry (USA) – při nedodržování bezpečných pracovních postupů založila obsluha požár, který se rozšířil až na reaktorovou halu (1975),
- Jaslovské Bohunice (ČSSR) - únik aktivity do sekundáru způsobený nedůslednou kontrolou zaváděných palivových článků (1977),
- Three Mile Island (USA) – po havarijním odstavení reaktoru únik chladiva s následným tavením aktivní zóny způsobený nepozorností obsluhy (1979),
- Černobyl (SSSR) – exploze v aktivní zóně zaviněná úmyslným odstavením všech automatických bezpečnostních prvků (1986). Zejména poslední uvedená havárie ukázala možné katastrofální následky, které mohou vzniknout v jaderných elektrárnách (JE) v důsledku selhání LČ.

Spolehlivost a bezpečnost jaderných elektráren má i závažný politický aspekt, jak ukazují aktivity rakouských politiků a nátlakových skupin v Rakousku i České republice. Protože spolehlivost celého systému je determinovaná jeho nejslabším článkem, je LČ jako nejslabší článek systému významným faktorem při zajišťování spolehlivosti jaderných elektráren.

Podceňování rizik, neznalost způsobů jejich identifikace a omezování jsou limitující faktory dalšího zvyšování spolehlivosti provozu nejen jaderných zařízení, ale i většiny složitých technických zařízení a provozů.

Řešitelský tým projektu 1H-PK/21 „Metody a nástroje hodnocení a zvyšování spolehlivosti lidského činitele v provozu JE“ vydává první část materiálu k tématu spolehlivosti lidského činitele s cílem seznámit pracovníky zabývající se problematikou spolehlivosti složitých technických zařízení i odbornou veřejnost s problematikou LČ v těchto systémech. Na základě výsledků dosažných ve výše uvedeném projektu bude v r. 2007 zpracována druhá část, věnovaná popisu metod a nástrojů pro identifikaci selhání LČ a pro zvyšování jeho spolehlivosti.

1 RIZIKOVÉ FAKTORY PRŮMYSLOVÝCH SPOLEČNOSTÍ

Závažné průmyslové havárie v chemických továrnách, v jaderných elektrárnách, tragédie při letech do vesmíru, katastrofy dopravních letadel a jiné, měly vždy několik typických společných příznaků: byly to havárie složitých technologických systémů, nebyly iniciovány jednoduchou chybou či selháním jedné komponenty a nebezpečí, která je vyvolala, byla většinou již dopředu známa. Pochopení takových havárií a možnosti účinné ochrany si vynutilo novou koncepci bezpečnosti dnes známou jako systémové havárie. Spočívá zejména v tom, že bezpečnost složitých systémů je chápána jako emergentní vlastnost jejich hierarchické struktury. Za rozhodující ukazatel bezpečnosti systémů jsou pokládána taková omezení vztahující se na jejich konstrukci a řízení, která eliminují, nebo alespoň redukují možná ohrožení provozu na kontrolovatelnou úroveň.

V předkládané studii je podán jak výklad základních pojmů a teoretických principů, na nichž je systémový přístup k haváriím složitých technologických systémů založen, tak celkový přehled o vývoji a současné praxi rozboru a prevence systémových havárií.

V závěrečné části studie jsou popsány hlavní aspekty havárií v jaderných zařízeních, roztříděné podle tříúrovňové hierarchické struktury příčin havárií. Hlavním účelem této studie je přiblížit systémový přístup k haváriím složitých systémů našim odborníkům v bezpečnosti rizikových provozů a podnítit jeho širší využívání zejména v jaderné energetice.

1.1 Změna postoje k riziku

Každá lidská činnost představuje riziko; neexistuje život bez rizika. Bezpečné zápalky a bezpečná břitva, jako příklad, nejsou bezpečné, ale pouze bezpečnější, než některé jiné. Pokrok vyžaduje přijetí rizika a navzdory velkému technologickému pokroku nejsme schopní veškerá rizika odstranit. Dnes však lidé vyžadují mnohem více než v minulosti, dnes chtějí, aby riziko bylo známo a kontrolováno v takové míře, jak jen to je prakticky možné.

Převládajícím fenoménem dneška je posun od čistě osobní odpovědnosti ke kolektivní, nebo podnikové odpovědnosti za rizika. Na začátku minulého století si dělníci museli sami své vlastní nástroje zajistit tak, aby s nimi mohli bezpečně manipulovat. Znali rizika své práce a přejímali odpovědnost za svou vlastní bezpečnost. Tento postoj byl částečně odůvodnitelný skutečností, že pracující věnovali celou svou kariéru výrobějednoho, nebo dvou produktů. Svoji práci důkladně znali a měli pod kontrolou vše, co souviselo s jejím vykonáváním.

V dnešní době jsou dělníci daleko víc závislí na svých zaměstnavatelích. To přirozeně vede k posunu odpovědnosti za bezpečnost od pracovníků k zaměstnavateli. Ve většině průmyslových zemí se od zaměstnavatelů požaduje, aby zabezpečili bezpečné pracovní prostředí a nutné vybavení a zařízení pro jeho udržování. Navíc, změny zákonů a odpovědnost za jejich plnění vedou k programům bezpečných produktů, které chrání jak pracující při jejich výrobě, tak spotřebitele.

Je jasné, že pokud jde o riziko, dnešní složitá, technologicky orientovaná společnost požaduje, aby důvěra veřejnosti byla založena na znalostech expertů. V tomto smyslu je odpovědnost za detekci a ochranu před nebezpečím přenesena z obyvatelstva na stát, na management podniků, na inženýry, bezpečnostní experty a na jiné odborníky. Není ale rozumné úplně se vzdát osobní odpovědnosti. V některých případech jako např. při havárii v Bhopalu se obyvatelstvo při havarijním plánování a účinném chování při havárii zcela spo-

lehlo na instituce, což mělo tragické následky. Chemická továrna Bhopal Union Carbide byla provozována z hlediska bezpečnosti zcela nedostatečně, takže pravděpodobnost, že v ní dojde k závažné havárii byla mnohonásobně vyšší, než by tomu bylo v případě dodržování zásad safety managementu, tj. bezpečné práce. Také havarijní plánování, evakuační plán, výcvik a pomůcky nebyly adekvátní možnému nebezpečí. Okolní obyvatelstvo nebylo varováno před vzniklým nebezpečím a nikdo mu neoznámil ani tak jednoduchá opatření jako např. dát si na obličej vlhký šátek, která mohla tehdy mnoha lidem zachránit život. Takovéto havárie vyburcovaly veřejnost k větší zainteresovanosti v otázkách řízení 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.

V popisu tragédie v Bhópálu vyjadřuje Bogard [8] tento nový postoj: „Nejsme bezpeční před riziky, která přinášejí nebezpečné technologie a každý výběr nové technologie přináší s sebou možnost nejhoršího možného scénáře, který musíme vzít v úvahu při každém rozhodování o její implementaci. Veřejnost má právo vědět přesně, jaké jsou tyto nejhorší scénáře a podílet se na všech rozhodnutích, které přímo nebo nepřímo ovlivňují jejich budoucí zdraví a blahobyt. V mnoha případech musíme přijmout fakt, že výsledkem využití takového kritéria může být rozhodnutí zabránit implementaci nebezpečné technologie.“

Zvýšené regionální a národní obavy o bezpečnost se v posledním desetiletí rozšířily na mezinárodní úroveň. Skleníkový efekt, kyselé deště a havárie takového rozsahu, jakým bylo uvolnění radioaktivity v Černobylu, neznají národní hranice. Globální ekonomika a velký destruktivní potenciál některých našich technologických výdobytků zesilují naše poznání, že riziko může mít mezinárodní důsledky a že jeho kontrola vyžaduje kooperativní přístup všech států.

Protože náklady na redukování rizika mohou být vysoké a často srovnatelné s jinými požadovanými cíli, je důležité zvažovat, zda zvýšené obavy veřejnosti a vlád z technologických rizik jsou oprávněné a zda se inženýři, ať hardwaroví či softwaroví, mají těmito problémy zatěžovat. Je zvyšování rizika v naší moderní společnosti výsledkem nových technologických výdobytků, nebo pouze zakoušíme neoprávněně novou formu luddizmu[1]?

1.2 Je zvýšená obava z nebezpečí oprávněná?

Určení, zda technologické riziko narůstá nebo ne, závisí na použití údajů a jejich interpretaci. Na jedné straně Harris a jeho kolegové [24] argumentují tím, že technologická nebezpečí vyjádřená termíny úmrtnosti lidí byla v minulosti mnohem větší v nedostatečně řízených stádiích průmyslového vývoje. Údaje z Výboru pro Národní bezpečnost poukazují na to, že nárůst úmrtnosti a úrazů obyvatelstva od začátku minulého století soustavně klesá, a že úmrtnost z technologických nebezpečí průběžně neroste. Varují však, že “pozitivní“ efekty technologie dosáhly na určitou dobu svého maximálního vlivu na úmrtnost lidí, ale technologická nebezpečí pokračují částečně neevidovaná a významně ovlivňují chronické příčiny smrti, které v současnosti představují v USA 85% úmrtnost.

Na druhé straně zkoumání výskytu technologických havárií potvrzuje více než zkoumání výskytu úmrtnosti a úrazů obyvatelstva, že technologické riziko se zvyšuje. Šedesát procent ze všech průmyslových katastrof od roku 1921 do 1989 se přihodilo po roce 1975. V roce 1989 Bogard [8] prokázal, že 12 z 19 velkých průmyslových havárií v 20. století, které si vyžádaly 100 a více úmrtí, se stalo po roce 1950. Když k tomu přidáme události menšího rozsahu, např. dopravní nehody, protržení přehrad a strukturální kolapsy, je podpora hypotézy o narůstání rizika evidentní.

Aby však nebyly věci tak jednoduché, je zde skutečnost, že navzdory zvýšení celkového počtu technologických havárií, došlo k poklesu výskytu havárií v určitých specifických typech systémů. Například počet havárií ve vojenském letectvu v poslední době výrazně poklesl. Toto zlepšení je třeba přičíst důrazu programů systémové bezpečnosti a zvýšenému úsilí o eliminaci a kontrolu nebezpečí. Zdá se, že tato zkušenost z vojenského letectví podporuje argument, že technologický pokrok nemusí zvýšit riziko, jestliže se vynaloží patřičné úsilí na jeho kontrolu. V současnosti se však zpomalil pokles havárií ve vojenském letectví, který je připisován využívání technik systémové bezpečnosti. Jedním z vysvětlení tohoto zpomalení může být jednoduše přirozené zvýšení těžkostí při hledání cest pro velká zlepšení, přestože by se tu mohly uplatnit i jiné, méně obvyklé faktory. Další snižování míry rizika je však náročnější.

Je jasné, že odpověď na naši otázku o oprávněnosti obav z nárůstu nebezpečí nenajdeme v těchto nejasných a vzájemně si odporujících statistických údajích. Ve skutečnosti velké změny v technologii, ke kterým došlo v éře po 2. světové válce, dělají v dnešní době dlouhodobé historické údaje o riziku nepoužitelnými. Předcházející zkušenost nám neumožňuje předvídat budoucnost, když rizikové faktory v současnosti jsou a v budoucnu i budou odlišné od faktorů z minulosti. Bližší pohled na tyto změny nám pomůže pochopit problémy, před které jsme dnes postaveni.

1.3 Unikátní rizikové faktory průmyslových společností

Definice rizika říká, že riziko je kombinací pravděpodobnosti havárie a závažnosti jejích potenciálních následků. Riziko stoupá, když se zvyšuje pravděpodobnost havárie nebo rozsah možných ztrát. Tyto dvě složky rizika mohou být ovlivňovány různými faktory. Některé z nich, obzvlášť významné v dnešní době, vytvářejí nová nebezpečí, jako například nárůst složitosti (komplexnosti), zvyšování počtu lidí vystavených riziku, zvyšování kumulace energií, centralizace, rozsah a tempo technologických změn v systémech, které se dnes snažíme vybudovat.

Nová nebezpečí a hrozby

Před průmyslovou revolucí bývaly příčinou neštěstí přírodní katastrofy nebo poruchy v několika relativně dobře známých a jednoduchých technologických zařízeních jako například vysokotlaké parní kotle. Ve 20. století vědecký a technologický pokrok zredukoval nebo eliminoval mnohá z dřívějších rizik. Například moderní medicína dokáže léčit nemoci, které předtím byly smrtelné.

Věda a nové technologie však přinesly nová nebezpečí. Nesprávné používání nebo předávkování antibiotiky vede ke vzniku nových rezistentních mikrobiálních kmenů. Děti již nepracují v uhelných dolech nebo jako kominíci, ale dnes jsou vystaveny chemikáliím a pesticidům v potravě a škodlivým látkám v ovzduší. Využívání radiačního záření zvýšilo riziko chorob a úmrtí z ozáření.

Mnohá z nových nebezpečí jsou záludnější, hůře odhalitelná a odstranitelná než v minulosti. Navíc, nemáme žádnou předcházející zkušenost, které bychom se mohli přidržovat při překonávání nových nebezpečí. Mnoho z toho, o čem jsme se poučili z předcházejících havárií, je uloženo v zákonech a poznatcích o dobré praxi. Avšak odpovídající zákony a normy pro mnohé z nových inženýrských odvětví a technologií ještě nejsou vypracovány. Mnohokrát se poučení získaná za celá staletí ztratí, když se starší technologie nahradí novějšími. Například, když se mechanické zařízení nahradí digitálními počítači. Mnohé přístupy k ochraně před haváriemi, které v minulosti fungovaly u jednodušších technologií, jako

např. zdvojování komponent jako ochrana před selháním jedné z nich, jsou pro kontrolu dnešních komplexních rizik neefektivní. I když redundance poskytuje ochranu před haváriemi zapříčiněnými selháním individuálních částí, není stejně efektivní vůči nebezpečím, která vytvářejí interakce mezi komponenty ve stále komplexnějších inženýrských systémech dneška. Redundance mohou ve skutečnosti zvýšit složitost až do takové míry, že vlastně ony samotné přispívají k haváriím.

Zvyšování složitosti

Mnohá z nových nebezpečí jsou spojena se zvyšující se složitostí systémů, které dnes budujeme. Složitost vytváří nejen nová nebezpečí, ale činí je i hůře odhalitelnými. Perrow [52] odlišuje havárie způsobené selháním komponent od těch, které nazývá systémovými haváriemi, jež vznikly v důsledku složitosti spleti navzájem působících komponent. Vyspělé technologické systémy jsou často sestaveny jako síť úzce na sebe vzájemně působících podsystémů. Ze spojů mezi podsystémy vznikají problémy a poruchy se šíří z jedné komponenty na druhou. Jako příklad takto se zvyšující složitosti můžeme uvést petrochemický závod, ve kterém jsou často mnohé odděleně probíhající chemické procesy zkombinovány do jedné kontinuální výroby bez meziskladů, které by oddělovaly jednotlivé samostatné provozní podsystémy.

Analýzy velkých průmyslových havárií nezvratně odhalily jako příčinu velmi složité souvislosti jevů místo selhání jednotlivých komponent. Pokud v minulosti bylo selhání komponent uváděno jako hlavní příčina havárií, většina dnešních havárií je výsledkem nebezpečných konstrukčních charakteristik složitých komponent a interakcí mezi nimi. Provoz mnoha dnešních systémů je už tak složitý, že mu ve skutečnosti rozumí pouze několik expertů. Vysoká složitost a vzájemné interakce konstruktérům komplikují úvahy o všech nebezpečích, dokonce i o velmi významných a také operátorům komplikují bezpečné ovládání normálních a poruchových provozních situací. Funkční složitost dnešních zařízení velmi komplikuje práci konstruktérů a rozsáhlé projekty jejich vybudování vyžadují spolupráci enormního množství lidí a týmů. Anonymita týmůpotlačuje individuální odpovědnost jejich členů. Mnohé nové specializace dnes nemají standardy individuální odpovědnosti a etiky, jaké byly zpracovány pro starší profese.

Kletz [35] vyzvedává paradox, že lidé jsou ochotni utrácet peníze za složitost a ne za jednoduchost. Uvádí příklad havárie, která se stala v jednom chemickém závodu ve Velké Británii. V tomto podniku měla čerpadla a některá potrubí vícenásobné rozdílné použití (módy), mezi které patřilo: přečerpávání metanolu z autocisterny do zásobníků na zpracování v továrně, a také i na přepravu zpracovaného metanolu z továrny. Otvírání, zavírání a nastavování jednotlivých ventilů, monitorování jejich otevření, zapínání a vypínání čerpadel bylo řízeno počítačem. K havárii došlo při vyprazdňování autocisterny. Čerpadlo bylo zapnuto z řídícího panelu, ale ještě před tím bylo ručnězastaveno tlačítkem ručního ovládání. Další operací mělo být přečerpání určitého množství metanolu ze zásobníku do továrny. Když bylo přečerpání ukončeno, počítačvydal příkaz pro vypnutí čerpadla. Protože bylo spuštěno ručně, nebylo vypnuto a došlo k výtoku metanolu.

V tomto případě by jednodušší konstrukční řešení spočívající v instalaci samostatného potrubí pro každou funkci (jež bylo po havárii zrealizováno) provedlo takovou chybu s daleko menší pravděpodobností a nebylo by ani o mnoho dražší vzhledem k životnosti výrobního zařízení.

Počítače často umožňují vytvořit systémy s velkým počtem vzájemněinteragujících částí a možných selhání, čímž podporují zbytečnou a nebezpečnou složitost v systémech. Kletz [35] poznamenává: „Programovatelné elektronické systémy nevnesly nové formy chyb

či selhání, ale zvýšením složitosti řízených procesů vytvořily více možností pro běžné chyby“. Jestliže akceptujeme Perrowův [52] argument, že příčinou těžkých havárií je interaktivní složitost a párové ovlivňování sousedních komponent, potom zavádění počítačů do řízení nebezpečných systémů či provozů může zvýšit riziko, pokud se přitom nebude věnovat velká péče minimalizování složitosti a vzájemných vazeb.

Vzrůstající vystavování se nebezpečí

Dnes se stává složitější nejen technologie, ale celá naše společnost je stále složitější, vzájemně provázaná a zranitelná. Následky havárie nezávisí jen na samotném nebezpečí, ale i na vystavení se tomuto nebezpečí, tj. doba trvání účinků a rozsahu zasaženého okolí. Dnes je mnohem více lidí vystaveno riziku než v minulých dobách. Například kapacita velkých letadel je soustavně zvyšována vzhledem k ekonomickým efektům. Nebezpečné provozy se budují stále blíže lokalit s velkou hustotou obyvatelstva.Velké továrny zaměstnávají vysoký počet zaměstnanců a nutí je denně dojíždět na velké vzdálenosti v přehuštěné městské dopravě. Vnitřní provázanost a složitost mohou vést k explozivnímu růstu nebezpečí, které přerůstá oblast jejího bezprostředního vlivu a umocňuje potenciál následků havárie.

Zvyšování kumulace energií a dosahů nebezpečí

Jiným faktorem, souvisejícím se zvýšeným rizikem, je objev a používání vysoce energetických zdrojů, jakými jsou např. extrémní paliva, vysokotlaké systémy či štěpení atomových jader, což velmi zvýšilo množství potenciálních ztrát. Přestože mnohé nové systémy používají konvenční energetické zdroje, obsahují zase technologie, které vyžadují nepoměrně větší množství energie než v minulosti. V teorii systémových havárií se nebezpečí všeobecně chápe jako nežádoucí přenos energie. Větší množství energie rozšiřuje plochu okolí, které může být potenciálně zasaženo havárií a zvyšuje množství možných ztrát. Nová nebezpečí, jako například únik radioaktivních látek, která mohou způsobit např. genetická poškození, nebo kontaminaci okolí, přinášejí potenciál pro zasažení nejen nynější generace, ale i dalších budoucích generací.

Zvyšování automatizace

Přestože se zdá, že by automatizace mohla snížit riziko chyby operátorů, zůstává skutečnost, že automatizace nevyloučila lidi ze systémů řízení, ale pouze je přesunula do údržbářských a opravářských funkcí a do vyšších úrovní supervizní kontroly a rozhodování. Efekty rozhodnutí a zásahů člověka na těchto vyšších úrovních řízení mohou být extrémně závažné, obzvlášť při paralelně se zvyšující složitosti zařízení, kde se proces rozhodování stává velmi obtížným.

Operátoři technologických procesů s automatizovanými systémy řízení nejčastěji pracují v ústřednách, kde se musí spolehnout na zprostředkované informace o stavu ovládaného zařízení. Tyto informace mohou být zavádějící. V roce 1997 zažil New York masivní a nákladný výpadek elektrické energie. Při řešení počátečních symptomů, když operátoři postupovali podle předepsaných předpisů, došlo k úplnému výpadku elektrické soustavy. Manipulanti v ústředně neměli dostatečné informace, že došlo k poruše dvou relé, přičemž porucha jednoho vedla k vysokému proudu ve vedení, kterým běžně protéká malý nebo žádný proud a chyba druhého relé zase blokovala proud ve vedení, takže tento se jevil jako normální. Operátoři nemohli tyto závažné skutečnosti rozpoznat a za příčinu havárie byla označena chyba člověka i přesto, že skutečná chyba byla způsobená vlastnostmi automatického systému.

Počet takových problémů se budou s trendem k decentralizaci automatického řízení jen zvyšovat. Mikroprocesory, vložené do zařízení nebo systémů, se stávají centry většiny řídících funkcí a jen informace na vysoké úrovni řízení jsou zpětně posílány do centra kontroly. Tato koncepce limituje možnosti operátorů, pokud brání širšímu poznání a chápání provozního stavu zařízení. Řídící smyčka ve své podstatě precizně maskuje vznik a následný vývoj poruchy, protože eliminuje bezprostřední účinky vzniklého problému přinejmenším na nějaký čas. Toto "maskování" však netrvá do nekonečna. Když je porucha konečně objevena, může být už mnohem těžší zasáhnout, protože první příznaky už mohou být potlačeny nebo zrušeny. Za dobu, kdy se do situace včlení člověk, symptomy, už mohou hlavními smyčkami řízení probíhajícího procesu proniknout vpřed nebo zpět. Např. v roce 1985 letoun čínských aerolinií Boeing 747 měl poruchu způsobující menší tah na vnějším pravém motoru. To způsobilo, že letadlo se začalo stáčet doprava. Autopilot tuto poruchu automaticky kompenzoval až do doby, kdy dosáhl limit svých kompenzačních možností a dále nemohl udržovat letadlo ve stabilním směru. V tomto momentu už posádka neměla dost času na určení příčiny nestability a na vhodný zásah. Letadlo začalo rotovat a vertikálně padat z výšky 31 500 stop ještě dřív, než mohla být příčina odhalena. Letadlo bylo zcela zničeno.

Systémy úspor energie zaváděné zejména v 70.letech minulého století do podniků s kontinuálními výrobními procesy (rafinérie, elektrárny a pod.) pro snižování spotřeby energie a zvyšování tepelné účinnosti, byly další komplikací související s automatizací. Např. teplo, generované určitým procesem, mělo být dále zužitkováváno pomocí tepelného výměníku. Jak se to často stává, vícenásobné cíle, v tomto případě bezpečnost a ekonomika, vedou ke konfliktům. Systémy pro úsporu energie vnášejí interakci mezi komponenty, které činí fungování celého systému méně přehledným jak pro konstruktéry, tak i pro operátory. Z pohledu konstruktérů se stává systematická analýza a predikování událostí, které mohou vést k haváriím, stále obtížnější. Z pohledu operátorů extrémní složitost ztěžuje diagnostikování provozních problémů a opět vede k maskování symptomů a vynucuje si jejich týmové přešetření. Místo, kde se objevily příznaky poruchy v zařízení poprvé, nemusí být místem, kde problémy vznikly.

Narůstající centralizace a výrobní kapacita

Narůstající automatizace je provázena centralizací průmyslové výroby do velkých továren a vytvářením potenciálu velkých ztrát a škod na zařízeních, lidech a okolí. Už několik desetiletí se velikost továren zvětšuje a roste výrobní kapacita zařízení a celé procesy prorůstají do neotestovaných oblastí. Např. pro jadernou energetiku dostali v r.1968 výrobci objednávky na elektrárny, které byly šestkrát větší než do té doby provozované elektrárny. Bylo to v průmyslovém odvětví, ve kterém se až do té doby považovalo dvojnásobné zvětšení výrobní kapacity za hraniční. Jaderná elektrárna Browns Ferry, na které došlo v r. 1975 k vážné havárii, byla desetkrát větší než všechny ostatní provozované elektrárny v roce 1966, když ji začali stavět [102].

Námořní doprava je dalším odvětvím, které prochází velkými změnami. Přepravní kapacita velkých zaoceánských lodí, zejména supertankerů na přepravu kapalin (ropy) a plynů, dávno přesáhla všechny představitelné meze vývoje respektujícího předcházející zkušenosti. Lodě jsou stavěny bez hlouběji zdůvodněných konstrukčních principů a bez redundantních systémů (dvojitý plášť), které se používaly předtím. Mostert [50] charakterizoval tyto lodě takto: „Gigantické supertankery vytvářejí abstraktní prostředí, ve kterém jsou posádky na míle vzdálené přímé zkušenosti s vlastnostmi a nebezpečím moří a oceánů. Vysoký stupeň automatizace ohrožuje tradiční cit a vnímavost inženýrů, které byly považovány za jejich stavovskou přednost. Právě tyto hodnoty byly v minulé době rozhodujícími bezpečnostními faktory v námořní dopravě".

Nárůst tempa technologických změn

Posledním rizikovým faktorem je nárůst tempa technologických změn v posledním století. Průměrná doba zavedení základních technických objevů do komerčního používání se zmenšila z třiceti let začátkem minulého století na pět a méně let v současnosti. Navíc počet nových výrobků nebo procesů exponenciálně narůstá. Dvacáté století se jeví jako největší akcelerátor nárůstu nových průmyslových odvětví založených na vědeckých a technologických inovacích, jakými jsou např. genové inženýrství a pod. Nebezpečné látky se začaly využívat v bezprecedentním rozsahu a ekonomické tlaky se často stavěly proti extenzivnímu testování jejich možných škodlivých účinků.

Vzrůstající tempo změn zmenšilo příležitost poučení se ze zkušeností. Systémy menšího rozsahu a relativně bezpečné se dosud mohly vyvíjet postupně metodou pokus-omyl. Pro většinu moderních výrobků a procesů, při kterých jsou změny velmi rychlé a postihy za chyby velmi vysoké, je učení pomocí pokusů a omylů nemožné. Konstrukce a provozní postupy musí být správné hned napoprvé, pokud existuje hrozba velkého požáru, výbuchu nebo úniku toxických látek. Christopher Hinton [13], který byl šéfem první britské jaderné elektrárny, v r.1957, řekl: „Všechny inženýrské technologie se zdokonalily ne na základě úspěchů, ale na základě vlastních chyb. Mosty, které spadly, přidaly našim vědomostem o konstrukcích mostů víc než ty, které stojí; kotle, které explodovaly nás naučily víc než ty, které nehavarovaly. Atomová energie však musí předcházet této výhodě zdokonalování se na základě poznatků umocněných chybami“. Výsledkem je, že empirická konstrukční pravidla a standardy zařízení jsou nahrazovány spoléháním na identifikaci a kontrolu rizik při provozu zařízení, nebo snahami o vybudování vysoce spolehlivých systémů, které nikdy nehavarují. Praktický úspěch kteréhokoliv z těchto přístupů je neurčitý v porovnání se staršími metodami, které vycházely z učení se ze zkušenosti a používání dobře otestovaných norem a návodů.

S problémem nárůstu množství technologických změn se musí vyrovnávat i vládní a společenské instituce a agentury, které udělují licence a vykonávají dozor nad bezpečností. Nové technologie, například počítače, vyžadují nové normy a postupy schvalování a samozřejmě čas, během kterého se vyvinou a vyrostou odborníci pro jejich aplikaci. Průmysl a společnost si nepřejí zpomalování progresu, přičemž dozorové orgány nemusí stačit jeho tempu.

Jaká bezpečnost je dostatečná bezpečnost?

Zdá se, že jsme se při hledání odpovědi na oprávněnost zvýšení obav z nebezpečí vrátili tam, kde jsme začínali - nemáme skutečný důkaz, že problém existuje, ale je dost faktů, které jeho existenci podporují. Když prověříme výše popsané rizikové faktory, můžeme jednoznačně tvrdit, že naše obavy o bezpečnost nových technologií jsou oprávněné.

To, že dnešní technologické změny a rizikové faktory nedovolují aplikovat předcházející zkušenosti se spolehlivostí zařízení ještě neznamená, že když se určité typy havárií v minulosti nepřihodily, je to záruka, že se nemohou vyskytnout v budoucnosti. Navíc, jestliže se musíme učit z havárií a jestliže nás chyby naučí více než úspěch, co potom můžeme dělat se systémy, ve kterých už jednoduchá porucha může mít tragické následky? Zde je proces učení se z chyb neakceptovatelný.

Systémový přístup k bezpečnosti redukuje riziko anticipováním havárií a jejich příčin pomocí předběžné analýzy nebezpečí (preliminary hazard analysis) více, než pomocí zjištění z rozborů vzniklých událostí (after-the-fact accident investigations) a eliminováním resp. kontrolou rizik tak, jak jen je to možné během celého životního cyklu systému. Cílem je ro-

zumět a řídit riziko ve smyslu eliminování havárií nebo redukování jejich následků. Úspěch tohoto přístupu se ukázal ve vojenství a kosmonautice.

Bohužel nebezpečí nelze nikdy kompletně odstranit ze všech systémů. Navíc, vzájemně si odporující cíle v systémech ztěžují už beztak komplikované předvídání havárií v technických systémech. Je principiálně možné konstruovat systémy, které jsou bezpečné vůči určitému typu rizik, ale navrhnout systém, který je chráněn před každým rizikem, vyžaduje tak velké množství kompromisů v jeho funkčnosti, že se ho ani nevyplatí sestavovat. Hledání správné rovnováhy je zde velmi těžké.

Wolf [72] upozorňuje, že se nacházíme v zajetí rozporuplné technologické kultury, která nás neochraňuje před potenciálními katastrofálními haváriemi a ani neakceptuje jejich následky, ba dokonce ani rostoucí počet havárií a jimi vyvolaných ztrát nás nepřinutí vzdát se nových a riskantních zařízení, které reprezentují technologický pokrok. Prospěch z technologie obyčejně přichází společně i s nevýhodami a společnost není ochotná žít bez mnoha z těchto bonusů. Jestliže je tento předpoklad správný, potom se proces přesného určení toho, jaké systémy budovat, a které technologie v nich používat, stává kritickým.

Existuje několik způsobů pro podobné rozhodování. Jedním extrémem je „anti-technologická“ pozice, která svaluje vinu za havárie jen na technologii a udává, že moderní technologie nesmí být používána v nebezpečných systémech. Tento jednoduchý a negativní postoj není řešením komplexních inženýrských a etických problémů. Opačným extrémem je pro-technologická pozice, která považuje každou novou technologii za dobrou. Tvrdí, že jestli se něco dá udělat, pak se to udělat musí. Ti, kteří zastávají tento názor, často přisuzují vinu za havárie lidem a předpokládají, že rizika budou redukována výměnou počítačů místo operátorů. Tento postoj je také velmi zjednodušující.

Převládajícím postojem naší společnosti je prospěchářství. Za jedinou smysluplnou cestu, jak se rozhodovat mezi technologií a rizikem, považuje prospěchářství použití analýzy rizika a užitku/zisku (risk-benefit analysis). Toto přesvědčení je tak rozšířené, že zpravidla akceptujeme analýzu “riziko-užitek“ jako jedinou cestu pro rozhodování u technologie a rizika, aniž bychom připouštěli i jiné alternativy.

1.4 Risk-zisk analýza a její alternativy

Podle utilitaristů jsou katastrofální havárie, jako např. havárie v Bhopalu, riziky moderních technologií, které se z dlouhodobého hlediska vyváží získaným užitkem. Rozhodnutí proto mohou být provedena na základě porovnávání rizik a zisků, spojených s využíváním moderních technologií.

Abychom se mohli takto rozhodovat, musíme být schopni (1) měřit riziko a (2) vybrat odpovídající úroveň rizika vzhledem k jeho akceptovatelnosti. Bohužel, měřit přesně riziko není možné, obzvlášť předtím, než je systém hotový. Pokud systém není navržen a zkonstruován, znalosti o jeho rizicích nejsou kompletní nebo ještě ani neexistují. Dokonce i kdyby mohlo být využito předchozích zkušeností, nemusí tyto být validním prediktorem budoucího rizika, snad jen tehdy, pokud by systém a jeho okolí zůstaly statickými. Už i malé změny v systému, resp. v jeho okolí mohou podstatně změnit potenciální riziko systému.

Toto dilema se pokouší řešit odhadování rizika. Cílem je kvantifikovat riziko včetně pravděpodobnosti výskytu a velikostí ztrát před tím, než jsou k dispozici historické údaje. Přesnost takových odhadů rizika je kontroverzní. William Ruckelshaus [60], bývalý šéf agentury pro životní prostředí USA tvrdí, že údaje z odhadů rizika jsou běžně používány jako určitý druh záminky. Říká: „Abychom se vyhnuli paralýze vyplývající z čekání na definitivní

údaje, předpokládáme, že máme větší znalosti, než mají v současnosti vědci a děláme rozhodnutí na základě takovýchto předpokladů."

Ve skutečnosti odhadování rizika nemůže nikdy poskytnout definitivní odpovědi na tyto typy otázek o riziku. Odhady extrémně nepravděpodobných příhod, jako např. těžká havárie jaderného reaktoru, nemohou mít stejnou vědeckou validitu jako odhady událostí, pro které existují bohaté statistiky. Protože jsou požadované pravděpodobnosti těžké havárie na reaktorech tak malé (např. až 10^{-7} rok^{-1}), prakticky není možné předurčit takový výskyt událostí přímo - postavením tisíce reaktorů, jejich provozováním po dobu 10 000 roků a soustavným zaznamenáváním jejich provozní historie.

Místo udávaného přímého určení jsou těžké havárie vypočítávány pomocí konstruování modelů interakcí událostí, které k těmto haváriím mohou vést. V praxi jsou brány v úvahu jen ty události, které můžeme hodnotit. Zároveň jsou však přítomny i příčinné faktory, které jsou většinou neměřitelné a podílely se téměř na všech velkých haváriích. Pravdou zůstává, že technika odhadování rizika je kontroverzní a výsledky mají daleko k tomu, aby mohly být univerzálně akceptovány jako smysluplné.

Avšak i v případě, že by riziko bylo možno měřit, zůstává problém výběru úrovně rizika. Nejčastěji používaným kritériem je tzv. akceptovatelné riziko. Spočívá v tom, že se vybere prahová úroveň, pod kterou jsou všechna rizika tolerovatelná. Kdo však určí, jaká úroveň rizika je akceptovatelná v porovnání s možným ziskem? Mnohokrát ti, kteří z toho mají užitek, jsou těmi, kteří rizika předvídají. Tento přístup lze nalézt také při hodnocení běžných pracovních rizik. Lidé, kteří jsou rizikem negativně ovlivněni, jsou jen málokdy dotazování na svá mínění, obzvláště tehdy, jestliže nemají zastoupení ve vlivných lobbystických skupinách nebo odborových sdruženích. Postoj těch, kteří rozhodují, se dobře odráží ve vyjádření ředitele Electricité de France, který vysvětlil francouzské tajemství o jaderné energetice takto: „Nebudete se radit s žábami, když jim vysušujete močál". Navíc kromě technických problémů přináší prospěchářství a risk-zisk analýzy mnoho filosofických a etických dilemat.

Příkladem morálních důsledků risk-zisk analýzy je případ s palivovými nádržemi u automobilu Ford Pinto. Ford věděl o nebezpečí exploze palivových nádrží při srážce. Avšak na základě provedených risk-zisk analýz, při kterých byly náklady na zvýšení odolnosti nádrže vůči nárazu a škody odhadnuty podle tehdy platného zákona pro smrtelné úrazy, se společnost rozhodla, že pro ni bude lacinější zaplatit zákonem požadované náklady za úmrtí než zvýšit odolnost palivové nádrže. Zisk v tomto případě měl Ford a rizika (nepeněžitá) byla přenesena na řidiče a cestujícími v autech Ford Pinto, kteří je takto museli nevědomky přijmout.. Admirál Bobby Inman [36] poukázal po havárii Challengeru v r. 1986 na to, že: „Je rozdíl mezi riziky, která podstupujeme z nevědomosti a riziky, která jsme přijali na základě snížení nákladů". Perrow [52] tvrdí, že konečným problémem není riziko, ale moc - moc přenést riziko na jiné při současném finančním profitu.

Dalším morálním problémem risk-zisk analýz je výběr společné měrné jednotky pro porovnávání ztrát a přínosů. Obyčejně se za takovouto jednotku stanovuje dolar. Tento výběr vyvolává otázku, jestli se na lidské utrpení můžeme dívat jako na náklady a jestli mu můžeme přiřadit dolarovou hodnotu, přičemž dalším problémem zůstává, jak toto přiřazení provést. Nejčastěji se toto dělá tak, že se vypočítá množství peněz, které by mohla postižená osoba vydělat od momentu jejího úmrtí do statisticky předpokládané doby její přirozené smrti. V tomto případě je mladý, zdravý a dobře vydělávající člověk cennější než mladý člověk s malým příjmem nebo než starší osoba, která je blízko důchodovému věku. Morální problémy takového přístupu jsou zjevné. Ovšem cenu lidského života jako takového vyjádřit nelze.

Pro používání akceptovatelného rizika jsou navrhovány různé alternativy. Optimální riziko zahrnuje srovnávání, kterým se minimalizuje součet všech nevyhnutelných dopadů. Optimálního rizika je dosaženo tehdy, když nárůst nákladů, resp. marginální náklady na redukci rizika se rovnají marginálním redukcím ve společenských nákladech, tj. když celkové náklady na snížení rizika a očekávané ztráty z rizika jsou minimální. Odhadování očekávaných ztrát však stále vyžaduje pravděpodobnostní odhady havárií a škod.

Perrow v knize Normální havárie (Normal Accidents) [52] předkládá model rozhodování, podle něhož lze dosáhnout omezení potenciálu pro havárie s velkými ztrátami na životech a současně minimalizovat efekty pomocí vyloučení technologií s vysokým rizikem. Tento model používá katastrofického potenciálu a nákladů na alternativy, aniž by potřeboval pravděpodobnostní vyjádření. Perrow považuje havárie za normální, a proto ve složitých systémech nevyhnutelné. V souladu s tímto chápáním musíme předpokládat, že k haváriím dojde a podle toho se i rozhodovat a ne předpokládat, že se havárie nestanou na základě odhadů jejich nízkých pravděpodobností.

Perrow rozděluje systémy s vysokým rizikem do tří kategorií. Do první kategorie patří ty systémy, které mají buď nízký katastrofický potenciál nebo vysoce nákladné alternativy, jako např. chemické továrny, letectví a letecká doprava, přehrady, doly a automobily. Tyto systémy je nutno tolerovat a nadále zlepšovat s přijatelným úsilím. Druhá kategorie zahrnuje technologie s ne příliš velkým katastrofickým potenciálem a s ne příliš velkými náklady na alternativy. Jsou to systémy či zařízení, bez kterých si neumíme některé činnosti představit (např. námořní doprava), nebo kde jsou očekávané přínosy podstatné (např. rekombinace DNA). Perrow navrhuje, aby tyto systémy byly pod co nejpřísnější kontrolou. Poslední kategorie zahrnuje systémy s vysokým katastrofickým potenciálem a s relativně levnými alternativami. Do této skupiny zařazuje jaderné zbraně a jadernou energetiku a dokazuje, že systémy z této kategorie by měly být odstaveny a odstraněny.

Problémem tohoto přístupu je, že neříká, jak se máme rozhodovat u konkrétních systémů. Věnuje se jen širokým třídám systémů. Alternativou je požadavek, aby se při použití nové technologie nezvýšil výskyt havárií. Například, když se havárie v určitém specifickém typu systémů vyskytovaly s určitou historickou četností, mělo by se potom při zavádění nové technologie požadovat, aby četnost výskytu havárií byla ekvivalentní té, která se považuje za akceptovatelnou. Tento přístup se zakládá na přesvědčení, že jestli veřejnost běžně akceptovala technologii s určitou frekvencí výskytu havárií, bude takovou frekvenci akceptovat i v budoucnosti.

Nehledě na technické problémy určování ekvivalence frekvence havárií v nových systémech, vystupují znovu závažné morální problémy tehdy, když nová technologie může snížit výskyt havárií jen za cenu změn a vyšších nákladů. Z etického hlediska se v těchto případech nedá mluvit o ekvivalentní bezpečnosti. Podívejme se na airbagy a jiná zlepšení bezpečnosti automobilů v současnosti. Za předpokladu, že akceptovatelné riziko je takové, jaké bylo veřejností přijímáno dosud, nejsou taková zlepšení nutná, pokud lidé zjevně akceptují současné riziko svou ochotou jezdit. Používání počítačů může nabízet široký potenciál zvýšení bezpečnosti, ale zároveň i dovoluje snížit bezpečnostní rezervy. Jejich použití proto zabezpečuje možnost ekonomického nárůstu nebo zvýšení produktivity. Při zachovaní stejné historické úrovně bezpečnosti zůstává otázka, zda musí být ekvivalentní úroveň rizika akceptováno, když je riziko možné redukovat. Nebo ještě hůře, opravdu redukují počítače riziko v takové míře, v jaké se předpokládá při rozhodování se o jejich nasazení? Ukazuje se, že nemáme úplně spolehlivé postupy pro takováto rozhodnutí. Částečným vysvětlením pro mezery matematických a inženýrských řešení je skutečnost, že výsledná rozhodnutí zahrnují hluboké filosofické a morální otázky a nejsou jen jednoduchými technickými výběry.

2 HIERARCHICKÝ MODEL KAUZALITY HAVÁRIÍ

Abychom byli schopni poradit, jakými způsoby lze zabránit vzniku havárií, musíme nejprve vědět, čím jsou havárie zapříčiněny. Determinování příčin havárií je složitější, než si často představujeme. Známe mnoho kategorií příčin: bezprostřední příčiny, pravděpodobné příčiny, kořenové příčiny, přispívající příčiny, relevantní příčiny, přímé/nepřímé příčiny, významné příčiny apod. Dříve, než se podíváme na to, co způsobuje havárie, považujeme za nutné objasnit, co vlastně slovo příčina znamená.

2.1 Pojem příčinnosti

Zamysleme se nad následující rekapitulací jevů, kterou uvedly jedny francouzské noviny:

Zámořská loď Baltic Star, registrovaná v Panamě, narazila v husté mlze plnou rychlostí na dno u pobřeží jednoho z ostrovů u Stockholmu. Dodatečnou analýzou byly identifikovány tyto události: jeden z kotlů praskl, ovládání kormidla reagovalo pomalu, kompas byl špatně nastaven, kapitán šel do podpalubí telefonovat, námořník vykonávající službu pozorovatele na můstku měl přestávku na kávu a řídící důstojník vydal v angličtině chybný příkaz kormidelníkovi, který mu mohl jen těžko rozumět, protože uměl pouze řecky.

Složitost podmínek a jevů přispívající k této havárii není až tak neobvyklá. Neobvyklé bylo pouze úplné přešetření přispívajících faktorů na rozdíl od běžného určení jedné příčiny, např. v tomto případě mlhy, nebo chyby člověka, bez zvážení ostatních faktorů. Ale ani tak rozsáhlé detailní vyšetřování nevzalo v úvahu širší organizační, nebo sociologické faktory, jako je velký tlak na kapitána lodi, aby dodržoval co nejpřesněji stanovený časový rozvrh, protože hrozí finanční ztráty z pozdějšího příjezdu do přístavu. Tyto faktory se staly důležitými složkami rozhodování posádky při práci. Tento tlak mohl vést k nedostatečné opatrnosti při zvažování nebezpečí mlhy.

Některé havárie jsou tak složité a propletené neurčitostmi, že nepřipouštějí jakékoliv jednoduché vysvětlení příčin, nebo dokonce i vyčerpávající zjištění všech působících faktorů. Např., způsobení tragického úniku metylisokyanatu (MIC) v Bhopalu bylo vedením podniku přiřčeno chybě člověka, kterou bylo napuštění vody do zásobníku MIC z nedostatečně vyčištěného potrubí. Pohled na podmínky, za kterých byl závod veden, však jasně upozorňoval na to, že k havárii musí dříve nebo později dojít bez ohledu na to, zda a jak se voda do zásobníku dostane: Ať by se voda dostala do zásobníku jakkoliv, nemohla by způsobit těžkou explozi, kdyby nebyla odpojena chladící jednotka a nebyl z ní vypuštěný freon, kdyby měřící a signalizační zařízení fungovalo správně a monitorovalo výrobní proces, kdyby byla učiněná vhodná opatření hned při prvním ucítění MIC místo odkladu jejich provedení až po svačinové pauze, nebo kdyby pračka plynů byla v provozu, nebo kdyby venkovní vodní sprchy byly navrženy tak, aby byly účinné do dostatečné výšky, nebo kdyby věž na spalování emisí byla funkční a měla dostatečnou kapacitu pro likvidaci velkých úniků.

Byl souběh všech těchto chyb a nedostatků celého bezpečnostního mechanismu jen jedinečnou náhodou, která se přihodí pouze jednou za dobu životnosti? Při povrchním pohledu se zdá neuvěřitelné, že by mohly současně selhat pračka plynů, spalovací věž, vodovodní odpad, chladící jednotka a různá měřící a signalizační zařízení. Bližší pohled nám však ukáže úplně jiný obraz.

Není nijak výjimečné, že se v podnicích odstaví pasivní bezpečnostní zařízení, kterými jsou např. chladící jednotky proto, aby se uspořilo, nebo že měřící a signalizační technika je často nefunkční. V továrně v Bhopalu bylo v kritické lokalitě více výstražných a bezpečnostních zařízení, která měla upozornit operátory na abnormální situaci. Mnoho limitních (prahových) úrovní pro výrobu a ochranu dělníků před MIC bylo v Bhopalu běžně překračováno. Dělníci tvrdili, že nebylo výjimkou nechat MIC v zásobní nádrži, což odporovalo bezpečnostním normám. Provozní předpisy nařizovaly, že chladící jednotka musí být v provozu vždy, když je MIC v systému. Tato chemikálie musí být udržovaná na teplotě, která nepřekročí 5 °C, aby nedošlo k nekontrolovatelným reakcím. Varovný signál oznamující vysokou teplotu měl zaznít při dosažení 11 °C. Chladící jednotka byla přesto odstavena a MIC byl běžně skladován při teplotách okolo 20 °C. Vedení podniku změnilo práh havarijního signálu na interval od 11 °C do 20 °C, čímž se vyloučila možnost včasného varování růstu teploty.

I další ochranná zařízení v podniku měla neadekvátně nastaveny prahové úrovně. Zmiňovaná pračka ventilačních plynů, i kdyby pracovala, byla navržena na neutralizaci jen malého množství plynu při nízkých tlacích a teplotách. Tlak unikajícího plynu během havárie překročil projektové hodnoty pračky přibližně dvaapůlkrát a jejich teplota byla vyšší asi o 80 °C, než dovoloval provoz pračky. Podobně věž na spalování unikajících par byla zcela neadekvátní pro zvládnutí odhadovaných 40 tun MIC, které unikly během havárie. Výstražné systémy (alarmy) pro různé účely bylo v továrně slyšet 20 až 30krát za týden, což vedlo k tomu, že při aktuálním alarmu nebylo možné rozlišit, zda je běžný, nebo vyhlašuje skutečný poplach. Bylo ironií, že se výstražné sirény nespustily po dobu dvou hodin poté, co byl detekován únik MIC a potom se spustily pouze na dobu 5-ti minut v souladu s bezpečnostní politikou společnosti. Navíc se ukázalo, že chování zaměstnanců po vyhlášení poplachu nebylo dostatečně nacvičeno v rámci přípravy na krizové situace. Když bylo nebezpečí během úniku oznámeno, mnoho zaměstnanců běželo z kontaminovaných částí továrny a zcela ignorovali autobusy, které stály připravené vedle budov. Směnoví dělníci měli jen minimální ochranné prostředky, např. nedostatek kyslíkových masek se objevil ihned v začátku havárie a většina zaměstnanců neměla žádné znalosti a výcvik, jak se chovat při mimořádných událostech.

Když začal únik MIC, policie nebyla informována. Když policie a novináři telefonovali mluvčímu podniku, ten nejdříve popřel, že došlo k havárii a později pak prohlásil, že MIC, který unikl, nebyl nebezpečný. Okolní obyvatelstvo nebylo před nebezpečím varováno před a ani během úniku a nebylo informováno o jednoduchých ochranách (jakou by byl např. vlhký šátek přiložený na tvář), které mohly ochránit před nadýcháním uniklé chemikálie. Kdyby bylo obyvatelstvo upozorněno a byly by mu poskytnuty jednoduché rady, mohlo být zachráněna většina ztracených životů.

Uvedené příklady částečně ilustrují složitost přiřazování příčin haváriím. Filosofové rozebírají pojem příčinnosti už celá století. Příčina musí předcházet účinek, který je na ní závislý, ale podmínka nebo jev může předcházet jinému jevu bez toho, aby ho způsoboval. Navíc, podmínku můžeme považovat za příčinu jevu i tehdy, když k ní nedojde vždy, když je daná podmínka splněna. Řízení v opilosti se např. považuje za příčinu havárií, ale být opilým během jízdy autem neznamená vždy způsobit havárii. Tento typ souvislosti je např. mezi kouřením a rakovinou plic.

Johan Stuart Mill [47] definoval příčinu jako postačující množinu nutných podmínek. “Příčina je celkovou sumou podmínek pozitivních i negativních dohromady, celek nahodilostí ze všech určení, které když nastanou, tak dojde k jednoznačnému následku.“ Např. požár vyžaduje hořlavý materiál, zdroj ohně a kyslík. Každá z těchto tří podmínek je nutná, ale jen všechny dohromady jsou postačující. Příčinou je potom současný výskyt všech tří pod-

mínek a ne pouze jedné z nich. Rozlišování mezi postačující a nutnou podmínkou je podstatné. Nějaká událost může být vyvolána pěti podmínkami, přičemž první a druhá z nich, jestliže se vyskytnou najednou, mohou vyvolat patřičný účinek a třetí, čtvrtá a pátá, jestliže se vyskytnou společně, ho mohou vyvolat také. V tomto případě jsou dvě příčiny (množiny podmínek postačujících ke vzniku jevu). Obě jsou tvořeny postačujícími množinami nutných podmínek.

V této studii budeme pod příčinami událostí rozumět množiny podmínek, ze kterých je každá pro vznik předmětné události nevyhnutelná, a které jsou společně pro vznik předmětné události postačující. Individuální podmínky budeme nazývat kauzálními podmínkami/ přispívajícími faktory, nebo podmínkami/faktory nebezpečí, abychom je odlišili od příčin událostí (havárií). Interpretace určení souvisejících s příčinou havárie je nutno provádět velmi pozorně.

2.2 Subjektivita při popisování příčinnosti

Popisy příčin havárií často zahrnují subjektivitu a filtrování. Pouze ojediněle jsou příčiny havárií vnímány identicky vedením společnosti, inženýry, představiteli odborů, operátory, zaměstnanci pojišťoven, soudci, policisty, novináři, státem a v neposlední řadě i oběťmi. Bogard [8] tvrdí, že každá specifikace možných příčin havárií bude nevyhnutelně nést znaky střetu zájmů. Některé podmínky mohou být považovány za nebezpečné jednou skupinou, přičemž druhá skupina je má za perfektně bezpečné a nevýznamné. K takovýmto střetům dochází často v situacích, při kterých jsou potřebná normativní, etická a politická posouzení. Navíc, rozhodnutí o příčině havárie mohou být ovlivněná hrozbou možných soudních sporů.

Opravdu, každý dotazovaný člověk může přisoudit k dané havárii různou příčinu. Jedna studie ukázala, že dělníci, kteří byli spokojeni se svou prací a byli začleněni do podnikání, přisuzovali událostem hlavně osobní příčiny. Naopak, nespokojení pracovníci, kteří měli na podnikání jen malý podíl, uváděli daleko častěji neosobní příčiny, které dokazovaly, že za události odpovídá podnik. V jiných studiích byly nalezeny rozdíly mezi určováním příčin havárií oběťmi, manažery bezpečnosti a vrcholovými manažery. Dalším faktorem subjektivity může být pracovní postavení v organizaci. Čím nižší je postavení, tím větší je tendence svádět události na faktory spojené s organizací a naopak, jednotlivci, kteří mají vysoké postavení v hierarchii, mají tendenci obviňovat podřízené. To odporuje údajům z hlášení o skoronehodách (near-miss), která dokazují, že příčinami vzniklých událostí jsou v převážné míře technické a organizační závady. Na základě přezkoumání mnoha havarijních rozborů Leplat [38] uvádí, že určení příčiny závisí na určitých charakteristikách oběti a analýze (hierarchické postavení, míra zainteresovanosti a spokojenost s prací) a dále na vztazích mezi obětí a analytikem a na stupni závažností havárie.

Identifikování příčiny může být dále ovlivněno i metodami sběru dat. Většinou jsou údaje o haváriích shromažďovány ve formě textových popisů časového průběhu události s tendencí soustřeďovat se na běžné okolnosti bezprostředních (proximálních) jevů, tj. těch, které časově těsně předcházely vzniklé události. Na jedné straně, formuláře pro zaznamenání jevů, které jsou předem připraveny 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 zvažovány při vyšetřování příčin události.

Jak se dalo očekávat, údaje o haváriích jsou často systematicky filtrovány a bývají nespolehlivé. Leplat tento jev vysvětluje tím, že mentální model havárie, který má analytik ve své mysli, způsobuje, že si zapamatuje nebo vezme v úvahu jen ty faktory, které jsou v souladu s jeho mentálním modelem havárie.

Havárie mohou být popsány formou řetězců jevů/faktů, cílů nebo motivů. Na vysvětlení uveďme příklad připravený Leplatem. Jde o havárii, která se stala, když chodec prudce vstoupil na chodník a upadl na dlažbu. Toto vysvětlení se skládá z popisu základního řetězce jevů, které vedly k nehodě. Vysvětlení, založené na cílech, by mělo zahrnovat fakt, že se k chodci velmi rychle přibližovalo auto a on chtěl být co nejdříve na chodníku. Vysvětlení, založené na motivech, by mělo popsat okolnosti rychlého přibližování auta a snahu chodce vyhnout se mu. Pokud základní řetězce faktů nejsou zpravidla předmětem sporné interpretace, vysvětlení, která zahrnují cíle a motivy, budou ovlivněna mentálním modelem a postoji analytika.

Sumárně můžeme na základě uvedeného konstatovat, že příčinné faktory, vybrané pro konkrétní havárii, mohou být do velké míry subjektivní a musí být proto vždy interpretovány s velkou opatrností.

2.3 Nepřiměřené zjednodušování při určování příčinnosti

Dalším problémem při identifikování příčin havárií je nepřiměřené zjednodušování. Mnohokrát se při velkých haváriích zdůrazní pouze některé faktory jako příčiny, přestože 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 apod. Ani jeden z těchto faktorů není dostatečnou příčinou smyku, ale jakýkoliv z nich bude často uváděn jako jediná příčina smyku. Určitá podmínka/faktor může být vybrána 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. Např. při havárii letadla DC-10 americké společnosti American Airlines v Chicagu v roce 1979 byla vina přisouzena jen chybě při údržbě a ne konstrukční chybě, která dovolovala hýbat ovládacím táhlem i při poškození křídla. Díky tomuto přehlédnutí nebyl výrobce McDonnell Douglas požádán o změnu konstrukce, která nadále představovala nebezpečí.

Společným typem přílišného zjednodušování je úřední, formálně zákonný přístup, kterým se havárie připisují jen selháním člověka, nebo technickým chybám, přičemž se ignorují organizační faktory a hledají se jednoduché zjevné příčiny.

Právnický přístup k příčinnosti

Právníci a pojišťovací agentury často příliš zjednodušují příčiny havárií a obyčejněidentifikují bezprostřední resp. přímou (proximate) příčinu havárie. 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. Takovéto určování může být ovlivněno platební schopností zúčastněných stran nebo politickými úvahami.

Všeobecně neexistuje žádné objektivní kritérium pro upřednostnění jednoho faktoru před druhým, které se podílely na havárii. Právnický přístup ke kauzalitě má výhodu jen pro určení viny a zodpovědnosti. Pro technický pokrok, kde 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 ignorována.

Haddon [20] dokazuje, že opatření proti haváriím nemají být určována podle relativního významu příčinných faktorů. Naopak, prioritní musí být taková opatření, která budou co nejefektivněji redukovat ztráty. Zjednodušené vysvětlení havárií často neposkytuje nevyhnutelné informace pro zabránění dalším haváriím v budoucnosti a kromě důvodů souvisejících s odpovědností, je vynakládání času na určení relativních příspěvků jednotlivých faktorů k haváriím neproduktivní.

Selhání člověka

Nejčastěji se vyskytujícím přílišným zjednodušením je podle zpráv o haváriích svalení viny na člověka (operátora, pilota, řidiče apod.). V každém systému, do kterého je včleněn člověk, může být hypoteticky příčina havárie vždy přiřazena člověku, ať už za jeho zásahy, nebo za nedostatečnou prevenci havárií. I v těchto případech, když je chyba člověka bezprostředně spojená s havárií, je chybou považovat člověka za jedinou příčinu havárie 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. Dobrým příkladem pro to je řešení nehod, k nimž docházelo při spojování železničních vagónů posunovači. Manažeři železnic vždy tvrdili, že příčinou smrtelných úrazů posunovačů při uváděné práci jsou jejich chyby a nedbalost a oni nemohou dělat víc, než jim domluvit, aby byli při práci pozornější. Nakonec do tohoto problému vstoupila vláda a nařídila, aby bylo na vagónech nainstalováno automatické spojovací zařízení. Výsledkem bylo, že počet smrtelných úrazů posunovačů na dráze se od té doby výrazněsnížil.

Všeobecně bývá jako příčina havárií udáváno selhání člověka. Analytici často zastaví rozbory při nalezení konkrétní chyby člověka a nevěnují náležitou pozornost jiným nevyhnutelným okolnostem, které musely spolupůsobit, aby této k chybě došlo. Protože můžeme o každé havárii říci, že ji způsobila chyba člověka, je takováto fráze demotivující pro konstruktivní přístup k akcím potřebným pro zabránění opakovaným selháním člověka. Je velmi jednoduché říci někomu: „Buď opatrnější.“ Bude vhodnější přestat se zjišťováním, jestli chyba člověka byla příčinou havárie a místo toho začít zkoumat prevenci proti selháním člověka.

Tendence obviňovat člověka za chybu je starého data. Převládala v dobách, kdy technologie výroby nebyla tak složitá, ale bohužel se ukázalo, že stále přežívá. Jedním z původců tohoto pohledu na příčiny nehod je teorie náchylnosti k nehodám, která se snažila dokázat, že za většinu nehod je odpovědný malý počet jednotlivců (i v tomto případě lze uplatnit Paterovo pravidlo 20/80). Navzdory četným studiím, které ukázaly, že je málo statistických dokladů pro tuto myšlenku, tento názor přetrvává zejména v tradičním průmyslu. Jiným prvkem v důrazu na odpovědnost jednotlivců-nehodářů je shora zmíněná legální dimenze při mnoha šetřeních nehod, která se často zaměřuje na hledání viníka pro určení náhrady škod, spíše než na identifikaci možných systémových příčin chyb.

Zdůraznění individuálních faktorů při vzniku nehod se odráží i v přístupu k jejich prevenci - zdůrazňuje se výběr, výcvik a přístup motivační a disciplinární k snižování nehod a chyb. Hlavní důraz je kladen na modifikaci chování pomocí přesvědčování (motivační kampaně) či trestání. Dalším rysem je zaměření na výběr jedinců podle výběrových kritérií, které mají zaručit, že vybraní lidé si budou při práci počínat svědomitě, ukázněně a budou schopni provádět činnost bezpečně, efektivně a úspěšně.

Základním předpokladem je, že jedinec má vždy volbu, zda se bude či nebude chovat nebezpečným způsobem. To ve svém důsledku znamená, že odpovědnost za prevenci

nehod nese v konečném důsledku pracovník. Vede to též k názoru, že pokud se management pokusil přesvědčit pracovníky, aby se chovali odpovědně, poskytl výcvik v bezpečných metodách práce a poskytl patřičné pomůcky, pak učinil vše pro prevenci nehod. Jestliže tato opatření selžou, jediným způsobem je disciplinární akce a konečně i propuštění pracovníka.

Není pochyb o tom, že výcvik, obzvláště specifický, k úkolům je extrémně důležitý jako pokus o snižování lidských selhání. Nicméně některé podniky pokládají problém lidských chyb za záležitost většinou pouze výcviku. Tam, kde faktory jako špatný design nebo nedostatečný management nejsou rozpoznávány, není výcvik účinný. I nejlépe školený pracovník pociťuje potíže, když se setká s komplikovaným problémem, špatně konstruovaným interface člověk-stroj, s nereálnými úkoly, s velkou pracovní zátěží a s neklidným prostředím (hluk, přerušování, stres). Žádný rozsah výcviku nemůže tyto nedostatky odstranit. Výcvik proto musí být zaměřen na základní příčiny chyb a nikoli pouze na jejich dílčí aspekty.

Přístup preferující disciplinární přístup je úzce spjat s filosofií motivačního přístupu. Z praktického hlediska je pro jedince dostatečným motivem to, aby nebyl přistižen a potrestán. Z filosofického hlediska se zdá nespravedlivé obviňovat člověka za nehodu tehdy, byla-li zapříčiněna faktory, které jsou mimo jeho kontrolu. Nerozumí-li pracovník špatně napsaným postupům anebo je-li zařízení špatně konstruováno, takže je velmi obtížné je ovládat bezchybně, pak potrestání jedince bude mít malý efekt na zamezení toho, aby se toto selhání opakovalo.

Zkoumání mnoha katastrof ukázalo, že základní podmínky selhání lze často vystopovat až k nevhodné politice podniku. Disciplinární akce mohou být vhodné tehdy, byly-li vyloučeny jiné příčiny, a kde jedinec porušil předpisy bez dobrého důvodu. Nicméně studie naznačují, že disciplinární akty byly z dlouhodobého hlediska neúčinné při snaze zvýšit používání osobních ochranných prostředků. Hlavním důvodem proti disciplinárnímu řízení je dále i to, že vytvářejí strach a zabraňují volnému toku informací o základních příčinách nehod. Pak je strach motivem pro to, aby se skoronehody či menší prohřešky skrývaly.

Vzhledem k předpokladu, že jednotlivci si mohou volit bezpečné formy chování sami, tradiční přístup naznačuje, že veškeré lidské chyby proto zasluhují výtku (za předpokladu, že správné chování bylo předmětem výcviku, a že jednotlivec proto ví, co je požadováno). To má řadu důsledků. Potlačuje jakékoli úvahy o alternativních příčinách jako jsou nepřiměřené pracovní postupy, výcvik či design zařízení a nepodporuje zkoumání základních příčin, které mohou být mnoha nehodám společné. Vzhledem ke konotaci výtek a obviňování spojených s výskytem chyb proto existují silné podněty k tomu, aby pracovníci skrývali incidenty či skoronehody, i když jsou zaviněny podmínkami, nad kterými nemají kontrolu. To znamená, že informace o podmínkách vedoucích k chybám, se nedostanou k manažerům, kteří mají pozici k prosazení nápravných akcí jako jsou například konstrukční a designové úpravy zařízení, zlepšený výcvik anebo změna pracovních postupů. Místo toho se téměř výlučně spoléhají na metody k manipulaci chování a vylučují tím jiné přístupy.

Tradiční přístup nepovzbuzuje úvahy o podstatných (kořenových) příčinách či mechanismech chyb. Proto systémy sbírání informací o nehodách se soustřeďují na charakteristiky jedinců, kteří mají nehodu a ne na další možné přispívající systémové příčiny jako jsou nepřiměřené postupy, nesprávný design úkolů a nedostatky v komunikaci. Stručně řečeno, podle tradičních názorů postačí najít konkrétního člověka jako viníka nehody a není třeba uvažovat o tom, jaké (polehčující) okolnosti mohly k nehodovému chování přispívat. Tím se úvaha zastavuje na poloviční cestě.

Úspěchy tradičního přístupu byly z velké části získány v oblasti bezpečnosti práce, kde je statistická evidence snadno dosažitelná, a která se zabývá incidencí zranění jedinců

v oblastech jako je uklouznutí či pády. Tyto nehody jsou přístupné změnám chování, protože chování, které vedlo k nehodě, je pod kontrolou jedinců a lze je snadno předvídat. Povaha rizika je též obvykle předvídatelná a chování, jak se vyhnout nehodě, lze explicitně stanovit. Přístup do uzavřených prostor nebo zvedání těžkých břemen jsou případy, pro něž lze předepsat vzor správného chování.

V případě bezpečnosti procesuálního charakteru výroby není situace ale tak jasná. Zavedení počítačů velmi mění roli pracovníka na řešitele problému a rozhodovatele v případě mimořádných událostí. V této roli nedostačuje, aby pracovník byl cvičen a podmiňován v tom, aby se vyhýbal chování, které vede k nehodám. Je nezbytné, aby uměl pružně reagovat v široké škále situací, které nelze předem předvídat. Tuto flexibilitu získává pracovník tehdy, dostává-li se mu podpora od designérů systému z hlediska dobrého zobrazování informací, vysoce kvalitních postupů a důkladného výcviku.

Pokud jde o chyby vedoucí k nehodám v procesu, není vhodné klást vinu pracovníkovi za podmínky, které jsou mimo jeho kontrolu a které vedou k chybám. Tyto úvahy naznačují, že přístup zaměřený na změnu chování nemůže sám o sobě zamezit mnoha typům chyb.

Technické chyby

Významným přílišným zjednodušováním je i zaměření se jen na technické chyby a bezprostřední fyzikální jevy. Tento typ převládajícího úzkého zaměření může vést k přehlédnutí některých nejdůležitějších faktorů havárie. Např. při výbuchu v chemické továrně v Flixborough (Velká Británie) v červnu 1974, při kterém přišlo o život 23 lidí a škody dosáhly hodnoty 50 mil. dolarů, věnovali vyšetřovatelé většinu svého úsilí určování toho, které z dvou potrubí prasklo první. Britský Vyšetřovací soud, který tuto katastrofu vyšetřoval, rozhodl, že: „Katastrofu způsobil současný výskyt velkého počtu nepravděpodobných chyb v konstrukci a při instalaci modifikací zařízení továrny a je velmi nepravděpodobné, že se taková kombinace chyb může ještě někdy v budoucnosti opakovat.“

Ruptura potrubí představovala jen jednu z příčin této katastrofy. Pro úplné vysvětlení a ochranu do budoucnosti před takovými haváriemi je nutná znalost praktik managementu továrny ve Flixborough, jako například provoz závodu bez trvalé přítomnosti kvalifikovaného inženýra, svolení provádět důležité modifikace na zařízení nekvalifikovanému personálu, měnit inženýring bez náležitého vyhodnocení bezpečnosti a skladovat velké množství nebezpečných chemikálií v blízkosti nebezpečných částí závodu. Britský Vyšetřovací soud úzkoprse konstatoval, že “v továrně byly nepochybně určité nedostatky při dodržování bezpečnostních postupů, ale žádný z nich neměl nejmenší podíl na katastrofě a na jejich následcích a nemusíme proto s nimi dále ztrácet čas“. Naštěstí, ostatní nepřijali toto úzké hledisko a Flixborough provedl velké změny v souladu s tím, jak dnes mohou být provozovaná nebezpečná zařízení ve Velké Británii.

Organizační faktory

Velké technologické provozy a technické systémy jsou víc než sbírkou technických částí 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 vytvořeny. Havárie jsou často svalovány 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 téměř vždy, kořeny v organizaci - v její kultuře, managementu a struktuře. Všechny tyto faktory jsou kritické pro bezpečnost technických systémů.

Významnou podporu pro hypotézu o převážném vlivu vyjmenovaných organizačních příčin na vznik havárií představuje přehled výsledků zjištění z velkých havárií z posledního období. Hlubší, nezávislé rozbory havárií jednoznačně zvýrazňují organizační a manažerské nedostatky. Např. zpráva Kemenyho komise [32] o havárii v Three Mile Island (TMI) obsahuje 19 stran doporučení, ze kterých pouze dvě jsou věnovány technickým otázkám a sedmnáct z nich se dotýká problémů managementu, výcviku a nedostatků v institucích jaderného průmyslu. Závěrem komise je, že jaderný průmysl musí dramaticky změnit svoje postoje k bezpečnosti a doporučila, aby provozovatelé a dodavatelé byli nuceni stanovit přiměřené bezpečnostní normy, a aby systematicky sbírali, sledovali a analyzovali zkušenosti z provozu, plánovali změny v reálných termínech jejich provedení, integrovali odpovědnosti managementu, jasně definovali role a odpovědnosti, získali vysoce kvalifikovaný personál, věnovali větší péči a pozornost provozním předpisům a stanovili termíny vyřešení bezpečnostních problémů.

Ve studii o havárii raketoplánu Challenger [59] se konstatuje, že tato havárie měla kořeny v kumulaci organizačních problémů. Komise kritizovala přílišné sebeuspokojení managementu, byrokratické postupy, nezájem o bezpečnost a nedostatky v procesech rozhodování. Cituje různé organizační a komunikační chyby, které ovlivnily kritické rozhodnutí o startu raketoplánu dne 28.1.1986 včetně nedostatečných požadavků pro oznamování problémů, neadekvátní analýzy trendů výskytu poruch, chybné interpretace kritických míst, nedostatečné zdroje pro zajištění bezpečnosti, nedostatečné zapojení bezpečnostního personálu do diskusí a procesů rozhodování o bezpečnosti, neodpovídající autorita, odpovědnost a nezávislost bezpečnostních útvarů. Uvedené příklady nejsou ojedinělé. Ve většině velkých havárií z posledních 25 let byly technické informace o potřebné prevenci havárií dopředu známy a často i implementovány. Při každé havárii se však ukázalo, že technické informace a řešení byla kontaminována trhlinami v organizaci a managementu.

Multifaktoriální vysvětlení havárií

Všeobecně je nepravděpodobné, že kterákoli jednotlivá podmínka nebo faktor může být rozhodující, nebo dokonce postačující pro způsobení havárie složitého systému. Ve většině systémů, které byly konstruovány s náležitou péčí o jejich bezpečnost, budou havárie nebo ohrožení záviset na mnohonásobnosti příčinných faktorů a na složitých kombinacích podmínek technických, personálních, organizačních a sociálních.

Doklady lze nalézt v pečlivém provedení plánu výstavby Thermal Oxide Reprocessing Plant v Sellafieldu v Anglii. Významný anglický odborník v problematice lidské spolehlivosti Barry Kirwan [76] vytvořil tým odborníků, kteří pod jeho vedením spolupracovali s investory na vypracování plánu výstavby nového podniku na zpracovávání odpadu z atomových elektráren. Toto odvětví průmyslu je kritické jak z hlediska bezpečnosti, tak z hlediska lidského výkonu, to znamená, že provoz s sebou nese rizika pro veřejnost, a že bezpečný provoz podniku je silně vázán na lidskou práci. Hlavním cílem bylo zabránit jakémukoli významnému či katastrofickému selhání v budoucím podniku tam, kde k takovému selhání může dojít buď pro lidskou chybu, či nedostatečný pracovní výkon lidí, anebo pro jiný problém, kde by mohlo lidské jednání zabránit katastrofě. Dalším cílem bylo snížit chyby v bezpečnosti na minimum, zlepšit detekci chyb a obnovu systému lidmi, jakož i toleranci k chybám. Týká se to zejména radiologických rizik (dosažení kritických množství štěpného materiálu, únik kontaminace apod.). Výstavba závodu probíhala v létech 1987-1991, projekt bezpečnosti obsahoval následujících devět specifických oblastí:

1) Design interface – k zajištění ergonomických interface, tj. sdělovacích a ovládacích prvků v centrech řízení

2) Design procedur – k podpoře efektivních pracovních postupů

3) Metody výcviku – k vývinu efektivních výcvikových metod v nových a řídkých kritických úkolech

4) Údržba a testování – k zajištění, aby zařízení bylo udržovatelné a testovatelné z ergonomických perspektiv a k úvaze o riziku takových operací.

5) Personál a kvalifikace – k zajištění, aby byly k dispozici vhodné lidské zdroje pro normální i abnormální operace

6) Schopnost reagovat v nouzových případech – k zajištění, aby při řídkých událostech měli operátoři prostředky k zajištění bezpečné reakce a obnově stabilního stavu systému

7) Management – příspěvek managementu k snižování rizik. To byl nový prvek, jak naznačilo vyšetřování Černobylu, které vedlo k rozvoji nové oblasti – kultury bezpečnosti

8) Zpětná vazba a operační informace – k podpoře dodávání vyčerpávajících informací vyprodukovaných ve fázi designu do použitelné a praktické podoby pro budoucí operátory a manažery podniku, zajišťující to, že podrobné aspekty zůstanou v paměti podniku

9) Hodnocení rizik – analýza chyb v celém spektru operačních úkolů, které mohou ovlivňovat rizika – analýza úkolů a chyb a kvantifikace pravděpodobnosti lidských chyb, specifikace ukazatelů snížení chyb, včetně dokumentace a informací o bezpečnosti.

Plán výstavby byl skutečně realizován v roce 1992. Po více než deseti letech bezchybného fungování podniku však došlo na podzim 2005 k havárii, při níž došlo k úniku radioaktivního materiálu do okolí podniku. Tento případ dokazuje, že ani pečlivé uvážení všech myslitelných bezpečnostních aspektů ve fázi plánů na výstavbu podniku nedokáže zabránit možným haváriím v budoucnu. Tato výtka neznamená, že by systémový přístup ve fázi projekce byl nadbytečný či nevhodný, ale že řízení podniku nesmí podlehnout bezstarostnosti, že je vše dobře zajištěno a polevit v ostražitosti vzhledem k možným trhlinám z hlediska bezpečného provozu.

Vysoká frekvence havárií, které měly komplexní příčiny, vyplývá pravděpodobně ze skutečnosti, že konkurenční organizační struktury a inženýring eliminují jednodušší příčiny. Pozitivní je, že obrovská složitost havarijních procesů znamená, že je možné najít mnoho příležitostí zasáhnout včas, nebo je eliminovat. Proto průřezové zvažování všech podmínek vedoucích k haváriím bude mnohem užitečnější, než zjednodušující vysvětlení.

2.4 Hierarchický přístup ke kauzalitě

Přestože je jasné, že havárie mají pouze výjimečně jednoduché příčiny, specifikace všech nevyhnutelných podmínek (včetně těch věcí, které absentovaly při zabránění havárií) může být nepraktické. Zkoumání příčin a příčinných podmínek bývá obvykle ovlivňováno cíli vyšetřování. Jestliže je cílem zabránit budoucím haváriím, musí se vyšetřování provést na vícerých hierarchických úrovních z hlediska technického, z hlediska faktorů chování člověka a z hlediska organizace a dozoru.

Lewycky [42] navrhl tříúrovňový hierarchický model pro pochopení havárie (1. úroveň - mechanizmus, 2. úroveň -podmínky/faktory, 3. úroveň -omezení/požadavky). Je to zevšeobecněná struktura kauzality u havárií, kde nejnižší úroveň popisuje mechanizmus havárie, tj. základní řetězce jevů/událostí, např. řidičprudce zabrzdil, auto dostalo smyk a narazilo do stromu; řidič byl při nárazu vymrštěn z auta a zraněn.

Druhá úroveň chápání příčinnosti havárie zahrnuje podmínky/faktory, resp. nepřítomnost podmínek, které dovolily, aby k událostem popsaných na první úrovni mohlo dojít. Např. řidič nevěděl, jak předejít smyku, nebo jak ho zarazit; auto nebylo vybaveno antiblokovými brzdami; řidič jel příliš rychle, silnice byla mokrá od deště a proto byla adheze snížená; před autem se náhle objevil nějaký předmět a řidič musel rychle zabrzdit; řidič neměl zapnutý ochranný pás; ochranný pás byl poškozený a pod. Na této úrovni mohou být zvažovány i takové podmínky, které nemusely být naplněny předtím, než k havárii došlo.

Třetí úroveň zahrnuje všechna omezení a nařízení, nebo jejich absenci, která umožnila, aby podmínky zjištěné na druhé úrovni způsobily události popsané na první úrovni, nebo že dovolily existenci příčinných podmínek/faktorů jako takové. Tato úroveň zahrnuje omezení/nařízení/požadavky ve formě zákonů, vyhlášek a norem na technické a fyzikální podmínky, sociální dynamiku, činnost člověka, management a organizační kontrolu a na vládní, resp. socio-ekonomickou politiku v předmětné oblasti průmyslu.

Na třetí úroveň se často odvoláváme jako na kořenové příčiny havárie. Kořenové příčiny se vyskytují ve všeobecných třídách havárií; jsou to nedostatky, které nejenže přispěly k vyšetřeným haváriím, ale mohou ovlivnit i havárie v budoucnosti. V reakcích na havárie je zjevná tendence dát do pořádku jen specificky vybrané příčinné faktory, přičemž zůstanou nepovšimnuté všeobecnější, dokonce i kořenové příčiny. Daleko častěji bývá vina svalena na selhání člověka, nebo na nedostatky/poruchy zařízení, než např. na nedostatečný výcvik, absenci všeobecné kontroly (dozor) nebezpečí, nebo nedostatky managementu.

Protože se havárie pouze zřídkakdy opakují stejným způsobem, “záplaty“ na předcházející “díry“ mohou být neúčinné jako prevence budoucích havárií. Např., kdyby některý z dalších raketoplánů typu Challenger opět havaroval, je nepravděpodobné, že by byla tato havárie způsobená stejným problémem s těsnícím O-kroužkem jako v lednu r. 1986. Chybné těsnění urychlilo vznik havárie, ale kořenové příčiny identifikované při vyšetřování havárie se vztahovaly na nedostatky organizace celého projektu a NASA jako takové. Předcházení haváriím raketoplánů v budoucnosti vyžaduje přesné určení organizačních nedostatků.

Havárie ozařovacího přístroje Therac-25 (došlo k chybnému nastavení léčebné dávky při ozařování pacienta) nebyla způsobena stejnou chybou resp. chybami v softwaru. Také zde působily faktory jako přehnaná důvěra v software a nahrazení standardních mechanických ochran počítači, nedostatečné sledování a vyšetřování hlášených nehod a havárií a procedury výrobce pro odhadování rizika, která nepočítala s možnými chybami softwaru. Vždy, když došlo k předávkování pacienta a výrobce konečně připustil chybu svého zařízení, provedla se oprava předpokládané chyby hardwaru nebo softwaru a výrobce prohlásil, že jakákoliv další havárie je nemožná. V takové postupnosti to pokračovalo až do té doby, kdy dozorčí orgán nařídil výrobci přidat na ozařovače mechanické ochrany, změnit procedury pro vývoj softwaru, provést podrobné analýzy ohrožení a další změny. Takových příkladů opětovných havárií z důvodů neodstranění kořenových příčin v letectvu, námořní dopravě i v jiných nebezpečných provozech z posledního čtvrtstoletí, je možné najít v odborné literatuře velmi mnoho.

2.5 Kořenové příčiny havárií

Kořenové příčiny havárií resp. příčiny havárií třetí úrovně podle výše uvedeného hierarchického modelu havárií mohou být rozděleny do tří kategorií: (1) selhání prvků kultury bezpečnosti průmyslového odvětví, nebo organizace, (2) selhání prvků organizačních struktur a (3) povrchní, nebo neefektivní technické aktivity. V této části studie prozkoumáme vliv uvedených faktorů na havárie.

2.6 Trhliny v kultuře bezpečnosti

Kultura bezpečnosti v průmyslovém odvětví, nebo v organizaci, je všeobecný postoj a přístup k bezpečnosti těch, kteří do daného odvětví nebo organizace patří - management, zaměstnanci, státní dozor apod. Trhliny v kultuře bezpečnosti, zejména (1) přílišná důvěra a sebeuspokojení, (2) nezájem nebo nízká priorita bezpečnosti a (3) trhliny v rozlišení konfliktních cílů, vedly často k velkým haváriím.

Přílišná důvěra a sebeuspokojení

Sebeuspokojení a přílišná důvěra jsou společnými faktory většiny velkých havárií minulého století. Sebeuspokojení odpovědných pracovníků může být opravdu jedním z nejdůležitějších rizikových faktorů. Kemenyho komise [32] identifikovala jako hlavní přispívající faktor k havárií na TMI sebeuspokojení jaderného dozoru USA (NRC) s tvrzením, že k těžké havárii nemůže na JE dojít. Pracovní skupina NRC, která vypracovala opatření pro jaderný dozor USA po havárii v TMI zdůraznila, že přesvědčení o nemožnosti těžké havárie v JE je pravděpodobně jedním z nejvýznamnějších lidských faktorů, se kterým musí celý jaderný průmysl a NRC zápasit. Přestože celý Atomový zákon USA z r. 1954 hovoří o ochraně zdraví a bezpečnosti obyvatelstva, není tato fráze nikde definována. Jeden z prvních představitelů jaderného dozoru v USA,Harold Green prohlásil, že si nikdo tehdy nemyslel, že by bezpečnost byla problémem. Všichni předpokládali, že když se vydá zákon, který nařizuje, že má být něco správně provedeno, bude to tak [3].

Poučení a zkušenosti z havárií občas nepřekročí národní hranice. Po havárii na TMI francouzský premiér řekl: „Havárie na TMI se nemůže stát na jaderných elektrárnách ve Francii. My máme opravdu takové bezpečnostní systémy, které s možností havárie počítají a chrání nás před možnými následky. “Osm měsíců po havárii na TMI vysocí sovětští vládní a vědečtí představitele řekli delegaci z USA, že oni považují jadernou bezpečnost za vyřešenou otázku, a že problémy, které byly vyzdviženy v souvislosti s havárií na TMI, byly příliš zdramatizované. Citovali tehdejšího prezidenta Sovětské akademie věd, který prohlásil, že sovětské reaktory budou brzy tak bezpečné, aby mohly být instalovány na Rudém náměstí. Sovětský jaderný dozor popisoval riziko těžké havárie na černobylském typu jako extrémně malé ještě rok předtím, než k ní došlo a jen měsíc před havárií v Černobylu britský státní tajemník pro energii zopakoval často vyjadřované přesvědčení, že “jaderná energetika je nejbezpečnější formou výroby energie jakou člověk zná“.

Jaderná energetika není jedinou oblastí, ve které převládl neodůvodněný optimismus. Ve vyšetřovací zprávě o havárii Challengeru přiřadila prezidentská komise hlavní zjištění, kterými byly nízká bezpečnost, spolehlivost a zajištění kvality, právě rozebíraným dvěma faktorům – přílišné důvěře a sebeuspokojení. Richard Feynman, člen této komise, se na téma spolehlivosti raketoplánu ptal: „Co je příčinou takové fanatické víry managementu v technické zařízení?“ A uzavírá tím že: „Ať již pro jakýkoliv účel, interní nebo externí, management NASA nafoukl spolehlivost svých produktů až do úrovně fantazie“.

Havárie v Bhopalu je klasickým případem události způsobené převládajícím sebeuspokojením managementu. Havarijní únik MIC byl úplným překvapením téměř pro každého včetně vědců a odborníků na riziko.. Všichni věřili, že taková katastrofa se v tak moderní technologii nemůže stát, že tolik bezpečnostních systémů nemůže najednou selhat, a že závod v Bhopalu je modelovým závodem co se týká bezpečnosti. Byla činěna prohlášení o nadměrném důrazu a vystupňování bezpečnosti výroby. Mnozí zaměstnanci věřili, že byla zavedena dostatečná výstražná opatření, a že se pro bezpečnost provozu už nic víc nemohlo dělat. Problematické praktiky byly označené za akceptovatelné, nebo nevyhnutelné riziko.

Po tragédii v Bhopalu představitelé společnosti Union Carbide společně s Americkým úřadem pro veřejnou bezpečnost a zdraví (OSHA) prohlásili, že takový typ havárie se nemůže stát v závodě v městě Institut (Západní Virginie, USA), kde se také vyrábí MIC, protože je tam lepší vybavení, lepší personál a americká, všeobecně vyšší úroveň technologické kultury a vyspělosti. Ale jen o 8 měsíců později se tam stala podobná havárie, která si vyžádala hospitalizaci přibližně 100 lidí. Tak jako v Bhopalu, tak i v Institutu varovné sirény zazněly opožděně a poskytování potřebných informací veřejnosti bylo pomalé a nedostatečné.

Několik měsíců po havárii v Institutu došlo k úniku nebezpečných chemikálií v dalším podniku společnosti Union Carbide, při kterém se vytvořil toxický oblak plynu, který směřoval k blízkému nákupnímu středisku. Několika lidem musela být poskytnuta první pomoc a lékaři a zdravotnická zařízení ani po dvou dnech nevěděli, o jaké chemikálie se jednalo a odkud přišly, protože Union Carbide popřela existenci úniku.

U výše uvedených havárií, jako i při mnoha dalších, hrálo sebeuspokojení vedení a zaměstnanců očividně hlavní roli. Podrobnější prozkoumání různých aspektů sebeuspokojení nám pomůže lépe porozumět tomuto fenoménu a vidět, jak přispívá k haváriím. Níže budou diskutovány aspekty podcenění rizika, přílišné spolehání na redundanci, nerealistické odhady rizika, ignorování událostí s rozsáhlými následky a nízkou pravděpodobností, předpokládání poklesu rizika v čase, podhodnocení rizika ze softwaru a ignorování varovných znamení.

Podceňování rizika

Jedním z aspektů sebeuspokojení je základní tendence lidí podceňovat riziko. Většina havárií v dobře zkonstruovaných systémech zahrnovala dvě nebo více událostí, jejichž nejhorší kombinace se může vyskytnout jen s velmi nízkou pravděpodobností. Když se lidé snaží predikovat riziko systému explicitně, nebo implicitně, násobí nízké pravděpodobnosti jevů, předpokládají jejich vzájemnou nezávislost a dostávají nemožněmalá čísla, přestože ve skutečnosti jsou předmětné jevy závislé. Machol [44]pojmenovává tento fenomén „Coincidencie Titanic“.

Když byl Titanic v r. 1912 spuštěn na vodu, byl největší a nejbezpečnější lodí, jaká kdy byla postavena. Fakt, že měl být nepotopitelný, byl znám na celém světě a všeobecně byl akceptován. Dno lodi bylo konstruováno z dvojitého pláště a mělo 16 vodotěsně oddělitelných komor. Bylo vypočítáno, že až 4 komory mohly být naráz proraženy, aniž by se loď potopila. V historii havárií lodí byl počet 4 poškozených komor považován za dostatečný. Stavitelé slibovali nepotopitelnost lodi a důvěra v jejich prohlášení byla tak veliká, že jeden z lodních důstojníků ujistil jednu z cestujících dam, že “pouze Pán Bůh sám by tuto loď mohl potopit“. Pojišťovna Lloyd v Londýně vystavila pro Titanic certifikát nepotopitelnosti i přesto, že přepážky mezi 16 komorami dna nebyly dostatečně vysoké k tomu, aby každou z nich hermeticky uzavřely. Konstruktéři totiž počítali s tím, že v případě potíží bude čas zasáhnout ještě před tím, než voda přeteče do sousedních komor.

Jak je známo, na své první plavbě, při které se majitelé hned snažili překonat tehdejší rychlostní rekord, srazil se Titanic s ledovcem. Na jeho trupu se přitom vytvořila trhlina v délce 300 stop a bylo zaplavených 5 spolu sousedících komor. Loď se potopila s 1513 lidmi na palubě. V ten den na lodi přijali více varovných telegramů o přítomnosti ledovců na trase plavby, ale nikdo se jimi neznepokojoval. Když Titanic narazil do ledovce asi 95 mil jižně od Newfoundlandu, cestujícím bylo řečeno, že není žádný důvod k poplachu, a že mají zůstat ve svých kajutách. Posléze kapitán nařídil evakuaci lodi, ale ta se zvrhla v chaos a teror.

Klasický nácvik evakuace nebyl před tím proveden a námořníci neznali svoje povinnosti při evakuaci.

K tomuto neštěstí a k následným vysokým ztrátám na životech přispělo více koincidencí, např. kapitán připustil příliš vysokou rychlost plavby vzhledem k existujícím podmínkám, nebyla zabezpečena přiměřená strážní služba, na lodi nebyl dostatečný počet záchranných člunů, nebyl proveden výcvik používaní záchranných člunů, a přestože byly spuštěny správně, námořníci je neuměli dostatečně ovládat, telegrafista na lodi, která se plavila v blízkosti Titanicu spal, a proto neslyšel tísňové volání. Mnohé z těchto okolností je možno považovat za nezávislé, ale přestanou se tak jevit, když uvážíme přílišnou důvěru, spoléhání se na prohlašovanou nepotopitelnost, která pravděpodobně vedla k nadměrné rychlosti, nedostatečnému zabezpečení hlídek, k malému počtu záchranných člunů a nedostatečnému výcviku v jejich používání. To, že ke srážce s ledovcem došlo v noci, přispělo k tomu, že ledovec nebylo dobře vidět a vyhnout se mu bylo obtížnější než přes den. Zrovna tak byla noc příčinou, že telegrafista na blízké lodi spal. Společný součin pravděpodobností těchto všech podmínek/okolností neposkytne dobrý odhad pravděpodobnosti s jakou může dojít k havárii, jaká se stala Titanicu. V skutečnosti však všechny tyto faktory ukazují, že k neštěstí muselo nevyhnutelně dojít.

Fenomén, nazývaný “Titanic efekt“, vysvětluje skutečnost, že velkým haváriím často předchází přesvědčení, že k nim nemůže dojít. Titanic efekt hovoří o tom, že velikost katastrof se zmenšuje v takovém rozsahu, v jakém jsou lidé přesvědčeni, že jsou možné, a v jakém plánují zabránit nebo minimalizovat jejich účinky. Provést v předstihu potřebná opatření k jejich zabránění nebo k zvládnutí katastrof, se obyčejně vždy vyplácí, protože náklady na ně jsou neporovnatelné oproti vzniklým škodám.

Přílišné spoléhání na redundance

Redundance a diverzifikace se často používají ve snaze vyhnout se chybám/selháním a zvýšit spolehlivost. Například bezpečnostní systém v chemické továrně může být diverzní v takovém smyslu, že monitoruje dva nezávislé parametry, kupříkladu teplotu a tlak a je redundantní tím, že má více kanálů s logikou většinového výběru. I přesto se však může stát, že jediný faktor může způsobit, že všechny tyto složky selžou naráz, když dojde například k výpadku elektrického proudu, nebo k požáru. Chyby, které společně způsobily havárii (common-cause failures), jsou chyby, které jsou “koincidentní“ v čase, protože existovaly závislosti mezi podmínkami vedoucími k události. Tento typ chyb byl příčinou mnohých havárií zařízení, které byly zabezpečeny redundancemi a diverzitou bezpečnostních systémů.

Známou havárií takto zabezpečeného zařízení byl požár v jaderné elektrárněBrowns Ferry v Alabamě v r.1975. Nekontrolovaný požár trval 7,5 hodiny. Všechna bezpečnostní zařízení totálně selhala, protože oheň zničil redundantní elektrické napájení a řídící systémy. Jeden ze dvou jaderných reaktorů nebyl pod bezpečnou kontrolou po dobu několika hodin. Později se jej podařilo dostat pod kontrolu jedním ze zařízení, které nebylo součástí bezpečnostního systému, a které pouze náhodou nebylo poškozeno požárem. Inženýři ze státního jaderného dozoru USA (NRC) a operátoři z Browns Ferry soukromě přiznali, že k potenciálnímu katastrofálnímu úniku radioaktivity nedošlo pouze náhodou.

Jedním z důvodů při rozhodovaní o pokračování přípravy tragického vypuštění raketoplánu Challenger byla bezpečnostní rezerva ve zdvojených těsněních s O-kroužky. Znamenala, že když první těsnící O-kroužek nebude těsnit, splní tuto úlohu druhý O-kroužek. Při havárii chyba prvního těsnění zapříčinila podmínky, které vedly k selhání druhého těsnícího O-kroužku.

V listopadu 1961 všechny spojovací linky radarového systému včasné výstrahy mezi velením strategického letectva USA a veleními štábů včasné výstrahy náhle selhaly. Komerční telefonní linky byly také mimo provoz. Protože tento náhlý výpadek mohl být nepřátelskou akcí, byl vyslán poplašný signál po celých Spojených státech amerických. Později se zjistilo, že přestože redundantní spojovací linky mezi uváděnými institucemi byly zřízeny, vedly přes jednu společnou reléovou centrálu, i když bylo deklarováno, že tomu tak není. Přehřátí motoru na této centrále přerušilo celé spojení.

Všechny katastrofy způsobené společně působícími chybami ukazují na jeden paradox: zajištění redundance může vést k přílišné důvěře a k sebeuspokojení, které efekt redundance neguje.

Nerealistické odhadování rizika

Nerealistické odhadování rizika může vést také k sebeuspokojení z nemožnosti havárie a k absenci vhodných bezpečnostních aktivit. Např. namísto, aby vyšetřování začalo ihned po získání první informace o možném předávkování při ozařování přístrojem Therac-25 výrobce odpověděl, že pravděpodobnostní odhad rizika ukázal, že taková událost je nemožná a nic nepodnikl. Pravděpodobnost, že počítač způsobí předávkování, byla zahrnuta v poruchovém stromě jako událost typu “Počítač vybral špatnou energii“ a byla jí přiřazena pravděpodobnost 10^{-11} a událost typu “Počítač vybral nesprávný mód“ s přiřazenou pravděpodobností 4×10^{-9}.

Kvantitativní odhady měří jen to, co mohou změřit a ne nevyhnutelně to, co je potřebné, aby bylo změřeno. Neměřitelné faktory, např. konstrukční omyly, chyby managementu, se jednoduše přehlíží, i když mohou mít větší vliv na bezpečnost než ty , které se měří. Navíc, výchozí předpoklady pro odhad, jako například, že závod, nebo zařízení je postaveno v souladu s projektem, nebo že některé chyby jsou závislé, se také neberou v úvahu. Více roste přesvědčení, že vypočítaná čísla opravdu odpovídají reálnému riziku havárií, než že jsou výsledkem hodnocení specifických aspektů projektu.

V příručce amerického letectva, v níž jsou popsány havárie vysoce kritických systémů, je uveden přesvědčivý příklad takového odhadování rizika. Projekt daného zařízení počítal s pojistným ventilem pro zabránění přetlaku v systému, ovládaným operátorem. Druhý pojistný ventil byl nainstalován jako záložní pro případ, že by první selhal. Operátor musel vědět, že se první ventil neotevřel, aby mohl otevřít druhý pojistný ventil. Při jedné příležitosti se indikátor otevření prvního pojistného ventilu rozsvítil, avšak ten ve skutečnosti otevřený nebyl a systém explodoval. Vyšetřováním se ukázalo, že světelný ukazatel signalizoval pouze přítomnost napětí na ovládači ventilu, ale ne velikost jeho otevření, tedy pouze to, že aktivační tlačítko bylo stlačeno, ale nikoliv, že se ventil otvírá.

V rozsáhlých kvantitativních bezpečnostních analýzách tohoto návrhu se počítalo jen s velmi nízkou pravděpodobností současného selhání obou pojistných ventilů. Možnost chybného návrhu elektrického zapojení signalizace nebyla v analýzách zahrnuta - nebyla kvantifikovatelná. Na základě nízké hodnoty pravděpodobnosti současného selhání obou pojistných ventilů došlo k přesvědčení o bezpečnosti systému, tak, že příslušní pracovníci skutečné zapojení ani neodzkoušeli.

Téměř u všech velkých havárií z posledního období se vyskytly příčinné faktory, které nelze kvantifikovat. Je možno pokládat za fakt, že většina z důležitých příčinných faktorů na úrovni kořenových příčin (tj. omezení/nařízení), jsou neměřitelné a nekvantifikovatelné.

Dalším omezením pravděpodobnostního hodnocení bezpečnosti provozu zařízení je častá záměna důrazu na zvyšování bezpečnosti za dokazování, že systém je bezpečný

tak, jak byl původně navržen. Pozornost se odkloní od kritických míst návrhu a zaměří se na snižování čísel v odhadech. V nejhorším případě se tyto odhady začnou tvořit zpětně od požadované pravděpodobnosti (např. 10^{-9} za rok resp. životnost) a potom se sestavují modely, které potvrdí toto číslo pro existující projekt. Často jsou to spíše cvičení fantazie, než inženýring. William Ruckelhaus, který dvakrát předsedal úřadu pro ochranu životního prostředí USA upozornil, že: „Údaje o odhadu rizika jsou jako zajatý špión; jestliže jej budete mučit dost dlouho, vám řekne všechno, co jen budete chtít slyšet."

A nakonec posledním omezením používání číselně vyjádřených bezpečnostních cílů je nesprávná praxe konstruktérů, kteří se zaměřují jen na dosažení zvlášť sledovaných a upřednostněných cílů a nevěnují se náležitě ostatním, které mohou být pro celkovou bezpečnost stejně důležité. Uvedená omezení použití výsledků kvantitativních odhadů neznamenají, že kvantitativní analýza není užitečná pro některé účely. Pouze zdůrazňují, že údaje, kterými operuje, musí být interpretovány a používány s velkou opatrností.

Ignorování událostí s těžkými následky a malou pravděpodobností výskytu

Sebeuspokojení často vede k omezenému a nesystematickému posuzování vážných rizik. Obyčejně jsou vysoce pravděpodobná nebezpečí kontrolována, ale nebezpečí s těžkými následky a s (předpokládanou) malou pravděpodobností výskytu jsou přehlíženy a nepovažuje se za vhodné vyčlenit prostředky na jejich prevenci. Společným zjištěním z těžkých havárií je, že jevy/události, které se v nich vyskytly, byly známy před haváriemi, ale jejich výskyt byl považován za nemožný. Příkladem tohoto chování jsou havárie, které se staly v systémech s propracovanými programy bezpečnosti.

Všeobecně se lidé nejvíce naučí ze zkušenosti. Vyhýbat se se zvýšenou opatrností určitým nebezpečím nás naučí vlastní nebo bezprostřední zkušenost s nimi. Studie za studií odhaluje fakt, že nová bezpečnostní opatření/nařízení byla ve všech zemích přijata většinou po velkých haváriích a ne v předstihu. Zavírat bránu až potom, když kráva uteče, se zdá být nevyléčitelnou lidskou nemocí. Běžně tento mechanizmus funguje nejlépe při zábraně opakování malých, nebo středně velkých havárií s výraznou frekvencí výskytu. Zdá se však, že lidé nechtějí být proporcionálně více opatrní, aby se vyhnuli velkým, ale méně se vyskytujícím kalamitám, jaké ještě osobně nezažili. Fakt, že složitý systém ještě masivně nehavaroval, je asi podvědomě vnímán jako důkaz, že je vůči takovému selhání bezpečný, což následně vede k sebeuspokojení, ba až k lhostejnosti.

Operátorka přístroje na ozařování Therac-25, které se dvakrát stalo, že pacient byl předávkován, vypovídala, že byla ujištěná, že zařízení má tolik bezpečnostních prvků, že k předávkování pacienta nemůže dojít. Po prvních zprávách o předávkování pacientů výrobce namísto podrobného vyšetření znovu pouze prohlásil, že chyba nemohla být v jeho zařízení. Důkazem jeho tvrzení byl zase jen počet bezpečnostních prvků a později, po záměně hardwaru, výrobce tvrdil, že bezpečnost přístroje se zvýšila o pět řádů.

Během krize letu Apolla 13 pozemní řídicí personál nebyl schopen uvěřit tomu, co viděl na řídících panelech. Odmítání považovat oznamovaná fakta za pravdu vysvětlil jeden z inženýrů NASA takto: „Nikdo si nemyslel, že raketa může ztratit dva palivové články a dvě kyslíkové nádrže. To se nemohlo stát." Astronaut Jack Swigert potvrdil tento názor prohlášením: „Kdyby někdo připravil takovouto situaci na simulátoru, všichni bychom mu řekli, aby nefantazíroval." [30]

Není praktické požadovat, aby všechna nebezpečí, nezávisle na tom, za jak vzdálené je považujeme, byla eliminována nebo kontrolován, ale nezávislost a jiné zjednodušující předpoklady při neformálních nebo formálních odhadech rizika, by měla být volena jen s velkým skepticizmem. Neexistuje příčinný důvod vypouštět z mysli potenciální možnost katastrofální havárie, jaká se dosud nestala.

Předpoklad poklesu rizika v čase

Společnou hrozbou při většině havárií, na kterých mělo podíl sebeuspokojení, bylo přesvědčení, že systém musí být bezpečný, protože je provozován bez havárie už mnoho let. Přístroj Therac-25, byl bezpečně použit více než tisíckrát než došlo k prvnímu předávkování pacienta. Dlouholeté bezpečné používání nějakého zařízení ještě není zárukou, že k havárii nemůže dojít, i když se neformální odhady rizika rychle zmenšují. Riziko se ve skutečnosti může snižovat, zůstat stejné, nebo se dokonce po nějaké době zvýšit. Zvýšit se může z několika důvodů včetně faktu, že po dlouhé době bez výskytu havárií ubude opatrnosti a zvýší se úsilí vybudovat ještě složitější a vůči chybám odolnější systémy. Záměna priority bezpečnosti za jiné faktory, nejčastěji za produktivitu, vede k tomu, že manažeři se začínají postupně orientovat převážně na další faktory a bezpečnostní rezerva je stále více snižována. To dává možnost výskytu dost překvapujícímu faktu: čím více se zmenšuje výskyt chyb v systému, tím se může riziko jeho havárie ve skutečnosti zvyšovat.

Časem se může riziko zvětšit buď samotnými změnami zařízení jako výsledek jeho údržby, nebo vývoje, nebo změnou podmínek okolního prostředí. Například chování operátorů se může změnit díky důkladnému zvládnutí řídícího systému.

Problémem při prosazování bezpečnosti je nemožnost stanovení počtu havárií, kterým lze předejít dobrým programem bezpečnosti. Konečnou ironií je, že úspěšný program bezpečnosti může vést k sebeuspokojení tehdy, když se havárie nevyskytnou a toto sebeuspokojení může často vést k havárii. Z toho vyplývá, že čím je organizace úspěšnější v eliminování havárií, tím je pravděpodobnější, že sebeuspokojení v ní zvýší riziko. Příkladem takového vývoje je bezpečnostní program NASA, vypracovaný po havárii Apolla v r. 1967, při které zahynuli 3 kosmonauti. Byl to tehdy jeden z nejlepších programů bezpečnosti na světě. Úspěch dalších projektů NASA snížil důraz vedení na bezpečnost a s vědomím, že úspěch byl nevyhnutelný, se priority manažerů přesunuly k jiným projektovým cílům, zejména ke snižování rozpočtových nákladů. Výsledek se dostavil až po 20 letech, kdy havaroval raketoplán Challenger.

Podceňování rizika selhání software

Se zaváděním počítačů do řídících systémů složitých zařízení se rozšířila nová forma sebeuspokojení vyplývající z přesvědčení, že software se nemůže zmýlit, a že všechny jeho chyby budou odstraněny při testování. Obzvlášť pro ty, kteří nejsou softwarovými profesionály, je neomylnost softwaru přímo mýtem. Je pravda, že software, na rozdíl od hardwaru, nemá klasické chyby z opotřebování, ale jeho koncepční chyby se hledají a eliminují mnohem hůře. Módy chyb hardwaru jsou všeobecně limitovány a běžně se vůči nim dají vytvořit ochrany.

Nehoda přístroje Therac-25 představuje přesvědčivý příklad potenciálního výsledku sebeuspokojení z neomylnosti softwaru. Již jsme uvedli, že software tohoto zařízení ani nebyl zahrnut do původních analýz nebezpečí. Výrobce prohlásil, že chyby v programu jsou zredukovány extenzivním testováním na simulátoru a v terénních podmínkách na teleterapeutických jednotkách. Jakékoliv reziduální chyby nebyly proto zahrnuty v analýzách nebezpečí. Software se používáním neopotřebovává (nedegraduje), nepodléhá únavě a změnám při reprodukčních procesech. Když začala přibývat neštěstí z předávkování pacientů, nebyl software vůbec prověřován. Předávkování bylo připisováno provozním chybám hardwaru a byla řešena přidáváním dalších redundancí hardwaru. Tento nerealistický odhad rizika jenom zvyšoval sebeuspokojení ze zajištění bezpečnosti zařízení a prodlužoval absenci vyšetření havárií.

Hardwarové zdokonalení, blokády a ochrany, spolu s ostatními bezpečnostními zařízeními, jsou dnes běžně nahrazovány softwarem v mnohých rozdílných typech systémů včetně letecké dopravy, jaderných elektráren a zbraňových systémů. I tam, kde hardwarové ochrany dosud zůstaly, jsou často ovládány softwarem. Mnohá základní mechanická bezpečnostní zařízení, která vznikla již v minulosti, jsou velmi dobře otestována, jsou levná, spolehlivá a jsou postavena na jednoduchých fyzikálních principech. Jejich nahrazování programovatelnými zařízeními, které mají jen některé z požadovaných vlastností originálních ochran nejsou správným doporučením pro zachování úrovně bezpečnosti.

Podceňování softwarového rizika je možné vidět i na některých nových softwarových standardech pro civilní letectvo a jadernou energetiku. Softwarové funkce jsou definovány jako kritické pro bezpečnost jen tehdy, jestliže pouze tyto mohou způsobit havárii. Protože jsou systémy pouze ojediněle zkonstruovány tak, že jednoduchá chyba, nebo selhání, může způsobit katastrofu, bývá pouze malá část softwaru, nebo dokonce žádná, vypracována jako kritická pro bezpečnost.

Ignorování varovných znamení

Posledním aspektem sebeuspokojení je podceňování varovných znamení potenciálních havárií. Haváriím se často předejde varovnými oznámeními veřejnosti, přicházejícími sériemi drobných příhod, nebo jinými znameními. Tato znamení jsou často přehlížena odpovědnými osobami, protože ti jsou přesvědčeni, že velká havárie je nemožná. Je pravda, že je vždy více poruch a výpadků než havárií, protože většina zařízení je zkonstruovaná tak, aby byla buď odolná vůči jednoduchým selháním a chybám, anebo tyto chyby samy rozpoznají a bezpečně na ně zareagují (např. automatickým odstavením). Ty jsou obvykle napraveny dřív, než by mohlo dojít k nebezpečným situacím. Ani ty by nemusely končit haváriemi, pokud by nebyly vytvořeny specifické podmínky okolí, které jsou nevyhnutelné pro to, aby došlo k těžkým ztrátám a poškozením.

Už sedm let před explozí ve Flixborough upozorňoval hlavní inspektor továren ve Velké Británii na rizika spočívající ve zvýšeném používání a skladování velkého množství nebezpečných chemických materiálů v továrnách. Nejméně 6 vážných havárií se stalo v továrně v Bhópálu v průběhu 4 let před tragickým neštěstím v r. 1984, přičemž při jedné z nich v r. 1982 přišel o život 1 dělník. Lidé v klíčových manažerských pozicích byli vícekráte upozorňováni na potenciální nebezpečí plynoucí z více zdrojů. Jedním z nich byla i série novinových článků, které doslova předpovídaly závažnou havárii v této továrně. Místní správa a manažeři továrny neudělali nic. Znaky včasného varování byly ignorovány. Před havárií na TMI bylo zaznamenaných několik podobných událostí a chyb operátorů, které predikovaly tuto havárii a dokazovaly přetrvávající a neopravené chyby zařízení. Všechny tyto příznaky byly přehlíženy a odmítány. Např. od r. 1970 do havárie na TMI (v r. 1979) bylo zaznamenáno 11 případů právě takových nesprávných činností pojistných ventilů, které pak způsobily havárii na TMI.

James Creswell, inspektor jaderných reaktorů americké NRC, oznámil poruchy na dvou reaktorech typu Babcock and Wilcox (B&W) - Rancho Seco a Davis-Besse – když hlásiče nedávaly operátorům adekvátní informaci o provozním stavu reaktorů. V elektrárněDavis-Besse selhal systém doplňování vody, když se pojistný tlakový ventil otevřel a operátor vyhodnotil nesprávně hladinu vody v reaktoru na základě indikace hladiny v kompenzátoru objemu. Chybná informace vedla operátora k nesprávnému odstavení čerpadel havarijního chlazení. Více než rok před havárií v TMI se Creswell pokoušel sdělit své obavy, příslušným elektrárenským společnostem a firmě B&W. V elektrárně TMI nakonec našel dva inspektory

NRC, kteří ho byli ochotni podpořit, avšak marně. Creswellovi nakonec bylo na jeho otázky odpovězeno až den po havárii v elektrárně TMI.

Ještě jeden příklad nezájmu o varovná znamení, která předcházela havárii TMI. Tento příklad poskytuje zpráva Carlyle Michelsona, staršího jaderného inženýra dozoru v Tennessee Valley, poslaná na Divizi bezpečnosti systémů NRC v r. 1977, ve které upozornil na možnost vytváření parních bublin v chladícím zařízení reaktorů firmy B&W. Bylo v ní také zdůrazněno nebezpečí nesprávného vyhodnocení výšky hladiny v reaktoru na základě sledování hladiny v kompenzátoru objemu při vzniku parní bubliny. Podle protokolu měla být tato zpráva postoupena Divizi provozu reaktorů NRC, která měla na tyto problémy upozornit elektrárenské společnosti. Asistent ředitele Divizní bezpečnosti systémůřekl, že si myslel, že útvar inspekce a dozoru zasáhne v případě, když to bude nutné. Deset dní po TMI havárii požádal Poradní výbor pro dohled nad bezpečností reaktorů, aby NRC splnil některé z Michelsonových doporučení. Dne 22. března 1975, během rekonstrukce jaderné elektrárny Browns Ferry, se od plamene svíčky na detekci unikajících plynů vzňala polyuretanová izolace vodičůřídícího a kontrolního systému, což vedlo k těžkému poškození celého řízení systému a kontroly na základě společné chyby (common-mode failure) kabeláže zmíněného systému. Před tímto požárem bylo vedení elektrárny Browns Ferry mnohokrát varováno před vážnými nedostatky bezpečnosti, speciálně před nedostatky v programu požární ochrany. Na tato varování vedení elektrárny nereagovalo. Ke dvěma požárům došlo ještě dne 20. března 1975, tyto musely být uhašeny suchými chemikáliemi. Zpráva o těchto požárech nebyla korektně podaná a jejich vliv na bezpečnost nebyl vyhodnocen.

Požár ve stanici metra London`s King`s Cross v Londýně v r. 1987, při kterém zahynulo 31 lidí a mnozí další byli zraněni, byl prokazatelně způsoben dohořívající zápalkou, kterou odhodil cestující metra na eskalátoru. Vznítila se usazená mastnota a výpary vlivem zanedbaného čistění. Přestože i tyto faktory byly přímou příčinou požáru, kořenovou příčinou (příčina třetí úrovně), byl názor zodpovědných pracovníků, že náhodné požáry na eskalátorech a jiných zařízeních lze zvládnout dříve, než by mohly způsobit vážné škody nebo poranění. Tento názor byl přijat na základě toho, že mezi roky 1958 -1967 bylo každý rok průměrně 20 požárů, které způsobily pouze malé zakouření a nejevily se jako vážné ohrožení. Nanejvýš se pouze několik cestujících nadýchalo kouřových zplodin, nikdo však nezemřel. Proto vzniklo podvědomí zodpovědných pracovníků, že žádný vážný požár nemůže vzniknout, a proto i zaměstnanci metra neměli dostatečný havarijní výcvik a jejich činnost během katastrofického požáru byla chaotická a nekoordinovaná.

Doposud získaná zkušenost jednoznačně potvrzuje, že lidé mají sklon podceňovat riziko a ignorovat varovná znamení. Nejméně jedna, ale většinou i více vážných havárií je nutných proto, aby bylo v praxi účinně zasáhnuto proti rizikům. Zpravidla se postupně vyskytne několik podobných havárií po sobě, až do doby, kdy dojde k takové havárii, že její následky už není možné popřít a nadále přehlížet nedostatky, které ji způsobily.

Vláda, management, ale i výzkumní pracovníci reagují daleko více na velké katastrofy, než na havárie menšího rozsahu, nebo provozní poruchy, přestože posledně jmenované jsou daleko častější. Po potopení Titanicu bylo ihned doporučeno zavést 24 hodinovou službu pro obsluhu radiostanic na dopravních lodích, spolehlivé náhradní zdroje elektrické energie, výcvik posádky a cestujících pro používání záchranných člunů, zákaz používat světlice na otevřeném moři pro jiné účely, než pro signalizaci ohrožení apod. Podobná přísná legislativní opatření byla zavedena i po haváriích v chemických továrnách ve Flixborough a v Sevesu.

Navzdory těmto výsledkům musíme uznat, že velké havárie způsobily větší újmu než užitek z poučení, která jsme získali. Tuto skutečnost podporuje také fakt, že většina z toho, co se zjistilo při jejich analýzách, bylo známo dávno před tím, než se staly. Tyto znalosti však nebyly včas zohledněny.

Nízká priorita bezpečnosti v podnicích

Sebeuspokojení z bezpečnosti není pravidlem a lidé v průmyslu nebo v jiných organizacích se o bezpečnost obvykle starají. Jejich úsilí však může být neefektivní v případě, jestliže nemají podporu vrcholového managementu. Zajištění bezpečnosti musí být prvořadou snahou celé organizace a iniciovat ji musí právě vrcholové vedení. Zaměstnanci musí mít jistotu, že se jich společnost zastane, když vědomě budou upřednostňovat bezpečnost před jinými cíli. Neformální pravidla stejně jako formalizované předpisy a nařízení organizační kultury musí podporovat celkovou bezpečnostní politiku podniku/organizace. Nejdůležitější však je, aby všechny snahy a vyhlášení o bezpečnosti byly převedeny do praxe.

Jedním z indikátorů snahy managementu o bezpečnost jsou zdroje přiřazované k dosažení cílů bezpečnosti. V již uvedené Rogersově zprávě o havárii raketoplánu Challenger [59] se konstatuje, že tým hlavního inženýra odpovědného za bezpečnost, spolehlivost a kvalit sestával pouze ze 20 odborníků, ze kterých jeden člen věnoval této problematice pouze 25 % svého času a druhý jen 10 %. Před havárií v Bhópálu byly výraznězredukovány počty pracovníků směny, dále i výcvik a údržba. Vedení zdůvodňovalo, že tyto redukce nemají vliv na bezpečnost i přesto, že mnozí zaměstnanci upozorňovali na bezpečnostní dopady takových úprav.

Nejdůležitějšími úkoly managementu v prevenci havárií, je stanovení a implementace organizačních priorit. Někteří manažeři si uvědomují, že bezpečnost se vyplácí z dlouhodobého hlediska, jiní zase upřednostňují krátkodobé cíle před bezpečností. Vládní úřady a agentury pro ochranu zákazníků mohou vyvíjet nátlak na management, aby přistupoval k bezpečnosti vážně. Tento typ nátlaku však může být účinný jen tehdy, když získá společenskou podporu a důraz. Dalšími alternativami nátlaku na zvyšování priority bezpečnosti jsou vládní nařízení, zákony, požadavky pojišťoven či odborových organizací.

Problémy při řešení konfliktních cílů

Bezpečnost nepotřebuje, aby byla vnímána pouze jako cíl s vysokou prioritou, ale potřebuje i procedury pro řešení konfliktních cílů. Požadované cíle se často dostávají do vzájemného konfliktu a jejich vzájemné záměny jsou nevyhnutelné u každého návrhu, nebo ve vývojovém procesu. Snaha navrhnout systém tak, aby vyhovoval všem požadovaným cílům, nebo stanovit takové normy, které zaručí splnění vícero cílů bez zvažování jejich potenciálních konfliktů, může skončit jen neúspěchem. Klasickým případem nezvládnutého konfliktu mezi bezpečností a stanoveným rozvrhem činností je uvedená katastrofa Challengeru.

Bezpečnost často utrpí při záměně vzájemných konfliktních cílů kvůli tvrdosti argumentů ve prospěch zisku. Náklady a harmonogram jsou běžně hlavními ukazateli projektu, přičemž prospěch z investicí do bezpečnosti se ukáže až v dlouhodobé perspektivě a i potom je viditelný pouze nepřímo tím, že nedošlo k haváriím a nebyly nutné dodatečné modifikace a úpravy kvůli bezpečnosti systému. Neurčitosti, které mohou být hrozbou z dlouhodobého hlediska, se těžko kvantifikují, proto se daleko lépe zdůrazňují krátkodobé faktory podporující záměny konfliktních cílů. Upřednostnění zaručeného zvýšení produktivity na úkor prevence havárií s očividně nízkou pravděpodobností výskytu však není správnou cestou.

Přesvědčení, že bezpečnost je v konfliktu s bazální užitečností technologie, je všeobecně rozšířeno. Kontrola rizik často vyžaduje dostatek prostředků na úkor plánovaného zisku. Prospěch/užitek z technologie je smyslem její existence. Z pohledu zákazníka je užitek jasný a hmatatelný, neboť rizika výrobku jsou často snížena. Jelikož však sponzoři technologie, management i zákazníci, mají významné podíly (investice) na existenci technolo-

gie, proto nepřekvapí, že se v podnicích/organizacích rizikový management nepraktikuje v největším možném rozsahu. Pro určité skupiny může užitek převážit s ním korespondující rizika a proto se ti, kteří mají prospěch z provozu technologie, často dostávají do politických (názorových) sporů s rizikovými manažery, kteří se starají o všeobecný prospěch.

Přestože je faktem, že v některých případech si zvýšení bezpečnosti vyžádá nějakou částku z předpokládaného přínosu technologie, není to zákonem. Skutečný stav bude záviset na tom, co rozumíme předpokládaným přínosem technologie, a jak jsou bezpečnostní opatření implementována. Bezpečnost může být zvýšená bez dodatečných úprav a modifikací (downstream protection) zařízení tak, že se nebezpečí eliminují a kontrolují hned od začátku návrhu v perspektivě celého životního cyklu technologie (upstream hazard elimination and control). Tato cesta je mnohem levnější než dodatečné změny projektu a dokonce požadované náklady na zajištění bezpečnosti od začátku lze minimalizovat v porovnání s potenciálními náklady na škody u velkých havárií.

Velmi časté je také přesvědčení, že zvyšování bezpečnosti zpomaluje provoz a snižuje výkonnost. Reálná zkušenost však ukazuje, že za přiměřeně dlouhé období je bezpečný provoz všeobecně efektivnější a práce bývají dokončeny mnohem rychleji. Jednou z příčin tohoto efektu je eliminace různých přerušení a zdržení při práci vyvolávaných poruchami a haváriemi.

Přesvědčení, že bezpečné systémy jsou mnohem dražší, nebo že budování bezpečnosti od počátku projektu nevyhnutelně vyžaduje kompromisy s ostatními cíli, je pravdivé jen z části.

2.7 Neefektivní organizační struktura

Při mnohých vyšetřováních havárií se zjistilo, že určité organizace měly upřímnou snahu zajistit bezpečnost, ale jejich organizační struktury byly neefektivní pro implementaci předmětné snahy. Zebroski [73] zkoumal příčinné faktory čtyř velkých havárií
-Bhopal, Challenger, TMI a Černobyl - a u všech našel podobné nedostatky ve stylu a struktuře organizace, především mnohoúrovňovou hierarchii s rozptýlením odpovědnosti a slabou komunikací.

Základními principy managementu, které platí jak pro bezpečnost, tak i pro jiné cíle kvality, je potřeba stanovit jasně odpovědnosti, pracovní úkoly a povinnosti, zřetelné komunikační linie, principy spolupráce a administrativní důslednost. V souvislosti s haváriemi se výrazně projevily některé specifické problémy v organizačních strukturách: nejasné povinnosti a autority za bezpečnost společně s rozhodováním na nesprávné úrovni řízení, nedostatečná nezávislost útvaru pro bezpečnost ve struktuře řízení, nízká úroveň statusu pracovníků útvaru bezpečnosti a jejich vyloučení z přípravy kritických rozhodnutí a omezené informační kanály pro informace související s bezpečností.

Rozptýlení odpovědnosti a autority

Havárie jsou často spojeny s nedokonalou organizací, která obsahuje tzv. rozptýlené odpovědnosti za bezpečnost včetně nedostatečně definované práva a povinnosti v záležitostech bezpečnosti. Problémy narůstají obzvláště tehdy, když jsou povinnosti za bezpečnost rozděleny napříč organizačních hranic a v organizaci neexistuje osoba přímo pověřená odpovědností za celkovou bezpečnost. Pokud se na výrobě zařízení podílí více organizací/skupin, je nevyhnutelné, aby existoval centrální útvar zabývající se problémy vzájemného sladění tak, aby bylo zajištěno, že se ani jedna z nich nespolehne na to, že se o bezpečnost postará jiná skupina.

Nedostatečná nezávislost a nízký status personálu bezpečnostních útvarů

Bezpečnost se považuje za součást normálních činností, která je zajišťována speciálním organizačním útvarem bezpečnosti. Tento organizační útvar ve struktuře řízení a jeho nezávislost na projektovém nebo výrobním managementu, pro který zabezpečuje přehled nebo vstupy, je důležitý ve smyslu podřízenosti a poskytování zdrojů.

Ve zprávě Rogersovy komise o vyšetřování příčin havárie Challengeru [59] je jako příčinný faktor uveden nedostatek nezávislosti pracovníků zodpovědných za bezpečnost, spolehlivost a zajištění kvality, kteří byli pod supervizí organizace včetně těch, jejichž činnost měli kontrolovat. Podobná kritika byla vznesena při oficiálním vyšetřování exploze ve Flixborough, kde také neexistovala žádná inženýrská organizace nezávislá na linii managementu výroby, která by měla na starosti posouzení celého systému a zajištění adekvátní celkové kontroly.

Podobně jako nedostatečná nezávislost pracovníků bezpečnostních útvarů je s těžkými haváriemi spojen další z příčinných faktorů, a to nízký status těchto pracovníků a s ním zřejmě související fakt, že většinou nebývají přizváni ke kritickým diskusím a k rozhodnutím. Kritické telekonference před startem Challengera dne 27.1.1986 se nezúčastnil ani jeden z inženýrů odpovědných za bezpečnost, spolehlivost a kvalitu a také nikdo z nich nebyl zastoupen v manažerském týmu, který rozhodoval o odstartování raketoplánu. Status bezpečnostního personálu a jejího přizvání k tvorbě kritických rozhodnutí je pro každého pracovníka v organizaci jasným znakem skutečného (na rozdíl od deklarovaného) důrazu, jaký management klade na bezpečnost.

Omezené komunikační kanály a slabý informační tok

Při vyšetřování organizačních faktorů velkých havárií se často probírají komunikační problémy. Do r. 1983 se v projektu Shuttle (NASA) vyžadovalo odhlasování všech problémů, trendů a neúspěchů managementu na vyšších úrovních řízení. Po r. 1983 byly tyto požadavky silně potlačeny a pracovníci na vyšších úrovních přestali mít přehled o bezpečnosti, výrobě a otázkách okolo změn letových rozvrhů vyplývajících z problémů na nižších úrovních. NASA neměla ani stručný přehled anomálií, které mají být hlášeny, jestliže se vyskytnou během letu. Komunikační kanály a požadované informace musí být explicitně definovány. Nevyhnutelné jsou dva typy informačních toků:
(1) kompetenční (referenční) kanál, kterým se přenášejí cíle a politiky směrem dolůa
(2) měřící kanál, kterým se oznamuje aktuální stav věcí směrem nahoru.

Kompetenční kanál obsahuje důvody pro rozhodnutí, procedury a volby, které je třeba oznámit pracovníkům na nižších pozicích spolu s cíli a politikou za účelem vyhnutí se nežádoucím modifikacím vytvořeným na nižších úrovních řízení a dovolujícím detekci a korekci nesprávného pochopení a nesprávné interpretace. V měřícím kanálu je pro správné rozhodování podstatná zpětná vazba z provozních zkušeností a zprávy o technických neurčitostech a bezpečnostních problémech.

Organizace, které vyvíjejí rozsáhlý software pro velké projekty, jsou často úplně odděleny od bezpečnostních útvarů objednatele a informační tok mezi nimi prakticky neexistuje nebo je velmi omezený. Činnosti při vývoji softwaru mají sklon probíhat v relativní izolaci od systémové bezpečnosti a ostatních inženýrských činností, což také může vést k vážným bezpečnostním problémům.

2.8 Neefektivní technické aktivity

Skupina faktorů třetí úrovně (kořenových) přispívajících k haváriím odráží slabou úroveň implementace specifických činností nutných pro dosažení akceptovatelné úrovně bezpečnosti. Tyto problémy zahrnují: povrchní úsilí o dosažení bezpečnosti, neefektivní kontrolu rizik, chybné hodnocení změn a nesprávné shromažďování, zaznamenávání a používání informací důležitých pro bezpečnost.

Povrchní úsilí o dosažení bezpečnosti

Organizační útvary zajišťující bezpečnost se občas dostanou do byrokratických pastí, ve kterých se ocitají jiné organizace. Papírově vykázáno je všechno, co je splněno k danému termínu, nebo podle nároků na zajištění kvality. Ovšem to může být problémem pokud nastane stav, kdy to, co je vykázáno jako splněno, ve skutečnosti splněno není. Tento problém vyvstane nejpravděpodobněji tehdy, když jsou sami bezpečnostní inženýři zapojeni do přípravy projektu natolik, že ztratí svoji objektivitu a stanou se zastánci rozhodnutí přijatých řešitelskými skupinami tedy že deklarování splnění cíle je pro ně větší prioritou, než jeho faktické splnění.

Takovou práci bezpečnostních útvarů lze nazvat kosmetickým systémem bezpečnosti, který je charakteristický povrchním úsilím o bezpečnost a je obyčejným účetnictvím. Záznamy o nebezpečích jsou pedantsky zapsány dohromady s položkami, které velmi podporují a zdůvodňují každé konstrukční rozhodnutí i záměnu provedenou projektovým managementem a inženýry. V některých případech jsou provedeny adekvátní bezpečnostní analýzy, ale návazně na ně není zajištěno, aby nebezpečí byla pod kontrolou, a aby bezpečnostní zařízení byla správně nainstalována, udržována v provozuschopnosti.

Neefektivní kontrola rizik

Většina havárií nebyla výsledkem nedostatečných vědomostí o tom, jak jim předcházet, ale toho, že tyto vědomosti nebyly efektivně využity. Jak jsme se mohli přesvědčit z výše uvedených příkladů, významné faktory přispívající k haváriím byly téměř vždy identifikovány, ale nic se s nimi nedělalo, ať už v důsledku sebeuspokojení ze zajištění bezpečnosti, nebo z podcenění rizik. Dokonce i při snaze pracovníků odpovědných za bezpečnost jim nemusí být známy cesty prevence vážných a dobře pochopených nebezpečí. Je to vážný problém vzdělání, zvláště akutní při používání počítačů v bezpečnostně kritických systémech, kde programátoři vytvářející konkrétní software, mohou mít velmi slabé vědomosti z inženýrských praktik o zajišťování bezpečnosti. Pro některé havárie jsou nebezpečí identifikována a je snaha dostat je pod kontrolu, ale tato kontrola je neadekvátní. Jedním z frustrujících faktorů pracovníků usilujících o redukci rizik je, že výsledkem jejich redukce je pouhé přemístění rizika. Bezpečnostní opatření opravdu někdy způsobí havárii. Částečné roztavení aktivní zóny v jaderné elektrárně Detroit Fermi bylo např. způsobeno uvolněním zirkonové desky, která byla speciálně nainstalovaná pro snížení pravděpodobnosti tavení aktivní zóny. Trojúhelníkový kus zirkonia, který měl tekutý sodík v reaktoru usměrňovat, ho místo toho zablokoval.

Aby byla naše technologická opatření efektivní, potřebujeme pochopit, proč občas nefungují. Pro vysvětlení toho, proč byla minulá úsilí jao redukci rizik neúspěšná, se nabízejí 4 hlavní faktory: (1) používání „záplat“, které pouze eliminují specifické příčiny minulých havárií a neřeší bazální „díry“ projektu, (2) návrhy bezpečnostních zařízení, které vycházejí z nesprávných předpokladů, (3) bezpečnostní opatření, která zvyšují složitost

systémů a způsobují více havárií, než kterým zabraňují a (4) bezpečnostní zařízení jsou účinná pro dosažení jejich původních cílů, ale potom se používají k zdůvodňování redukce bezpečnostních rezerv.

Neúspěšné odstraňování bazálních „děr“ projektu

V některých případech technologické ochrany a zařízení nefungují proto, protože mají kompenzovat slabou organizaci nebo špatný návrh. Tuto úlohu splnit nedovedou. S odkazem na hierarchický model havárií je jasné, že je nepravděpodobné, aby změny provedené na druhé úrovni překlenuly nebo vyřešily nedostatečná omezení na třetí úrovni. Tato očekávání a spoléhání se pouze na evidenční kontrolu (checklists) provedených opatření způsobují neúspěšné odstraňování bazálních „děr“ v projektu. V evidenčních záznamech (checklists) se používají informace z předcházejících havárií. Přestože jsou užitečné pro poučení, tj. že se nezapomene na běžné věci, může jejich výlučné a slepé používání omezit faktory, které je třeba brát v úvahu dnes. Johnson [30] to dobře vystihl, když napsal, že se dají najít i třínásobné zámky na té bráně, kterou byli koně ukradeny, pokud jsou ostatní brány široce otevřené.

Zakládání ochrany na nesprávných předpokladech

Druhým důvodem, pro který mohou být opatření na redukci rizika neúspěšná je ten, že jejich působení je predikováno z nesprávných předpokladů. Kletz [34] v této souvislosti uvádí následující příklad. Zásobní nádrž byla naplňována jednou za den materiálem pro zpracování ve výrobě tak, aby jej bylo na dobu 24 hodin dostatek. Úkolem operátora bylo sledovat hladinu a v okamžiku, kdy byla nádrž naplněná na 90 %, měl vypnout plnicí čerpadlo a zavřít napouštěcí ventil. Tento úkol plnil operátor bezchybně 5 let, až jednou díky jeho momentální nepozornosti nádrž přetekla. Z nádrže vyteklo pouze malé množství, když to operátor zpozoroval a čerpadlo vypnul. Aby se podobným situacím předešlo, byla nainstalována ochrana proti vysoké hladině, která automaticky vypnula čerpadlo v okamžiku, kdy hladina v nádrži překročila 90 %. Všichni byli překvapeni, když asi po roce nádrž opět přetekla. Projektant ochrany počítal s tím, že operátor bude nadále sledovat hladinu při plnění nádrže a ochrana zasáhne jen v tom případě, když operátor výjimečně čerpadlo neodstaví. Mylně předpokládal, že šance současného selhání operátora i ochrany je zanedbatelná. Bohužel, tento odhad nebyl správný. Operátor zcela ponechal kontrolu hladiny nainstalované ochraně a svou pozornost věnoval svým ostatním pracovním povinnostem spoléhaje se na automatické odstavení čerpadla. Vedoucí s mistrem rozhodli, že operátor může být lépe využit i jinde. Ochrana selhala a nádrž přetekla. Bylo známo, že nainstalovaný typ ochrany má průměrnou dobu mezi selháními 2 roky, takže se mělo počítat s tím, že za tuto dobu může dojít k přetečení nádrže. Únik byl tentokrát daleko větší než předtím, protože operátor dělal něco jiného a nevěnoval hladině v nádrži žádnou pozornost. Tento případ není ojedinělý. Operátoři jsou často obviňováni z toho, že zapříčinili havárii, přestože stejná vina může být přisouzena konstruktérům, kteří nepochopili problémy chování člověka při monitorování procesů a měli nereální pohled na provoz zařízení.

Predikování funkce bezpečnostních zařízení na předpokladech, která nemusí být pravdivá (speciální předpoklady chování člověka), je vážnou chybou. Jedním z nich je běžněpředpokládaná nezávislost událostí nebo komponent. Jak bylo výše uvedeno, ochranná zařízení nepracují proto, protože události/jevy spolu souvisí, a tím zapříčiní koincidentní chyby ochranných zařízení.

Složitost

Třetím důvodem, proč bezpečnostní zařízení nemusí fungovat je, že se jimi může zvětšit složitost natolik, že v konečném důsledku zapříčiňují více havárií, než před kolika ochraňují. Takového zvýšení složitosti se častěji dosáhne tehdy, když jsou bezpečnostní zařízení a ochrany k původnímu řešení přidávána dodatečně. Když jsou nebezpečí identifikována hned v počátečních stádiích návrhu, mohou být odstraněna změnou původní koncepce, což je mnohem efektivnější, než snaha udržovat je pod kontrolou přidáváním dodatečných ochranných zařízení. Riziko může být redukováno bez zvyšování složitosti nebo nákladů a opatření redukce rizika mohou být účinnější.

Ochranné/bezpečnostní systémy jsou také doplňky standardního řešení technologického zařízení, které pomáhají navracet předmětná zařízení z nebezpečných provozních stavů do bezpečného provozu, nebo vygenerovat havarijní oznámení/signály o tom, že zařízení je v nestandardním stavu a představuje nebezpečí. Takovéto systémy jsou obyčejně drahé a jsou efektivní pouze tehdy, jestliže jsou mimořádně spolehlivé.

Mezi způsoby, kterými se ultra vysoká spolehlivost nejčastěji zajišťuje, patří redundance a diversifikace bezpečnostních systémů. Při jednom experimentálním leteckém výzkumu NASA se zjistilo, že všechny softwarové problémy, které se vyskytly během testovacích letů, pocházely z chyb v redundantním systému managementu řízení a ne z řídícího softwaru samotného, který pracoval bezvadně. Zdánlivá možnost lehkého přidávání dalších funkcí softwaru může nevědomě nabádat k doplnění funkcí počítačově řízených ochranných/bezpečnostních systémů, jako jsou například různé typy ověřovacích a testovacích funkcí. I zde se může složitost zvýšit tak, že nárůst rizika softwarových chyb je větší, než přidaná ochrana. Přidávání funkcí softwaru je lehké, ale určit, nakolik je to nutné, je daleko těžší.

Používání ochranných zařízení pro redukování bezpečnostní rezervy

V některých případech se bezpečnostním systémem dosáhne snížení rizika, ale v zápětí je tento využíván i pro zdůvodnění redukce bezpečnostní rezervy - například zvýšení výkonnosti je navrhováno zrychlením chodu zařízení. Čistým výtěžkem nemusí být redukce rizika, ale dokonce jeho zvýšení oproti původnímu zařízení. Pro letectvo to Perrow [52] vystihuje takto: „Nárůst bezpečnostního potenciálu neodpovídá technologickým zlepšením v letectvu, protože požadavky na rychlost, výšku, manévrovatelnost a létání za každého počasí se neustále zvyšují“. V okamžiku, kdy byl zaveden radarový systém pro předcházení kolizím, byla okamžitě redukována i minimální vzdálenost přiblížení letadel ve vzduchu. Odpovědnost leží na managementech, kteří používají zavedení bezpečnostních zařízení pro zdůvodnění redukce provozních nákladů, zvýšení produktivity a zisku, intenzivnější využívání času a pro redukci posádek.

Chybné hodnocení změn

Havárie často zahrnují i chyby z nesprávného vyhodnocení bezpečnosti po provedených změnách. Ve Flixborough se výrobní kapacita po provedených úpravách ztrojnásobila, ale bez náležité analýzy rizika. Také v Sevesu byl změněn provoz na výrobu různých chemikálií, které byly mnohem nebezpečnější, ale revize bezpečnosti nebyla provedena.

Každá změna, ať už hardwaru nebo softwaru, musí být vyhodnocena tak, aby se dalo určit, jestli jejím zavedením nebyla porušena bezpečnost. Změny v kritických částech hardwaru a softwaru vyžadují nejen kompletní regresní testování, ale úplnou analýzu systémové bezpečnosti. U vysoce nebezpečných systémů může být užitečnost navrhovaných

změn posouzena jako příliš relativní vůči nákladům na verifikování rizika souvisejícího s jejich zavedením.

Jedním z požadavků pro provedení efektivní analýzy změn je, že všechna bezpečnostní významná koncepční rozhodnutí musí být řádně zdokumentována. Systémoví inženýři a původní konstruktéři/tvůrci hardwaru i softwaru potřebují specifikovat omezení a předpoklady, ze kterých vycházely odhady bezpečnosti a bezpečnostně významné vlastnosti návrhu tak, aby ti, kteří zařízení provozují/udržují, neporušili nevědomky předpoklady bezpečnosti, nebo neeliminovali bezpečnostně významné vlastnosti projektu. Zodpovědní pracovníci, kteří musí dělat bezpečnostně významná rozhodnutí, musí důkladně poznat, proč tato rozhodnutí musí být přijata, aby neporušili výše uvedené předpoklady a vlastnosti bezpečnosti původního projektu.

Nedostatek informací

Zpětná vazba z provozních zkušeností je jedním z nejdůležitějších zdrojů informací pro navrhování, udržování a zlepšování bezpečnosti. Jsou významné dva typy dat:

(1) informace o poruchách a haváriích v jiných zařízeních a (2) údaje a trendy o poruchách ve vlastních zařízeních. Oba tyto typy dat musí být soustavně shromažďovány, vyhodnocovány a používány.

Shromažďování a zaznamenávání informací

Náročnost systematizování poznatků je důležitým faktorem při vysvětlování, proč dochází k podobným haváriím. Velká část historie havárií není kriticky posouzena a často ani není zaznamenána v použitelné formě. Přestože je známo, že vyšetřování havárií může poskytnout velmi užitečné informace pro zlepšení konstrukce nových systémů a pro vyhnutí se opakovaným podobným haváriím, lze jen těžko získat takové informace, které jsou dostatečně detailní proto, aby mohly být užitečné pro tyto účely. Například oficiální zpráva z vyšetřování požáru na stanici metra King`s Cross uvádí, že mezi odděleními správy metra byla jen velmi malá výměna informací a velmi slabé využití poznatků z jiných průmyslových odvětví a organizací.

Trendy, které musely být spojeny s anomáliemi „O“-kroužků na raketoplánu nebyly zpozorovány nebo hlášeny před havárií Challengeru. Během prvních devíti letůraketoplánu bylo nalezeno pouze jedno místní poškození O-těsnění. Mezi desátým a dvacátým pátým letem, který byl pro Challenger tragickým, byly u více než poloviny letůzjištěny lokální úniky přes O-těsnění, nebo eroze. Tyto do očí bijící změny chování „O“-kroužků měly být pozorovány a zřejmě dovedeny až do zjištění kořenových příčin. Nebyla provedena žádná analýza trendů. Přestože uváděným poruchám „O“-kroužků věnovali inženýři ve výrobě, při testech a letech během letů raketoplánu velkou pozornost, signifikantnost vyvíjejícího se trendu nebyla zaznamenána. Ředitel, zodpovědný za bezpečnost, spolehlivost a kvalitu v letovém středisku, během výslechů po havárii přiznal, že vyhnutí se této tragédii byla otázka shromažďování a vyhodnocování dat o celém letu správným způsobem. Závěrečná zpráva vyšetřovací komise udává, že zjišťování trendů je standardní a očekávanou funkcí pro zajištění spolehlivosti a kvality v každém programu. Dokonce i velmi povrchní prozkoumání výskytu chyb muselo indikovat, že se vyvíjí velmi vážná a potenciálně katastrofální situace na všech spojích raketových motorů s „O“-kroužky. Nezpozorování a neohlášení tohoto trendu lze v terminologii NASA popsat jen jako “vymizení kvality“, jako chyba programu vyloučit problémy, kterým se dá vyhnout. Kdyby tento program fungoval správně, k tragédii Challengeru by nedošlo. Trend měl být identifikován a analyzován tak, aby se zjistily fyzikální procesy, které destruovaly O-těsnění a ohrožovaly těsnost celého spoje.

Několik havárií, které měly katastrofální následky - TMI, Challenger, Bhopal, Černobyl, Therac-25, Titanic a jiné, si vyžádalo, aby jejich vyšetřování bylo provedeno pod dohledem vlád, nebo oficiálních institucí. Mnohé výsledky z vyšetřovacích zpráv těchto havárií jsou v předchozím textu této studie často citovány, protože poskytují podstatné informace pro potvrzení nebo vyvrácení hypotéz a pro poučení se z chyb, které by se už neměly opakovat. Je tomu tak proto, že vyšetřování byla provedena důkladně a v plném rozsahu.

Jakákoli pozorná vyšetřování příčin havárií mají vždy určité odchylky a neúplnosti. Nekompletní hodnocení, například ta, která ze všeho viní operátory, jsou horší než neužitečná, protože povzbuzují návrháře k tomu, aby ignorovali jiné faktory, které přispěly k haváriím. Operování s odpovědnostmi věci také komplikuje, protože příčinná informace může být použita jako podklad pro soud. Společnosti se mohou bránit tvrdému pohledu na havárii a jednotlivci nemusí poskytnout kompletní informaci ze strachu o práci.

Použití informací

Informace musí být nejen zaznamenány a dostupné, ale musí se i používat, aby byly účinné pro prevenci havárií. Operátoři jaderných elektráren v USA jsou povinni vyplnit poruchová hlášení (licensee event report - LER) vždy, když v provozu dojde k jakékoliv události. Přestože je k dispozici i zpětná vazba z těchto hlášení, v minulosti nebyla adekvátně využívána [20]. Vyšetření TMI havárie ukázalo, že lepší využívání zpráv LER mohlo havárii TMI zabránit. Opravdu, před TMI firma Babcock & Wilcox neměla žádnou formální proceduru pro analýzu problémů v elektrárnách, které postavili a ani na prohlížení hlášení LER, které byly poslány z jiných JE.

Studie o bezpečnostních informačních systémech různých společností, vypracovaná Kjellenem [33] ukázala, že všeobecně byly tyto systémy neadekvátní pro dosažení požadavků systematické kontroly havárií, např. shromážděná data byla nevhodně filtrována a proto nepřesná, použité metody byly nedostatečné pro analýzy a sumarizování příčinných dat, informace nebyly předkládány těm, kteří dělají rozhodnutí, a takovým způsobem, aby pro ně měly smysl. Následkem toho bylo, že poučení z předcházejících zkušeností bylo opožděné a neúplné.

Efektivní systém, ať už formální nebo neformální, vyžaduje pro ohlašování poruch delegování adekvátní odpovědnosti podle významu instituce, které se hlášení podává (vedení podniku, vládní úřady, ...), dále systém pro zpracování poruchových hlášení, procedury pro analýzy poruch a identifikování příčinných faktorů a procedury pro stanovování nápravných opatření.

Inženýři formulují získané zkušenosti do podoby standardů, návodů, norem a kontrolních dotazníků (checklists). Tyto formy už mají svou tradici a umožňují dobré šíření osvědčených řešení. Postupy pro identifikaci nebezpečí vycházejí také z předcházejících zkušeností, ale využívání standardů a norem napomáhá tomu, abychom se mohli vyhnout i těm nebezpečím, které nebyly specificky identifikovány a mohou být pro konstruktéry a analytiky nebezpečí neznámé.

Naneštěstí softwarové inženýrství nemá ještě dostatečně dlouhou zkušenost potřebnou pro vyvinutí výše uvedených standardů a norem a zatím si nevyvinulo efektivní prostředky pro širší využívání poznatků ze zjištěných chyb. Neumann [51] napsal knihu o poruchách, které byly neformálně oznamovány redakcím časopisů o počítačích. Neexistuje však způsob, jak posoudit správnost většiny z uvedených hlášení a v mnoha částech těchto zpráv nejsou zahrnuty dostatečné informace, kterých by bylo možno využít k prevenci budoucích poruch. Průřezová vyšetřování poruch souvisejících s počítači nejsou až na

několik výjimek do teď publikována ani jinak shromažďována.

2.9 Shrnutí

V této kapitole jsme podrobně probrali nejdůležitější příčinné faktory třetí úrovně, které se významně podílely při haváriích v minulosti. Některé z nich se vztahují k nedostatkům kultury bezpečnosti v daném průmyslovém odvětví, neboli organizaci a k postojům managementu, jako např. sebeuspokojení, přehlížení, nebo přiřazování nízké priority bezpečnosti, nedostatečné postupy pro rozřešení konfliktních cílů atd.

Sebeuspokojení bylo společným faktorem velkých havárií. Faktory související se sebeuspokojením jsou podceňování rizika, přílišné spoléhání se na redundanci, nerealistické odhadování rizika, ignorování událostí s nízkou pravděpodobností a současně s těžkými následky, předpoklad snižování rizika, podceňování rizika ze softwaru a nevšímavost vůči varovným znamením.

Zvláštními nedostatky v kultuře bezpečnosti jsou problémy řešení vzájemně konfliktních cílů. Aby se konfliktní cíle a zamýšlené změny na zařízeních vyřešily správně, je nutné mít emotivní program systémové bezpečnosti, který je podporován managementem na všech úrovních řízení. Bezpečnost musí být složkou každého rozhodování, a to tak, aby technická zlepšení nebyla zrušená špatnými rozhodnutími managementu, nebo organizační kulturou podniku/odvětví, která klade větší důraz a pozornost na jiné cíle, než na bezpečnost.

V jiných případech se potvrdil upřímný zájem a snaha managementu o zajištění bezpečnosti, ale organizační struktura byla neefektivní pro implementování této snahy. Např. autorita a odpovědnost za bezpečnost se rozplynula v organizaci, bezpečnostní personál měl nízký status, nebo nebyl nezávislý na projektovém managementu a komunikační kanály pro bezpečnostní problémy byly nedostatečné.

Poslední skupina zahrnuje špatné implementování specifických technických aktivit nevyhnutelných k dosažení akceptovatelné úrovně bezpečnosti, povrchní úsilí o bezpečnost, neefektivní kontrolu rizika, chybné opětovné vyhodnocení bezpečnosti po provedených změnách a nedostatky ve sběru (shromažďování), zaznamenávání, vyhodnocování a využívání informací z provozu.

3 TEORIE SYSTÉMŮ

3.1 Poznámky k teorii systémů

Správné porozumění technologii vyžaduje pochopení její historie, vědeckého základu, kulturního a sociálního prostředí, ve kterém byla vyvinuta a ve kterém se využívá. Systémová bezpečnost má svoje kořeny v bezpečnostním inženýrství, která se datuje už od 19. století. Relativně nová disciplína systémové bezpečnosti je odpovědí na podmínky, které vznikly po 2. světové válce, když se vyvinuly její “rodičovské“ disciplíny - systémové inženýrství a systémová analýza na řešení nových a komplexních inženýrských problémů. Vědec-

ká báze všech těchto nových proudů inženýrství spočívá v teorii systémů, jejíž vývoj začal v třicátých letech minulého století.

3.2 Inženýrství bezpečnosti před 2. světovou válkou

Lidé se vždy zajímali o svou bezpečnost. Dříve než došlo k rozvoji průmyslu, byly pro lidi největší hrozbou přírodní katastrofy. S nástupem průmyslové revoluce v Evropěa USA se situace začala měnit. Pracující v továrnách byli vnímáni jen jako náklady a často se s nimi zacházelo hůře než s otroky s tím rozdílem, že otrok byl majetkem svého pána a ten si svůj majetek chtěl chránit. Najmutí, nebo propuštění dělníka nic nestálo. Převažujícím postojem bylo, že když lidé přijmou zaměstnání, akceptují i rizika s ním spojená a musí být dostatečně pozorní, aby se nebezpečí vyhnuli. Tehdy byly továrny plné nebezpečí, např. stroje bez ochranných štítů, otevřené jámy, nechráněné dopravní pásy apod. Neexistovaly žádné požární únikové východy a osvětlení bylo většinou nevyhovující. Jen těžko by se dal najít den, ve kterém se nějaký dělník nezranil nebo dokonce nezahynul. Pracovní právo bylo také pouze v počátcích a zaručovalo pouze minimální ochranu dělníků [18].

Hrůzostrašné pracovní podmínky vedly k sociálním vzpourám, které vedli aktivisti a vedoucí odborů. Horníci, železničáři a ostatní robotníci se začali zajímat o nebezpečí své práce a agitovat za lepší pracovní podmínky. Koncem 19. století vznikaly v USA dobrovolné organizace pro bezpečnost, jako např. Americké sdružení pro veřejné zdraví (American Public Health Association), nebo Národní sdružení požární ochrany (National Fire Protection Association). Prvotní úsilí o bezpečnost se zaměřovalo více na zdraví, než na bezpečnost, protože havárie byly vnímány jako náhodné události, které nebylo možno odvrátit.

Péče o bezpečnost práce začala dříve v Evropě než v Americe. Otto von Bismarck stanovil v Německu zaměstnavateli v r. 1880 povinnou náhradu škod a pojištění bezpečnosti práce placené dělníkům. Z politického hlediska to byl krok proti socialistům a měl ukázat, že jeho vláda dělá dostatečné sociální reformy pro zlepšení poměrůpracující třídy. Tento Bismarckův příklad se brzy rozšířil do většiny zemí Evropy.

Dalším typem zákonné ochrany bezpečnosti práce byl zákon pro továrny a dílny v Anglii z r. 1844, který jako první nařizoval ochranu před haváriemi a úrazy způsobenými transmisními převody z vodních, nebo parních zdrojů energie. Později podobné zákony stanovily standardy pro vysokotlaká parní zařízení a vysokonapěťová elektrická zařízení.

V USA zaměstnavatelé zůstávali lhostejní k mnoha smrtelným úrazům svých zaměstnanců. Pravděpodobně až sociální revolty a agitace odborářů proti špatným pracovním podmínkám vedly k sociálním reformám a k zásahu vlády na ochranu dělníků a veřejnosti. Federálnímu zákonu předcházely zákony v jednotlivých státech. Např. v r. 1869 byl vydán v Pensylvánii zákon o bezpečnosti v dolech a v r. 1877 byl vydán v Massachusetts zákon o ochraně pracovních strojů a pořádku v továrnách. První úspěšný zákon o bezpečnosti práce a strojů v USA byl vydán v r. 1852 a stanovil požadavky na kotle parních lodí. Jeho vydání bylo výsledkem tlaku veřejnosti a série námořních katastrof, při kterých zahynuly tisíce lidí. První zákon o úrazovém odškodňování dělníků byl vydán ve státě New York v r. 1908. Tento zákon požadoval po zaměstnavatelích, aby dělníkům platili odškodné za úrazy, které se staly při práci, bez ohledu na zavinění.

Když management podniků zjistil, že je povinen platit za úrazy při práci, začal vyvíjet úsilí na prevenci úrazů, což bylo zrodem organizovaného hnutí za průmyslovou bezpečnost. Majitelé a manažeři si uvědomili, že havárie je stojí mnoho peněz ve smyslu nižší produktivity a začali brát bezpečnost vážně. První útvar průmyslové bezpečnosti ve firmě byl založen

začátkem r. 1890. V podnicích, kde často docházelo k těžkým úrazům (např. hutě, doly), se začínaly vydávat bezpečnostní předpisy/normy. V tomto období prezident korporace US Steel Corporation napsal: „Korporace očekává od všech svých společností vynaložení jakéhokoliv úsilí, které vede k praktické prevenci úrazů jejich zaměstnanců. Náklady, nevyhnutelné pro tyto účely, budou schváleny. Nic, co může zlepšit ochranu dělníků, nesmí být zanedbáno“ [31].

Někteří inženýři si uvědomili potřebu prevence nebezpečí hned na začátku nástupu průmyslové výroby. James Watt upozorňoval na nebezpečí vysokotlakých parních strojů už začátkem r. 1800. Davyho bezpečnostní lampa, vynalezená v tomto období, pomáhala snížit nebezpečí exploze metanu v dolech. V r.1869 vyvinul George Westinghouse vzduchovou brzdu, která výrazně zvýšila bezpečnost železniční dopravy. Patentový úřad pro bezpečnost strojů v USA vydal první patent na bezpečnostní pojistku pro stroje na plnění lahví sodou. Koncem 19. století už začali inženýři považovat bezpečnost, stejně jako funkčnost, za regulérní složku projektu. Jednou z prvních organizací pro studium havárií byla Společnost pro prevenci havárií v továrnách, nazývaná též Mulhousekou společností, protože byla založená ve městě Mulhouse ve Francii. Ta pořádala pravidelná roční setkání za účelem výměny poznatků o zlepšovaní bezpečnosti v továrnách a vydávala encyklopedii technik prevence úrazů v letech 1889 a 1895 [63]. Začátkem 20. století byla založena Německá inženýrská společnost pro prevenci havárií. Tehdy se začalo v inženýrské technické literatuře deklarovat, že bezpečnost musí být zabudována již v projektu. První článek věnovaný bezpečnému návrhu strojů byl prezentovaný Americké společnosti strojního inženýrství Johanem H. Cooprem v r. 1891. V r. 1899 Johan Cauder vydal v Anglii knihu: „Prevence havárií v továrnách“, kde uvedl statistiky havárií a detailně popsal bezpečnostní/ochranné zařízení. V knize je zdůrazněna potřeba předvídání havárií a zabudování bezpečnosti. Autor dokazuje, že legislativa k donucení výrobců zajišťovat bezpečnost výrobků není nutná, protože síly tržního mechanizmu je k tomu budou dostatečně nutit. Později, po přestěhování do USA, autor tento svůj názor změnil a v r. 1911 se dožadoval legislativního nátlaku na zaměstnavatele pro zajištění bezpečnosti výrobků [11].

Otázky bezpečnosti práce a strojů byly publikovány nejdříve v odborářském tisku. První technický časopis věnovaný jen otázkám prevence havárií, The Journal of Industrial Safety, začal vycházet v USA v r. 1911. V r. 1914 byly v USA publikovány první bezpečnostní normy, které byly sestaveny pod vedením Carla M. Hansena [23]. Podle těchto norem zajištění bezpečnosti vyžaduje: (1) zajištění největší možné bezpečnosti pro operátory a ostatní dělníky, (2) automatické působení ochran a bezpečnostních zařízení jak jen je to možné, (3) být integrální částí zařízení samotných a (4) neomezovat výstupy a efektivitu zařízení, na kterých jsou ochranná zařízení instalována. První studií, která se zabývala bezpečností jako samostatným předmětem, byla práce H. W. Heinricha, z r. 1929, ve které autor zpracoval 50 000 průmyslových havárií. Konstatuje se v ní, že na každý těžký pracovní úraz připadlo 29 menších zranění a 300 poruch bez ohlášených zranění a také, že těžkému zranění předcházelo tisíce skoronehod. Tato hypotéza se stala známou jako Heinrichova pyramida, která je statistickým základem pro eliminování nebezpečí ještě před tím, než dojde k těžkému úrazu.

Jiná studie [67], pocházející ze stejného období, se zabývala vyvrácením tehdy široce převládajícího přesvědčení, že bezpečnější zařízení s bezpečnostními ochranami jsou neefektivní a méně produktivní. Byla to velmi rozsáhlá studie, na jejímž vypracování se podílely velké inženýrské společnosti, zaměstnanci dvaceti průmyslových odvětví a šedestát výrobních skupin. Závěrečná zpráva potvrdila hypotézu, že produktivita roste se zvyšující se bezpečností, což je poučení, které by měli vzít v úvahu mnozí lidé i dnes. Studie vysvětluje historický úkaz nárůstu počtu havárií i přes úsilí průmyslové bezpečnosti, které je věnováno jejich redukci. Zjistilo se, že zvyšování počtu havárií souvisí s velkým nárůstem rychlosti,

s jakou se americký průmysl mechanizoval. Mechanizace ovlivnila bezpečnost třemi způsoby: (1) odstranila používání ručního nářadí, (2) došlo k většímu vystavení údržbářského personálu nebezpečí a (3) umožnila zrychlení provozu a dávkování vstupního materiálu. Závěr studie je, že přestože se i v průmyslu zvýšilo vystavení se nebezpečí na člověka za hodinu, produktivita vykazovaná na člověka a hodinu se natolik zvýšila, že nebezpečí v poměru k produktivitě se ve skutečnosti snížilo.

V prvních fázích zájmu o bezpečnost byl kladen důraz na nebezpečné fyzické podmínky. Jejich náprava byla významným pokrokem na počátku 20. století. Když zlepšení už nebyla tak výrazná, hledala se další vysvětlení. Heinrich publikoval v r. 1931 knihu s názvem Prevence průmyslových havárií, ve které dokazuje, že havárie jsou výsledkem nebezpečných činností a nebezpečných podmínek a tvrdí, že lidé způsobují mnohem více havárií, než nebezpečné podmínky [25]. Toto tvrzení se stalo základem pro mnohé budoucí argumenty.

Odvolávajíce se na výše citovanou Heinrichovu hypotézu, začali oponenti mechanického řešení bezpečnosti upírat svoji pozornost od nebezpečných strojů na nebezpečné činnosti uživatelů. Tvrdilo se, že dělníci se sklonem k selhání, dohromady s vlastní neopatrností, byli zodpovědní za 85 až 90 % všech průmyslových havárií. Většina dnešních údajů o haváriích ukazuje, že lidé jsou daleko častěji obviňováni za způsobené havárie, než nebezpečné podmínky, a to dokonce i tehdy, když nebezpečné podmínky nevyhnutelně přivodí selhání člověka. Heinrich byl zároveň prvním, kdo vypracoval koncepční model pro vybudování teoretického rámce průmyslové bezpečnosti. Předložil “teorii domina“ způsobení havárie, která je v porovnání s dnešními teoriemi značně jednoduchá.

Druhá světová válka si vyžádala větší snahu o bezpečnost, než předcházející období. Současně s enormním nárůstem válečné výroby, největším v historii, hrozivě vzrostl počet havárií a úrazů. Jejich výskyt byl tak vysoký, že Alianci kvůli nim hrozilo nebezpečí porážky. Statistiky dokázaly, že při průmyslových haváriích zahynulo více lidí než na frontě. Po tomto zjištění byl iniciován velký program bezpečnosti a ochrany zdraví, ve kterém byly pro průmyslovou bezpečnost vycvičeny tisíce lidí. Po skončení války zaniklo i mnoho aktivit pro bezpečnost a zdraví, protože už dále neplatily vysoké válečné priority a zájem o bezpečnost tak (na krátko) poklesl.

S návratem normálních podmínek a prosperity se starost o bezpečnost a zdraví opět ukázala jako nevyhnutelná a výskyt úrazů a havárií se dramaticky snížil [65]. Poválečné období dalo vyrůst novému přístupu k bezpečnosti založenému na principech systémového inženýrství. I přes snahu některých inženýrů posilovat ideu zabudování bezpečnosti přímo do výrobků a průmyslových procesů, byla většina bezpečnostních programů založena na „a posteriori“ filosofii, tj. po havárii se provede podrobné vyšetřování a stanoví se, jak předcházet podobným haváriím v budoucnosti. Protože většina průmyslové výroby má relativně malý rozsah, vývoj nových, bezpečnějších výrobků a procesů byl značně pomalý při poučení z předcházejících chyb. Nástupem narůstající složitosti a ceny nových výrobků se předcházející přístup učení z chyb stal neekonomický, až nepřípustný. Objevením a využíváním vysoko energetických zdrojů, jakými jsou např. exotická paliva, vysokotlaké systémy a jaderná štěpná reakce, se zvětšily potenciální dopady havárií. V případě některých průmyslových odvětvích, např. v jaderném průmyslu, je už jen jedna havárie považovaná za nepřípustnou. Prudký rozvoj technologií po druhé světové válce přinutil průmysl přemýšlet v terminologii teorie systémů.

3.3 Teorie systémů

Počátky teorie systémů se datují do třicátých let minulého století a tato teorie je považována za reakci na určité limity vědy při zvládání složitosti. Dvěma hlavními představiteli tohoto přístupu byli Norbert Wiener, jehož specializací bylo inženýrství řízení a komunikace v technice a Ludwig von Bertalanffy, specializující se v biologii. Bertalanffy zdůrazňoval, že ideje z rozličných oblastí lze kombinovat do všeobecné teorie systémůa je proto považován za zakladatele tohoto přístupu [27].

Teorie systémů je doplňkovým přístupem a reakcí na vědecký redukcionismus. Redukování, opakovatelnost a vyvratitelnost formují společně základ vědeckých metod. Princip analytické redukce ve vědeckém přístupu, který spočívá v rozdělení problému na samostatné části a jejich následné separátní zkoumání, je spojován s Descartesem.

Princip redukcionizmu spočívá ve třech předpokladech [27]:

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

Jsou to smysluplné předpoklady pro mnohé fyzikální zákonitosti takových systémů, ve kterých se projevuje organizovaná jednoduchost [70]. V těchto systémech je dokonale známa povaha jejich interakcí a interakce komponent mohou být zkoumány po párech, což znamená, že počet zvažovaných interakcí je limitován. To je možné jen u takových systémů, které jsou pro účely analýz rozdělitelné vzájemně se neovlivňujícími subsystémy, aniž by byly zkresleny výsledky. Tento přístup je mimořádně efektivní ve fyzice a je aplikovaný zejména ve strukturální mechanice.

Druhým typem systémů jsou ty, které teoretici označili za neorganizovanou složitost, což znamená, že v nich neexistuje podkladová struktura, která dovoluje efektivně aplikovat redukcionizmus při jejich zkoumání. Tyto systémy však mohou být často zkoumány jako agregáty, tj. komplexy, jejichž chování se dá studovat statisticky. Ve fyzice se tento přístup uplatnil ve statistické mechanice.

Třetí typ systémů zastupuje organizovanou složitost (komplexnost). Jsou to systémy příliš složité pro úplnou analýzu a příliš organizované pro statistiku. Je to právě ten typ systémů, které popisují mnohé komplexní inženýrské systémy poválečné éry, jako jsou například biologické a sociální systémy. Organizovaná složitost obzvlášť dobře reprezentuje problémy, na které se naráží při tvorbě složitých softwarů.

Systémový přístup se zaměřuje na systém jako celek a ne na jeho samostatné části. Vychází z předpokladu, že některé vlastnosti systémů mohou být adekvátně zkoumány jako celek jen tehdy, když se vezmou v úvahu všechny vlastnosti a proměnné daného systému a souvislosti vzájemných sociálních a technických aspektů[56]. Aspekty a proměnné systémů se odvodí ze vzájemných vztahů mezi částmi systémů z toho, jak vzájemně mezi sebou interagují a ladí. Systémový přístup se soustřeďuje na analýzu a design celku a jeho odlišnosti od komponent a částí.

Teorie systémů vychází z několika axiomatických definicí. Systém je množina prvků, které se společně projevují jako celek k dosažení určitých společných cílů resp. výsledků. Všechny prvky jsou vzájemně provázány a buď přímo, nebo nepřímo spjaty jeden s druhým.

Tato představa systému je založena na předpokladech, že systémové cíle je možno definovat, a že stavba systému je atomistická, tzn. že systém může být rozdělený na jednotlivé komponenty a mechanizmus jejich vzájemných interakcí lze popsat.

Stav systému je v kterémkoliv časovém okamžiku určený množinou relevantních vlastností, které popisují systém v daném čase. Okolí systému je množina komponent a jejich vlastností, které nejsou částmi systému, ale jejichž chování může ovlivňovat stav systému. Hranice mezi systémem a okolím je definovaná jako vstup nebo výstup čehokoliv co přes ni přechází. A nakonec hierarchie systémů představuje skutečnost, že každá množina prvků, kterou můžeme považovat za systém, je všeobecně přinejmenším potenciálně částí hierarchie systémů, tzn. že systém může obsahovat podsystémy a také může být částí většího systému.

Je důležité připomenout, že systém je vždy pouze modelem, abstrakcí v mysli analytika. V jednom a tom samém systému může pozorovatel vidět jiné účely než jeho projektant (pokud jde o umělý, člověkem vytvořený systém). Proto je třeba, aby pozorovatel i projektant definovali (1) hranice systému, (2) vstupy a výstupy, (3) prvky/komponenty, (4) strukturu, (5) relevantní interakce mezi komponenty a mechanismem, kterým si systém zachovává integritu a (6) účel resp. cíl, pro který má smysl považovat danou množinu prvků za koherentní entitu.

Teoretické základy pro zkoumání systémů projevujících organizovanou složitost jsou založeny na dvou párech idejí, kterými jsou emergentnost a hierarchie jako první dvojice a komunikace a řízení jako druhá dvojice.

Emergentnost a hierarchie

Obecný model organizované složitosti se dá vyjádřit termíny hierarchie úrovní organizace, kde je každá vyšší úroveň složitější než předcházející pod ní a má emergentní vlastnosti. Emergentní vlastnosti neexistují na nižší úrovni, nemají smysl v jazyku příslušejícím nižším úrovním. Např. tvar jablka, přestože by byl vysvětlitelný v termínech jablečných buněk, nemá smysl popisovat na této nízké úrovni. Pojem “emergentní“ vyjadřuje chápaní vývoje, jehož vyšší forma existence vzniká na základě nižší, a to tím, že nižší prvky vstupují do nových, na nižší úrovni neznámých souvislostí. Říká, že na dané úrovni složitosti jsou některé vlastnosti, které jsou pro tuto úroveň charakteristické (emergentní), neredukovatelné.

Hierarchie zkoumá základní rozdíly mezi jednotlivými úrovněmi složitosti. Jejím cílem je vysvětlit vztahy mezi rozdílnými úrovněmi, tj. čím jsou generovány, co je odděluje a co je spojuje. Emergentní vlastnosti sdružené s množinou komponent na jedné úrovni hierarchie se vztahují k omezením jejich stupňů volnosti. Popis emergentních vlastností vyplývajících z uložených omezení vyžaduje jazyk vyšší úrovně (metajazyk), než je úroveň, která popisuje samotné komponenty.

Vzhledem k předmětu této studie je jasné, že bezpečnost je emergentní vlastností systémů. Určit, jestli je jaderná elektrárna akceptovatelně bezpečná, není možné prověřením jednotlivých pojistných ventilů elektrárny. Vyjádření o bezpečnosti ventilů, stejně jako i např. o bezpečnosti softwaru bez upřesnění kontextu, o jaké ventily se jedná nebo jaký byl použit software, nemá smysl. Učinit by bylo možno závěry o spolehlivosti ventilů, kde je spolehlivost definována jako pravděpodobnost, že ventily budou plnit svoji specifickou funkci během určité doby a za daných podmínek. To je jeden ze základních rozdílů mezi bezpečností a spolehlivostí. Bezpečnost může být určena jen vztahy mezi ventily a ostatními komponentami elektrárny, ale jen v kontextu celku. Pro názornost lze uvést příklad: vstrčí-li dělník ruku do lisu, stroj mu ji spolehlivě rozdrtí. Stroj je spolehlivý, ale ne bezpečný. Ochra-

na proti tomuto nebezpečí spočívá v instalaci fotobuňky, která zablokuje stroj v okamžiku, kdy je ruka v aktivní zóně stroje. Funguje-li tato ochrana spolehlivě, pak lze konstatovat, že stroj je ve smyslu vzniku podobného úrazu současně spolehlivý a bezpečný. Ostatní možnosti poškození zdraví však zohledněny nejsou.

Námi uvedený hierarchický model havárií je postaven na hierarchii úrovní, přičemž omezení, nebo jejich absence na vyšších úrovních ovládá, nebo dovoluje chování na nižších hierarchických úrovních.

Komunikace a řízení

Druhým párem pojmů teorie systémů je komunikace a řízení. Omezení kladená na aktivity probíhající na určité úrovni hierarchie, které definují zákony chování na této úrovni, dávají smysl na vyšší úrovni řízení a jsou určitým druhem řízení. Hierarchie jsou charakterizovány řídícími procesy na styčných plochách mezi jednotlivými úrovněmi. Spojení mezi řídícími mechanismy, které byly studovány v přírodních systémech a mezi člověkem vytvořenými systémy, vysvětluje část teorie systémů známá jako kybernetika resp. teorie regulačních obvodů.

Řízení v otevřených systémech, tj. v takových, které mají vstupy a výstupy z/do svého okolí, vyžaduje přítomnost komunikace. Bertalanffy rozlišuje mezi uzavřenými systémy, ve kterých jsou komponenty nezaměnitelně nastaveny v rovnováze a otevřenými systémy, které mohou být z rovnováhy vyvedeny změnami v jejich okolí. Zdůrazňuje, že organizmy, které reprezentují otevřené systémy, mohou dosáhnout rovnováhy (stacionárního stavu), která je závislá na kontinuálních, vzájemných výměnách s okolím.

Tímto způsobem se můžeme podívat i na umělé (člověkem vytvořené) systémy, jakými jsou např. továrny a složité technologické systémy. Projektant takovýchto děl musí zvažovat nejen jednotlivé komponenty, nebo zařízení továrny, ale i továrnu jako celek. Fungování továrny musí být řízeno tak, aby byly splněny cíle výroby a dodrženy nákladové, bezpečnostní a kvalitativní omezení. Vedení závodu dostává informace o stavu provozu z měřitelných ukazatelů pomocí zpětné vazby a využívá je pro iniciování řídících/regulačních zásahů tak, aby se provoz vrátil do odpovídajícího stavu. To dosvědčuje, že udržování hierarchie v každém otevřeném systému vyžaduje samostatnou množinu procesů pro přenos informací, které jsou nevyhnutelné pro kontrolu a regulaci.

3.4 Systémové inženýrství

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

- velkým množstvím částí, počtem replik identických částí, prováděných funkcí a nákladů,
- složitostí v tom smyslu, že změna jedné proměnné ovlivňovala mnohé další proměnné a to navíc nelineárním způsobem,
- poloautomatizací, tj. s rozhraním člověk-stroj, kde člověk vykonává určité funkce a stroj vykonáva jiné, a
- nepredikovatelností, tj. nahodilostí vstupů a jiných poruch okolí.

Hlavní principy systémového inženýrství jsou:

- definování cílů a ladění činnosti systému pro jejich dosažení,
- stanovení a používání kritérií pro proces rozhodování,
- vyvíjení alternativ,
- modelování systémů pro analýzy a
- implementace managementu a kontroly.

Systémové inženýrství bylo nejintenzivněji využíváno v letectví a ve zbrojním průmyslu při vývoji balistických raket. Uvedené principy jsou dnes všeobecně považovány za dobrou inženýrskou praxi. Pokud je většina inženýrství založená na technologii a vědě, systémové inženýrství považuje za ekvivalentní významnou složku svojí praxe i management inženýrských procesů. Cílem systémového inženýrství je optimalizace provozu systémů podle prioritních kritérií návrhu. Základem každého přístupu pro dosažení tohoto cíle je výchozí předpoklad systémového inženýrství, že optimalizace jednotlivých komponent nebo podsystémů všeobecně nezaručuje vytvoření optimálního systému. Je to známý fakt, že zlepšení některého z podsystémů, může ve skutečnosti zhoršit vlastnosti celého systému. Když si uvědomíme, že podle principu hierarchie je každý systém vlastně podsystémem nějakého většího systému, představuje tento princip prakticky neřešitelný problém.

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

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

3.5 Systémové analýzy

V průběhu padesátých let minulého století vyvinula RAND Corporation paralelně s rozvíjením systémového inženýrství metodologii nazvanou systémová analýza pro racionální postup při vyhodnocování alternativ návrhů při procesu rozhodování. Ve stručnosti lze říci, že systémová analýza je metoda pro rozsáhlé ekonomické odhadování nákladů a dopadů různých způsobů dosažení určitého cíle. Systémová analýza je provázaná s operačním výzkumem, je však více ucelenější, méně kvantitativní a více orientovaná směrem k širším strategickým a politickým otázkám [27]. Ve většině případů nedokážeme eliminovat všechny složky neurčitosti při procesech rozhodování, protože k tomu nelze získat všechny relevantní informace. Z toho vyplývá, že následky jednotlivých směrů postupu nemohou být kompletně determinovány. Systémová analýza poskytuje organizovaný proces pro získávání a zjišťování specifických informací souvisejících s daným rozhodnutím. Systémové inženýrství a systémová analýza jsou už dlouhé roky fakticky sloučeny a využívány při tvorbě komplexních systémů člověk-stroj, kde systémová analýza zabezpečuje údaje pro proces rozhodování a organizuje postupy výběru nejlepší alternativy návrhu. Tyto dvě disciplíny tvoří spolu teoretický a metodologický základ systémové bezpečnosti.

3.6 Základy systémové bezpečnosti

Tuto část je vhodné začít poznámkou pana Greenwalta, bývalého prezidenta firmy DuPont, že jeho firma má už 150-letý program bezpečnosti. Firemní program bezpečnosti byl ustanoven na základě francouzského zákona, který požadoval, aby výrobci výbušnin žili v areálu továrny spolu se svými rodinami.

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

Stručná historie systémové bezpečnosti

Počátek vývoje systémové bezpečnosti, jako samostatné disciplíny, spadá do období bezprostředně po ukončení 2. světové války a je spjat s leteckými inženýry. Vojenské letectví má dlouhodobě špatné zkušenosti s leteckými haváriemi. Např. od r. 1952 do r. 1966 ztratilo 7715 letadel, ve kterých zahynulo 8547 osob včetně 3822 pilotů. Vina za většinu z těchto havárií byla na pilotech. Mnozí inženýři leteckého průmyslu však nebyli přesvědčeni, že příčina havárií je tak jednoduchá. Argumentovali, že bezpečnost musí být navrhována a zabudován do letadel právě tak, jako jeho manévrovatelnost, stabilita a strukturální integrita [48,64].

Pod vedením Jeroma Lederera byly v r. 1954 uspořádané semináře Nadace letecké bezpečnosti, na kterých se společně scházeli inženýři, operátoři leteckého provozu a manažerský personál. Na těchto seminářích byl poprvé použit termín „systémová bezpečnost“. Ve stejné době vojenské letectvo začalo pořádat symposia, kde zdůrazňovala profesionální přístup k bezpečnosti motorů, elektro zařízení, přístrojů letové kontroly a jiných částí letadel, avšak nepřistupovala k bezpečnosti jako k systémovému problému.

Když vojenské letectvo začalo vyvíjet mezikontinentálně balistické rakety, nebylo už možné obviňovat piloty za havárie těchto raket a za jejich těžké následky. Tekuté palivo, které používali v prvních raketových motorech, bylo svou vysokou toxicitou daleko nebezpečnější než bojové plyny ve 2. světové válce a svou reaktivností destruktivnější, než většina v tom období používaných výbušnin [22].

V tomto období byl Úřad jaderného dozoru v USA (NRC) vyzván k veřejné debatě o bezpečnosti jaderné energie, civilní letectví se snažilo redukovat havárie letadel, aby přesvědčilo skeptickou veřejnost k využívání letecké dopravy, chemický průmysl budoval větší továrny na výrobu stále nebezpečnějších chemikálií. Tyto paralelní aktivity vyústily do rozličných přístupů řešení problémů bezpečnosti.

Systémová bezpečnost vzešla z programu vývoje interkontinentálních balistických raket. V padesátých letech, kdy byly vyvíjeny rakety Atlas a Titan, vznikl intenzivní politický tlak na získání nosiče pro jaderné hlavice. Ve snaze zkrátit čas mezi počítačovým konceptem projektu a dosažením provozního stavu byl souběžně vyvinut a používán speciální inženýrský přístup. V rámci tohoto přístupu byly rakety a odpalovací zařízení, ve kterých byly rakety udržovány v pohotovosti, budovány současně s testy raket a výcvikem personálu. Vojenské letectvo si uvědomovalo, že tento přístup by mohl vést k mnohým nákladným do-

datečným změnám a úpravám, avšak vůči ceně za nepřipravenost na nukleární válku bylo pro získání času cokoliv levné. Fungování takovéhoto přístupu si vyžádalo enormní úsilí a tomu odpovídající náklady [58].

V prvních raketových projektech nebyla systémová bezpečnost identifikována a přidělována jako specifická zodpovědnost konkrétní osobě/orgánu. Naopak, jak bylo tehdy zvykem, byl za bezpečnost odpovědný projektant, manažer a hlavní inženýr. Do těchto projektů však vstoupila vyspělá technologie a podstatně větší složitost než v projektech předcházejících a nevýhody standardního přístupu k bezpečnosti se staly zjevnými, i když se na mnohé problémy interface podsystémů přicházelo už příliš pozdě.

Havárie raketových střel byly velmi drahé a výsledky vyšetřování jejich příčin ukázaly vážné nedostatky bezpečnosti v celém systému, které si žádaly široké změny a nápravy. Náklady, které by byly potřebné k vykonání nutných modifikací a úprav se ukázaly tak vysoké, že bylo rozhodnuto celý tento zbrojní program odložit a urychlit nasazení raketovému systému Minuteman. Tak se stalo, že velký raketový zbrojní systém, původně navrhovaný na dobu použití nejméně 10 let, byl používán méně než 2 roky pro nedostatky jeho bezpečnosti [58].

Vyšetřování prvních havárií kosmických zařízení jasně ukázalo, že příčiny velkého počtu z nich vyplývají z nedostatků návrhu, provozu a managementu. Tehdejší přístup k bezpečnosti založený na postupnosti „let-náprava-let“ byl očividně nevyhovující. Podle tohoto přístupu bylo vyšetřování havárie zaměřeno na rekonstrukci příčin, přijetí opatření, anebo minimalizování opětovného vzniku havárie ze zjištěných příčin a případné standardizování přijatých opatření. Ačkoliv byl tento přístup efektivní pro redukování havárií z odhalených příčin, Ministerstvo obrany USA a později i ostatní pochopili, že je velmi drahý a v případě například jaderných zbraní neakceptovatelný. Toto poznání vedlo k osvojení přístupů systémové bezpečnosti pro účinné zabránění vzniku havárií ještě před tím, než se vyskytne poprvé.

První specifikování systémové bezpečnosti pro armádu publikovalo vojenské letectvo USA v r.1962 a raketová střela Minuteman ICBM byla prvním zbrojním systémem, která měla smluvně, formálně a odborně zajištěný program systémové bezpečnosti. V USA byly tak velké obavy z nepozorného odpálení rakety, že Ministerstvo obrany USA exportovalo vyvinuté techniky systémové bezpečnosti do bývalého SSSR a doporučilo jejich použití [10].

První standard specifikující systémovou bezpečnost byl vypracován Vojenským letectvem USA v r.1966 pod označením MIL-S-381 30A. V červnu 1969 se stal standardem systémové bezpečnosti pod označením MIL-STD-882C. Tato norma stanoví, že zhotovitel si musí stanovit a udržovat efektivní program systémové bezpečnosti naplánovaný a integrovaný ze všech fází vývoje zařízení, výroby, provozu a případné likvidace. Program systémové bezpečnosti bude zabezpečovat přesně stanovený postup metodické kontroly bezpečnostních aspektů a hodnotit projekt zařízení ve smyslu identifikování nebezpečí a předepsání časově i nákladně efektivních nápravných zásahů. Cíle programu systémové bezpečnosti mají zajistit následující:

- bezpečnost zařízení odpovídající jeho poslání a zabudování v něm,
- identifikaci, vyhodnocení, eliminaci anebo kontrolu na akceptovatelné úrovni nebezpečí přidružených k systému, podsystému a jednotlivým částem,
- kontrola nad nebezpečími, která nemohou být eliminována je zajištěná tak, aby chránila personál, zařízení a majetek,
- použití nových materiálů, anebo výrobků a testovacích technik musí být spojené jenom s minimálním rizikem,
- nápravná opatření požadovaná pro zlepšení bezpečnosti jsou minimalizována

dočasným včleněním bezpečnostních faktorů během vzniku systému,

- historické údaje o bezpečnosti generované podobnými programy bezpečnosti jsou brány v úvahu a používány všude, kde je to vhodné.

Na tomto vojenském standardu systémové bezpečnosti jsou postaveny mnohé následné požadavky a programy mnoha agentur a průmyslných odvětví.

Vesmírný program byl druhou velkou oblastí aplikace přístupů systémové bezpečnosti. Dokud nedošlo k požáru Apolla-1 v r. 1967 na Kennedyho mysu, při kterém zahynuli tři kosmonauti, zaměřovalo se bezpečnostní úsilí jen na průmyslovou bezpečnost dělníků. Toto neštěstí bylo upozorněním pro NASA a jeho odpovědní
pracovníci zadali společnostem General Electric a Daytona Beach, aby vyvinuly politiky a procedury, které se staly modelem pro bezpečnost civilních kosmických aktivit [49].

Rozsáhlý program systémové bezpečnosti stanovený pro vesmírné projekty byl většinou postaven na programech Vojenského letectva a Ministerstva obrany USA. Mnoho stejných inženýrů a firem, které měly vypracovány formální programy systémové bezpečnosti odpovídající nárokům Ministerstva obrany USA pro dodavatele, byly zahrnuty i do vesmírných programů a jejich technologie a management byly přeneseny do nové aplikace.

Když se počítače staly komponentami s neustále rostoucím významem ve složitých systémech, vynořila se i obava o bezpečnostní aspekty softwaru v programech NASA a Ministerstva obrany USA. První aktivity okolo bezpečnosti softwaru byly provedeny v programu Space Ahuttle v 70. letech minulého století. Jmenovitě byla vyvinuta analýza bezpečnosti pro kritické funkce softwaru řídícího start a přistání raketoplánu. Ministerstvo obrany USA spolu s vojenským letectvem začalo s integrací softwaru do programů systémové bezpečnosti začátkem 80. let minulého století. Rozsáhlý soubor úloh pro bezpečnostní analýzy softwaru byl zapracován do standardu MIL-STD-882B v červenci 1987.

Komerční průmyslová odvětví si buď adaptovala programy systémové bezpečnosti z vojenství či 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 komponent) 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, která nejsou vidět, pokud se na tyto části díváme jako na oddělené. V mnohých průmyslových odvětvích se potvrdilo, že zabudování bezpečnosti do zařízení nebo výrobků může zredukovat celkové náklady na jejich životní cyklus, a že dosažení akceptovatelné úrovně bezpečnosti vyžaduje přístupy systémové bezpečnosti.

Základní ideje

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

Prvotním zájmem systémové bezpečnosti je management rizik: jeho identifikace, vyhodnocení, eliminace anebo kontrola pomocí analýzy designu, anebo manažérských procedur. Muelle [39] nazval novou disciplínu „inženýrství systémové bezpečnosti“ v r. 1968 jako „organizované veřejné mínění“. Měl na mysli plánovaný, osvojený a systematický přístup k identifikování, analyzování a kontrolování nebezpečí během celého životního cyklu systému za účelem redukce havárií.

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

I navzdory tomu, že je systémová bezpečnost 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 bezpečnosti a managementu rizika. Především systémová bezpečnost:

- zdůrazňuje budování bezpečnosti a ne její přidávání do vytvářeného systému,
- se zaobírá systémem jako celkem a ne pouze podsystémy a komponentami
- pojímá nebezpečí poněkud šíře než jen jako chyby,
- klade větší důraz na analýzu, než na později 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.

Analýzy rizik

Analýzy rizik zjišťují faktory související s haváriemi. Používají se (1) při vývoji a to k identifikaci a odhadu potenciálních nebezpečí a podmínek, které k nim mohou vést tak, aby mohly být eliminovány, anebo kontrolovány hned v zárodku konceptu systému, (2) během provozu a při zkoušení už existujícího systému za účelem zlepšení jeho bezpečnosti a (3) při udělování licence na zjištění a prokázání akceptovatelné bezpečnosti plánovaných, anebo existujících systémů pro dozorové orgány. Typ analýzy rizik závisí na účelu, pro který má být vykonána – ať už pro zvýšení bezpečnosti, přesvědčení dozoru o akceptovatelné bezpečnosti apod. Analýzy systémové bezpečnosti, tak jako jsou originálně definovány v armádních projektech, pro které byly vyvinuty, jsou rozdělené do 4 stádií podle toho, kdy jsou vykonávány a na jaké cíle jsou zaměřeny.

Předběžná analýza nebezpečí (Preliminary Hazard Analysis – PHA) se vykonává v prvních stádiích životního cyklu systému pro identifikaci kritických funkcí systému a celkových nebezpečí tak, že bezpečnostní úvahy jsou obsaženy v porovnávacích studiích a alternativách projektu. Proces vypracování PHA je interaktivní. PHA se kompletuje s přibývajícími poznatky o konstrukci a změnách, které byly během projektování provedeny. Protože PHA začíná hned ve stádiu formování koncepce systému, kdy jsou známy jen minimální detaily, jsou odhady nebezpečí a úrovně rizik obsažené v této analýze nevyhnutelně jen kvalitativně a rozsahově omezené.

Analýza systémového nebezpečí (Systems Hazard Analysis – SHA) začíná před ukončením návrhu jako jeho předběžná prověrka a pokračuje průběžně s doplněním návrhu a realizací změn. Zahrnuje detailní studie možných nebezpečí na rozhraní mezi pod-

systémy, anebo při provozu celého zařízení, včetně potenciálních selhání člověka. SHA je specificky zaměřená na zkoumání rozhraní z hlediska (1) souladu s požadovanými bezpečnostními kritérii, (2) degradace bezpečnosti vyplývající z normálního provozu zařízení a (3) možných kombinací nezávislých, závislých a simultánních nebezpečných událostí, anebo chyb, včetně poruch, bezpečnostních zařízení. Účelem SHA je doporučení změn, navrhnutí zařízení pro kontrolu zajištění bezpečnosti a vyhodnocení splnění požadavků na bezpečnost systému.

Analýza nebezpečí podsystémů (Subsystem Hazard Analysis – SSHA) začíná prakticky zároveň s navrhováním detailů podsystémů a završuje se při ukončování návrhů jejich konečného řešení. Podobně jako při analýze systémového nebezpečí jsou při analýzách nebezpečí podsystémů vyhodnocovány požadované projektové změny z hlediska všech uvažovaných provozních modů každého podsystému, jejich kritických vstupů a výstupů a funkčních vazeb mezi vnitřními komponentami a přístrojovou nadstavbou. Zjišťují se při ní i nevyhnutelná opatření pro určení, jak eliminovat, anebo redukovat rizika z identifikovaných nebezpečí a vyhodnocuje se, jak navrhované řešení každého podsystému splní specifikované určení.

SHA a SSHA jsou vypracovávány podobnými způsoby, liší se jen svými cíli. SSHA zjišťuje, jak provoz anebo selhání jednotlivých komponent ovlivní celou bezpečnost systému a SHA určuje, jak standardní a poruchové stavy komponent při jeho společném provozu mohou ovlivnit systémovou bezpečnost.

Analýza nebezpečí provozu a její podpory (Operating and Support Hazard Analysis – OSHA) identifikuje nebezpečí a procedury redukce rizik během všech fází používání a údržby systému. Je speciálně zaměřená na zjišťování nebezpečí generovaných rozhraním člověk-stroj.

Projekt pro bezpečnost

Jakmile je už nebezpečí jednou identifikováno, musí být nejvyšší prioritou jeho eliminace, anebo jeho spolehlivá kontrola. Systémová bezpečnost obsahuje má široce akceptované priority jak zvládnout rizika [21]:

1 Eliminovat rizika (skutečná bezpečnost)
2 Redukovat rizika
3 Zvládnout rizika
4 Lokalizovat a zmírňovat škody.

Uvedené priority neznamenají, že stačí, aby byla jen jedna z nich aplikovaná při daném projektu, anebo že jen nejvyšší priorita je nejžádanější Ani skutečně bezpečný projekt (1. priorita) není schopen zabránit za každých okolností, či už normálních, anebo abnormálních, každému impulzu schopnému způsobit havárii, anebo zabránit vytvoření zdraví škodlivých účinků. Pokud tedy není možné kompletně eliminovat riziko je dalším nejlepším výběrem ochrana před nimi, anebo minimalizovat jeho vzniku tak, že se příslušné bezpečnostní ochranná opatření přímo zabudují do projektu jak ochrany, tak i do limitních podmínek provozu projektovaného zařízení.

Dalšími v akceptovatelném pořádku priorit jsou zařízení na zvládnutí nebezpečí a zmírnění jejich účinků (bezpečnostní systémy). Jsou to např. pojistné ventily, které chrání před nedovoleným přetlakem v případech, kdy 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). Pro uvedení do činnosti nepotřebují žádný přidaný impuls. Příkladem pasivního bezpečnostního systému je železniční návěstidlo, 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 za účelem zabránění havárie anebo zmírnění jejích následků 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.

Projekt pro bezpečnost musí být vždy vybaven pro minimalizování škod v případech, že bezpečnostní opatření a systémy selžou, anebo se vyskytne neidentifikované nebezpečí. Minimalizování škod může mít podobu (1) varovné a výstražné signalizace, výcviku, pokynů a procedur pro chování v nebezpečných situacích, anebo (2) izolace nebezpečných zařízení od osídlených center. Opatření před nehodami včetně havarijního plánování musí být vypracováno ještě před tím, než bude zařízení spuštěno do provozu. Při vzniku havárie by už na to nemuselo být dostatek času. Systémová bezpečnost má též priority pro výběr specifického dohledu nad bezpečností:

(1) odstranit nebezpečí, (2) použít ochranné systémy pro likvidaci jeho výskytu,
(3) poskytnout výstražné zařízení k upozornění operátorů a ostatního personálu a
(4) poskytovat výcvik.

Management bezpečnosti

Nejdůležitějším aspektem systémové bezpečnosti v termínech prevence havárií jsou procedury managementu bezpečnosti. Účinný management bezpečnosti spočívá ve stanovení politiky a v definování cílů bezpečnosti, tj. v plánování úloh a procedur; v definování zodpovědnosti a určení kompetencí; v dokumentování a průběžném sledování nebezpečí včetně kontrol; v udržování bezpečnostního informačního systému včetně zpětné vazby a forem hlášení poruch/havárií apod.

Systémová bezpečnost je zodpovědná za zajištění bezpečnosti systému jako celku včetně analýzy interface mezi komponentami. Aktivity na úrovni bezpečnosti komponentů, jako např. bezpečnosti raketové odpalovací rampy, mohou být součástí všeobecné odpovědnosti za systémovou bezpečnost, anebo mohou být částí inženýringu komponent při velkých a komplexních projektech. Pro vymezené druhy nebezpečí, jakými mohou být požáry, provoz jaderných zařízení anebo výbušné prostředí, může být požadováno další členění zodpovědnosti za bezpečnost. Při jakémkoli stupňovitém rozčlenění úsilí o systémovou bezpečnost mají hlavní zodpovědnost za integraci jednotlivých bezpečnostních aktivit a informací inženýři systémové bezpečnosti. Systémová bezpečnost je obyčejně provázaná s odpovídajícími inženýrskými, anebo vědeckými disciplínami, jako např. inženýrství spolehlivosti, zajištění kvality, lidský faktor apod.

Jaké procesy a úlohy systémové bezpečnosti budou prováděny v konkrétním projektu, bude záviset na jeho velikosti a úrovni rizika projektovaného systému.

3.7 Cena a efektivita systémové bezpečnosti

Z praktických důvodů musí být přístupy systémové bezpečnosti efektivně a cenově dostupné. Např. vojenské letectvo implementovalo několik dobře vypracovaných bezpečnostních programů a poukázalo na to, že pro tyto programy nejsou velké investice nutné.

Havárie vojenských letadel USA (asi 200 událostí ročně), spolu s implementací bezpečnostních opatření zjištěných po jejich vyšetření, stojí více jak 1 miliardu dolarů. Typický program systémové bezpečnosti pro letectví vyjde při velkých projektech na 5 až 10 milionů dolarů [17]. Jiné běžné odhady nákladů na dobré programy systémové bezpečnosti udávají hodnotu 5 až 7 % nákladů na celý projekt. V leteckém průmyslu se náklady na program systémové bezpečnosti vrátí už při zachránění jednoho letadla. Návratnosti nákladů na program systémové bezpečnosti se dosáhne tehdy, když se zabrání haváriím. Efektivnost programu systémové bezpečnosti se prokazuje velmi těžko, protože měřit něco, co se nestalo, je těžké. Trend snížení počtu havárií vojenských letadel po zavedení důrazného programu systémové bezpečnosti byl přijat jako ukazatel zlepšení bezpečnosti a jednoznačně přiřazený úsilí vynaloženému na tento program.

Jedním z nepřímých způsobů měření efektivnosti programu systémové bezpečnosti, byť i ne celkem uspokojivý pro nedostatek porovnávaných faktorů, je porovnávání systémů, které měly program systémové bezpečnosti s těmi, které ho neměly. Dobrým příkladem pro tento způsob prokazování efektivnosti programu systémové bezpečnosti je případ vývoje vojenských stíhaček F-4 a F-14 pro námořnictvo USA. Obě dvě tato letadla měla přibližně stejné bojové poslání, přičemž stíhačka F-4 neměla formální program systémové bezpečnosti a stíhačka F-14 takovýto program měla. Kumulativně měly materiálové poruchy u F-4 četnost 9,52/100 000 hod., u F-14 byla tato četnost 5,77/100 000 hod. Tento rozdíl četnosti se ještě zvětšil, když začaly skupinové lety. Tyto rozdíly četnosti byly zčásti vysvětlovány některými jedinečnými vlastnostmi jednotlivých typů stíhaček, avšak porovnávací údaje jednoznačně podpořily efektivitu zavedení programu systémové bezpečnosti.

Jinou cestou zjišťování efektivnosti programu systémové bezpečnosti je vykazování nebezpečí, které bylo personálem systémové bezpečnosti korigováno ještěpředtím, než došlo k havárii, anebo bylo jinak zjištěno.

Třetí cestou odhadování efektivnosti programů systémové bezpečnosti je zkoumání případů, při kterých nebylo respektované doporučení systémové bezpečnosti a došlo k haváriím. Frola a Miller [17] uvádějí více příkladů pro tuto, stejně jako i pro předcházející cestu zjišťování efektivnosti programů systémové bezpečnosti. Většina z nich jsou z leteckého průmyslu a hovoří o případech, kdy z úsporných důvodů přijaté řešení nevyhovovalo nárokům systémové bezpečnosti a muselo být změněno po haváriích, které byly způsobeny tímto přijatým opatřením.

3.8 Inženýrství spolehlivosti

Rozdíl mezi inženýrstvím spolehlivosti a systémovou bezpečností není dodnes jasně vymezen. Pro jeho zvýraznění uvidíme v této části studie charakteristické znaky tohoto rozdílu a specifické návrhy inženýrství spolehlivosti.

Inženýrství spolehlivosti se přednostně zabývá chybami a redukováním četnosti jejich výskytu [22]. Spolehlivost je definován jako charakteristika daného objektu vyjádřená pomocí pravděpodobnosti, že tento bude vykonávat specifikovaným způsobem funkce, které jsou na něm požadovány během stanoveného časového intervalu a za stanovených resp. předpokládaných podmínek. Nejprudší rozmach inženýrství spolehlivosti byl v prvních letech po 2. světové válce v energetice nebo elektrotechnickém průmyslu. Významnou úlohu sehrálo i v projektech NASA.

Reprezentativními technikami inženýrství spolehlivosti pro minimalizaci chyb komponentů (součástek) a tím i chyb komplexních systémů, které byly zapříčiněny chybami komponentů jsou:

- paralelní redundance
- zálohování zařízení
- koeficient a rezerva bezpečnosti
- snižování počtu přetížení
- limitování doby použití.

Tyto techniky jsou prokazatelně efektivní pro zvýšení spolehlivosti, ale bezpečnost nevyhnutelně nezvyšují, ba dokonce za jistých okolností ji mohou redukovat. Analýzy nebezpečí při systémové bezpečnosti se dívají na interakce a nezaměřují se jen na chyby anebo nejistoty inženýrského řešení.

Inženýři spolehlivosti často považují spolehlivost a bezpečnost za synonyma. To je pravda jen v některých speciálních případech. Všeobecně má bezpečnost o něco širší význam jako chyba a chyby ještě nemusí snižovat bezpečnost. Běžně mají spolehlivost a bezpečnost mnoho společných vlastností. Mnohé havárie však nastanou bez toho, že by selhala nějaká komponenta. Právě naopak, častokrát všechny komponenty při nich fungovaly podle očekávání a bezchybně. Taktéž se může stát, že komponenty mohou selhat (mít poruchu) bez toho, aby došlo k havárii.

Havárie mohou být zapříčiněny provozem zařízení mimo povolené rozsahy hodnot parametrů a časových limitů, ze kterých vycházely analýzy spolehlivosti. To nám říká, že systém může mít vysokou spolehlivost a přece může havarovat. Navíc, generalizované pravděpodobnosti a analýzy spolehlivosti se nemohou přímo aplikovat na specifické, anebo lokální podmínky. Např. pravděpodobnost, že srážka letadla s ptákem způsobí havárii je o něco vyšší na ostrově Midway, než kdekoliv jinde. Nejdůležitější je, že havárie mnohokrát nejsou výsledkem jednoduchých kombinací chyb/selhání komponentů.

Bezpečnost je emergentní 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 řídícího systému, zásahů člověka a konstrukčních chyb. Analýzy spolehlivosti se zaobírají jen pravděpodobnostmi havárií souvisejících s chybami; nevyšetřují potenciální škody, které může způsobit správná činnost (provoz) jednotlivých komponentů.

Není možné, aby inženýrství spolehlivosti nahradilo systémovou bezpečnost, může ji ale doplnit. Musí to však být provedeno s jasným vědomím, že konečným cílem je zvýšení odolnosti systému vůči nebezpečím náhodných chyb. Je to vždy lepší, když se zařízení/systém navrhuje tak, že individuálně náhodné chyby nemohou způsobit havárii i kdyby se vyskytly, ačkoliv to není vždy možné.

Velmi opatrní musíme být při aplikování technik odhadování spolehlivosti pro posuzování bezpečnosti. Pro potenciální havárie, které nemohou být zapříčiněny událostmi, které lze vyjádřit pravděpodobnostmi, lze všeobecně používat míry pravděpodobnosti rizika. Odhady pravděpodobnosti měří pravděpodobnost náhodných chyb a ne pravděpodobnost nebezpečí anebo havárií. Když se při analýzách systémové bezpečnosti najde projektová chyba, bude daleko účinnější, jestliže se odstraní, než když budeme někoho přesvědčovat pomocí vypočítaných pravděpodobností, že tato chyba nikdy nezpůsobí havárii. Vysoké hodnoty pravděpodobnosti nezaručují bezpečnost a bezpečnost nevyžaduje naprostou spolehlivost.

Hlavním nedostatkem pravděpodobnostních modelů nejčastěji není to, co zahrnují, ale to co nezahrnují. Veselý a kol. [69] uvádějí názorný příklad ohraničení a rozšíření problému při spolehlivém modelování. Příklad zní: „Uvažujme ohraničený systém, uvnitř kterého se mohou vyskytnout poruchové události s četností řádově 10^{-3} a výše. Rozšiřme teď jeho hranice tak, že do nového systému zahrneme i události, u kterých četnost výskytu byla řekněme řádově 10^{-4}, anebo vyšší. Pokud bychom pro náš původní systém navrhli dvojnásobnou redundanci, mohli bychom zredukovat četnost výskytu událostí v něm na hodnotu 10^{-6}. Dominantními událostmi v novém systému se však stanou události s četností 10^{-4}, zatím co návrháři systému budou v zajetí iluze, že systém bude o dva řády bezpečnější, resp. spolehlivější, než ve skutečnosti je. Pokud se v podobných případech, jaký uvádí uvedený příklad neuvažuje správně, může se lehko dospět i k takovým absurdním hodnotám četnosti událostí jako 10^{-16} anebo 10^{-18}. Tyto nízké hodnoty jednoduše hovoří o tom, že systém neselže uvažovaným způsobem. Ovšem ve skutečnosti selže s daleko vyšší pravděpodobností a způsobem, který jsme neuvažovali“.

Jeden ze zakladatelů systémové bezpečnosti, C. O. Miller [48] upozorňuje, že odlišování nebezpečí od chyb je podstatné pro to, abychom porozuměli rozdílu mezi bezpečností a spolehlivostí.

4 LIDSKÉ CHYBY A LIDSKÁ SPOLEHLIVOST

Velká část nehod a havárií byla způsobena chybou lidí, ať již bezprostředněpřímým selháním člověka, anebo v důsledku působení nějakého latentního faktoru, jehož příčiny lze opět spatřovat v jednání lidí. Dokonce se tvrdí, že za veškeré nehody jsou odpovědni lidé, kteří systém navrhli, vyrobili, implementovali a provozují jej. K tak vyloženě technické závadě, jako bylo například prasknutí těsnicího „O“-kroužku v plášti kosmické lodi Challenger, došlo v důsledku celého řetězce příčin, jejichž zrod lze vystopovat až do jednání lidí, kteří byli odpovědni za bezpečnost tohoto systému. Konec konců, všechny předchozí kapitoly poučují, že za systémovým selháním vždy stojí člověk. Není divu, že problematika lidské spolehlivosti a role člověka v technických, technologických, sociotechnických i společenských systémech se stala předmětem mnoha analýz a analytických systémů.

4.1 Vznik ergonomie

Zájem o lidské chyby je poměrně nového data. Za 2. světové války začali konstruktéři letadel uvažovat, proč řízení letounu dělá potíže nezkušeným nováčkům. V jednu chvíli války bylo na straně spojenců ztraceno dokonce více letadel v důsledku chyb pilotů, než bojových akcí nepřítele. Díky rozvíjející se systémové teorii nehledali odborníci příčinu pouze v lidech, ale zaměřili se na to, jak lze složitý stroj konstruovat tak, aby se to nováčci naučili co nejrychleji a nejefektivněji. Analýzou činnosti pilotů dospěli k tomu, že musí změnit ovládací a sdělovací systém tak, aby vyhovoval lidské přirozenosti. Tak vlastně položili základy oboru, který byl později nazván „Human Factors“ (v USA) anebo „ergonomie“ (v Anglii).

Rozvoj tohoto oboru nabral po válce rychlé tempo. Byly vytvořeny první učebnice (například Chapanis [97], Murell [92]), sestaveny pokyny pro uplatňování ergonomických principů při konstrukci složitých sdělovacích a ovládacích systémů, vypracovány tabulky

srovnávající možnosti strojů ve srovnání s člověkem apod. V r. 1957 byla ustavena Human Factors Society of America (v r. 1992 byl název změněn na Human Factors and Ergonomics Society), která se sehrála vůdčí roli v dalším rozvoji ergonomie a podnítila vznik Mezinárodní ergonomické asociace v r. 1961.

Základem ergonomie je systémový pohled na činnost člověka, jehož kapacita pro dané úkoly je omezená jeho přirozenými vlastnostmi, mezi něž patří vnímání, pozornost, paměť, úsudek, řešení problémů a rozhodování, z fyzických vlastností pak síla, rychlost, pohyblivost, vytrvalost, odolnost vůči působení fyzikálních, chemických či biologických činitelů. Z hlediska bezpečnosti práce jsou psychologické kvality lidí důležitější než vlastnosti tělesné, proto se ergonomie v tomto pojetí značně uplatňuje při řešení problematiky lidské spolehlivosti.

V šedesátých letech 20. století došlo k rozvoji ergonomie především v oblasti interface systému člověk-stroj se zvláštním důrazem na design vstupních informačních zdrojů a výstupních ovládacích zařízení. Tato fáze byla později nazvána s jemnou ironií jako ergonomie „knoflíků a ciferníků“ (knobs and dials). Model lidského chování je poznamenán v té době převládajícím behaviorismem, který se soustřeďuje výlučně na vstupy a výstupy do a ze systému a vlastní psychickou oblast pokládá za černou skříňku, která není přístupna pozorování objektivními vědeckými metodami. Zájem se soustředil na formální aspekty procesu příjmu a zpracovávání informací, kde člověk je chápán jako kanál pro přenos informací. Studovány byly otázky jako je kapacita tohoto kanálu v čase, například kolik informací je člověk schopen přijmout a zpracovat za jednotku času, na jakých podmínkách úspěšnost přenosu závisí apod. Mentální zátěž byla chápána výlučně jako množství informací, kterou člověk zpracovává v daném čase. Byla studována schopnost lidí zvládat extrémně vysoké úrovně informací v různých situacích, například při řízení letového provozu. Koncept člověka jako kanálu zpracovávání informací byl užitečný při zdůrazňování potřeby konstruovat systémy, které respektují lidské kapacity a omezení. Nerespektovány ovšem byly takové problémy jako je význam těchto informací, záměry, které lidé sledují a psychické procesy jako řešení problémů, rozhodování a diagnóza. Navzdory těmto omezením se stal tradiční ergonomický přístup zdrojem mnoha praktických aplikací a technik.

Dalšími otázkami, určovanými praktickými úkoly člověka, byl výzkum vigilančních procesů, které jsou spojeny s monitorováním nezřetelných a řídce se vyskytujících signálů jako je například sledování radarových obrazovek. Tento problém byl traktován rovněž v teorii detekce signálů, věnované lidské kapacitě správně či chybně rozpoznávat málo zřetelné podněty či útvary.

Ergonomický přístup zdůrazňuje špatný poměr mezi lidskou kapacitou a nároky systému jako hlavního zdroje lidských chyb. Z tohoto hlediska se zásadním zlepšením jeví nutnost zajištění toho, aby design systému bral do úvahy fyzické a mentální charakteristiky člověka. To zahrnuje následující úkoly:

- Design pracoviště a práce přizpůsobovat požadavkům pracovníků s rozdílnými fyzickými a mentálními charakteristikami
- Design interface člověk-stroj, se zaměřením zejména na kontrolní panely, navrhovat tak, aby byla informace o procesu dobře přístupná a interpretována, a aby mohly být plynule činěny příslušné ovládací akce
- Design fyzického prostředí navrhovat tak, aby byly minimalizovány negativní tělesné a psychologické účinky nepříznivých podmínek
- Optimalizovat mentální a tělesnou zátěž pracovníka.

Tento přístup je popisován jako „přizpůsobení práce člověku“. Ergonomický přístup lze aplikovat jak na bezpečnost práce a procesu, tak na problematiku pracovního stresu z hlediska jeho prevence a zlepšování pracovních podmínek.

Tradiční ergonomický přístup poskytuje techniku a data k optimalizaci lidského výkonu a minimalizaci chyb určité kategorie. Hlavní pole aplikace ergonomie je při designu nových systémů. Nicméně jsou k dispozici i kontrolní listiny pro hodnocení ergonomických nedostatků, které mohou být podkladem pro odhalování a nápravu chyb v existujících systémech.

Toto zúžené nazírání na lidskou psychiku sice vedlo ke stanovení mnoha užitečných principů pro konstrukci sdělovacích a ovládacích systémů, jejichž nedostatky přispívají k méně spolehlivým výkonům lidí, avšak bylo zcela nedostatečnou základnou pro analýzu lidských chyb a pro pochopení jejich podstaty. Navíc ještě, tento tradiční ergonomický rámec neposkytuje systematickou oporu pro zacházení a eliminaci kognitivních chyb v oblastech jako je diagnóza a řešení problémů.

Nicméně se do povědomí projektantů a inženýrů dostalo mnoho důkazů, že při analýze nehod se nemohou zastavit pouze při konstatování, že jejich příčinou byla lidská chyba, nýbrž že musí uvažovat o tom, proč a čím byla tato chyba podmíněna.

4.2 Kognitivní přístup

Poznatky a teorie kognitivní psychologie, aplikované při analýze lidské spolehlivosti se vyvinuly v průběhu 70. a 80. let 20. století změnou náhledu na člověka. Člověk již nebyl považován jako pasivní černá skříňka, ale nové poznatky umožnily popisovat úmysly jednotlivců a že jejich akce jsou ovlivňovány budoucími cíli a plány. Tento přístup je aplikovatelný zejména na činnosti jako je plánování a jednání při mimořádných situacích. Metody zahrnují analýzu kognitivních úkolů, která se zaměřuje na chyby při zpracovávání informací a na používání podpory rozhodování pro jednání v mimořádných situacích. Tento přístup je nejúplnější z hlediska hodnocení příčin chyb, které jsou v pozadí jevové stránky. To znamená, že je obzvláštně relevantní pro analýzu opakujících se chyb a pro predikci specifických chyb, které mohou mít závažné důsledky, což je součást analýzy bezpečnosti.

Kognitivní ergonomie se nadále zabývá zpracováváním informací nicméně od dosavadního přístupu se liší v tom, že dále zkoumá, jak lidé tyto informace vnitřně reprezentují a používají k řízení chování. Klíčovým rozdílem od klasického ergonomického přístupu je, že kognitivní přístup zdůrazňuje roli záměrů, cílů a významu jako centrálního aspektu lidského chování.

Namísto koncepce člověka jako pasivního elementu systému, kognitivní přístup zdůrazňuje skutečnost, že informace jsou vždy nositeli nějakého významu, a že akce lidí jsou téměř vždy nasměrovány k určitému explicitnímu či implicitnímu cíli. Kognitivní přístup tak otevírá onu pomyslnou černou skříňku.

Klasifikace chyb z kognitivní perspektivy

Účinný systém klasifikace chyb je důležitý z několika hledisek. Chceme-li soustředit údaje o lidských chybách v průmyslových situacích pro odhalení náročných trendů, identifikaci opakujících se typů chyb anebo pro vývin kvantitativní báze četnosti chyb, potřebujeme bázi pro seskupování chyb podobného typu. V ranné fázi ergonomie nebyla rozvinuta teorie chyb, která by spojila vnější formu chyby se základními mentálními procesy, které jim dávají

vzniknout. Pokud není toto spojení provedeno, není možné klasifikovat chyby systematicky, neboť stejný způsob externí chyby může být zaviněn řadou zcela rozličných základních příčin. Reason [78] uvádí následující příklad: pro chybu pracovníka, který místo ventilu A zavře blízký ventil B existuje přinejmenším pět možných vysvětlení:

1) Ventily jsou blízko sebe a špatně označeny. Pracovník nebyl seznámen s ovládáním ventilů a proto zvolil ten nesprávný. Možná příčina: špatná identifikace spolu s nedostatkem obeznámenosti, jež vedla k chybnému úmyslu (jakmile došlo ke špatné identifikaci, pracovník zamýšlel uzavřít nesprávný ventil).

2) Pracovník mohl přeslechnout pokyny dané jeho nadřízeným a myslet, že správný ventil je B. Možná příčina: selhání komunikace, která dává vzniknout nesprávnému úmyslu.

3) Vzhledem k blízkosti obou ventilů, i když pracovník zamýšlel uzavřít ventil A, nesprávně operoval s ventilem B (správný úmysl, ale špatné provedení).

4) Pracovník uzavíral ventil B velmi často jako součást své každodenní práce. Operování s ventilem A bylo zasuto v dlouhé řadě sekvencí jiných operací, podobných s těmi, jež jsou normálně asociovány s ventilem B. Pracovník věděl, že má uzavřít A, byl však vyrušen kolegou a vrátil se zpět ke svému silnému zvyku uzavřít B. Možná příčina: vliv silného zvyku v důsledku externího vyrušení (správný úmysl, ale špatné provedení).

5) Pracovník věděl, že má zavřít A. Nicméně pracovníci věřili, že navzdory operačním pokynům má zavření B stejný účinek jako zavření A, a že to způsobí méně poruch pro výrobu. Možná příčina: porušení jako výsledek nesprávně pochopené instrukce a neformální podniková kultura soustředit se spíše na výrobu než na bezpečné cíle (špatný záměr).

Tato vysvětlení nevyčerpávají možnosti vzhledem k základním příčinám, avšak ilustrují důležitý bod, a to, že analýza lidských chyb jako vnějších forem nedostačuje. Mají-li být základní příčiny chyb objasněny a vyvinuty příslušné strategie pro zacházení s nimi, je zapotřebí důkladnějšího přístupu. Je zapotřebí klasifikovat chyby na základěpodstatných příčin, které specifikují typy chyb, které je možno predikovat jako funkci specifických podmínek.

Jednoduchou klasifikaci lidských chyb uvádějí Swain a Guttmann [77], kteří odlišují chyby „vynechání“ (omission) od chyb „provedení“ (commission). První druh znamená, že člověk vynechal či neprovedl nějaký krok, který provést měl, například zapomněl, neuvědomil si, nerozpoznal signál apod. Druhou skupinu charakterizují akce provedené nesprávně, ať již ve špatném pořadí, příliš brzy nebo příliš pozdě, v příliš malém rozsahu nebo ve špatném směru. K tomuto třídění přidávají oba autoři ještě další chybu, kdy člověk provede něco, co není požadováno. Toto jednoduché třídění je založeno na vnějších znacích, avšak nepostihuje psychologické příčiny chyb.

Reason [78] definuje lidskou chybu jako obecně použitelný výraz, který zahrnuje všechny události, kde plánovaný sled mentálních nebo fyzických činností nedosahuje zamýšleného výsledku a jestliže tato selhání nemohou být připsána na vrub intervenci nějakého náhodného působení. Z toho vyplývá, že 1) chyba je založena na nedosažení výsledku či cíle. Systém neudělal to, co se předpokládalo. 2) slova „plánovaný a zamýšlený“ znamenají, že úmysl je ústřední v celé perspektivě teoretických úvah. Úmysl sestává ze dvou elementů: a) konečný stav, kterého má být dosaženo (cíl), b) prostředky (činnost), kterými má být cíl dosažen. Rozlišujeme typy chyb označované jako slip, lapse, mistake a vědomé, tj. záměrné porušení pravidel.

Slip je chybné provedení nějaké akce a chyba se stane, jestliže člověk se snaží provádět správnou akci, ale udělá ji nesprávně. Například tehdy, když lékař či sestra dá do infuse nesprávnou dávku, ačkoli zná správnou, anebo ze sportu například špatné trefení míče ve fotbalu, kdy obránce ve snaze odvrátit centrovaný míč vsítí vlastní gól, anebo přihraje míč přímo na nohu soupeři. Česky bychom mohli označit tento druh chyb prostřednictvím termínu vypůjčeného ze sportovního žargonu jako „kiks“ nebo „minela“. Chyby se vztahují na pozorovatelnou činnost a jsou obvykle spojeny s chybami pozornosti či percepce. Údržbářova pozornost může být narušena a ten pak odmontuje jinou hydraulickou hadici, než měl. Věděl, čeho chce docílit, nicméně provedl jednoduchou chybu. Vzhledem k tomu, že to věděl, je zbytečný další výcvik. Nejúčinnější strategie zábrany tohoto typu chyb spočívá v aplikaci nějaké formy designu. Zámky nebo fittingy, které se hodí pouze na dané zařízení, jsou v tomto případě nejlepším způsobem prevence.

Lapse jsou vnitřní události, obvykle jsou to výpadky paměti. Jde o vynechání nějaké činnosti, česky je lze označit jako opomenutí. Například chirurg zapomene nějaký nástroj v otevřeném těle a zašije pacienta. Prevence pak spočívá v používání prostředků pro podporu paměti, například tím, že se před šitím použité nástroje spočítají.

Mistake je chyba, která se stane, když člověk podniká nesprávnou akci. Česky je možno označit je jako omyl. Akce může být udělána perfektně, ale není to akce, která měla být provedena. Například lékař předepíše lék, na který je pacient alergický. Omyly se odehrávají na vyšší úrovni než je percepce - jde o mentální procesy obsažené při vyhodnocení dostupných informací, plánování, formulace úmyslu a posouzení pravděpodobných důsledků plánovaných akcí. Zapomene-li údržbář pracovní postup, anebo ho nikdy plně nepochopil, pak může špatně rozhodnout, zejména v případě, kdy manipulace s novým zařízením či nástrojem, který je pro něj neznámý. Jde o volbu špatné akce. V tomto případě je nejdůležitější prevencí výcvik.

Vědomé porušení je akce, učiněná záměrně, která však není správná. Lidé zamýšlejí pouze porušit pravidlo, ale ne trpět možnými důsledky. Pracovníci občas jednají zkratkovitě, protože chtějí zvýšit svou produktivitu anebo dokončit úkol. Poruchy pravidel bývají managementem tolerovány, ba občas i vyžadovány. Tento druh chyb je nejobtížněji potlačitelný. Jsou to záměrná porušení bezpečnostních pravidel. Existuje celá řada faktorů, které ovlivňují pravděpodobnost porušování pravidel. Lze je dělit na: 1) faktory, jež přímo motivují pracovníka k porušení pravidel (nazvané přímé motivy) a 2) doplňkové faktory, které zvyšují (popř. snižují) pravděpodobnost, že jedinec spáchá porušení (nazývané behaviorální modifikátory). Například vyhnutí se těžké fyzické práci může být přímým motivem k zanedbání povinnosti, nicméně nedostatek účinného dozoru je behaviorálním modifikátorem, který zvyšuje pravděpodobnost zanedbání, neboť je nízká šance, že může být odhalen. Prevence vědomých porušení bezpečnostních pravidel spočívá jednak v provádění důsledné kontroly, jednak v motivování k dodržování správných postupů.

Tento systém klasifikace činnosti je založen na principu, kolik kognitivního úsilí nebo zdrojů využíváme k provedení úkolu.

Model SRK (Skill, Rules, Knowledge) je klasifikace činnosti a chyb na bázi dovedností, pravidel a znalostí, kterou vytvořil J. Rasmussen [79]. Tato klasifikace typů chyb při zpracovávání informací ovlivnila řadu přístupů a metodických nástrojů k analýze chyb lidí v práci. Činnost člověka lze roztřídit do tří kategorií:

Činnosti založené na dovednosti (Skill-based): člověk provádí rutinní, vysoce nacvičené úkoly, které lze charakterizovat jako automatizované. Vyjma příležitostné kontroly je takové chování spojeno s malým vědomým úsilím.

Činnosti založené na pravidle (Rule-based): znamená řešení situace, která nastává tehdy, jestliže se situace trochu změní a modifikuje naše předprogramované chování a nastalá situace je nám známa anebo jsme v ní vycvičeni. Úspěch je založen na používání pravidel, protože aplikujeme známé principy.

Činnosti založené na znalostech (Knowledge-based): tento druh činnosti se odehrává v nových situacích, kdy nemáme žádná aplikovatelná pravidla. Může mít formu řešení problému, přičemž se používá analytického myšlení a uchovaných znalostí.

Jak zdůvodnil Reason [78], „kiksy" a opomenutí se vztahují hlavně k úkolům založeným na dovednostech, v nichž není mnoho kognitivního úsilí. Malé rozdíly v situaci mohou být nepovšimnuty (selhání pozornosti). Na jeden krok v postupu je tedy možné si nevzpomenout. Omyly se objevují zejména při úkolech založených na používaných pravidlech a na znalostech, například neexistuje pravidlo pro danou situaci, anebo není nalezeno správné řešení problému.

Uvedené třídění umožňuje analýzu systémů z hlediska kognitivních procesů. Nabízí vodítka o kognitivní charakteristice, schopnostech a omezeních lidí, což má implikace nejen k tomu, jaký druh chyb může být činěn, ale i určité podněty k tomu, jak konstruovat systémy tak, aby bylo zabráněno vzniku chyb. Jak však uvidíme dále, tato taxonomie doznala počátkem 90. let podstatných změn, které odstraňují některé teoretické nedostatky a zavádějí nové koncepty do úvah o lidských chybách, které realističtěji reflektují lidskou činnost zejména v oblasti těchto činností založených na znalostech.

Na základě předchozích klasifikací vytvořil Reason [78] model GEMS (Generic Error Modelling System), který se týká kognitivních chyb. Klasifikace je založena na formách chyb při zpracovávání informací, jako je omezení zdrojů (např. přetížení, ztráta informací) a přidává k nim dvě další tendence k chybování: (1) nevhodné použití schémat, Schémata jsou vnitřními obrazy vnějších událostí a jevů, které používáme při zvládání velkého počtu přicházejících informací. Jedná se o rutinní činnosti, které mohou být vykonávána často automaticky, tj. bez vědomého úsilí. Mohou být chybné například v abnormální situaci, která je podobná situaci obvyklé. V takovém případě operátor nevidí rozdíl a domnívá se, že jde o obvyklou situaci. Pak nesprávně použije často používaného schématu. V tom je obsažena minimalizace úsilí (ekonomie kognitivního úsilí).(2) Dalším prvkem je heuristika (strategie) používaná v obtížných situacích, která může být chybná. Model GEMS je uveden v Tabulce 1 Přílohy A.

Mentální model a vhled do situace

Přístup modelu SRK se zdá být poněkud mechanistický v tom, že se snaží pro každý případ chyby nalézt algoritmus správného provedení, který však nemusí vždy platit. Jiným přístupem, který více respektuje roli znalostí, zejména ve složitých případech, kdy je nutnost zpracovávat velké množství informací, je teorie mentálních modelů a model vhledu do situace.

Jedním z důrazných kroků k začlenění vyšších kognitivních funkcí do posuzování lidské spolehlivosti bylo vytvoření konceptu vhledu do situace, založeném na teorii mentálního modelu. Endsley [80] prezentuje teoretický model vhledu do situace (situation awareness, SA), který definuje jako stav poznání situace, probíhající ve třech kognitivních úrovních: 1) percepce prvků současné situace, 2) porozumění současné situaci, 3) projekce budoucího stavu situace. V komplexním a dynamickém prostředí je lidské rozhodování vysoce závislé na uvědomění si situace, tj. trvale se vyvíjejícím obrazu (mentálním modelu) stavu prostředí. Velmi pozoruhodné je zejména zavedení kategorie predikce budoucího stavu sys-

tému do mentálního modelu, která umožňuje rozšířit jeho aplikaci na velkou oblast systémů, které dosud stály stranou zájmu ergonomie (například sociální a ekonomické systémy).

Vhled do situace ovlivňuje rozhodování, což pak dále opět má vliv na provádění akcí. SA je na druhé straně ovlivňován stavem prostředí, jakož i faktory systému a úkolu i individuálními faktory. Faktory úkolu a systému zahrnují: kapacitu systému, design interface, stres, pracovní zátěž, složitost a automatizaci. Individuální faktory zahrnují: cíle, očekávání, dlouhodobou paměť, mechanismy zpracovávání informací, automatismy, schopnosti, zkušenost a výcvik.

V jednotlivých kategoriích SA (tj. percepci, porozumění a předvídání) je třeba hodnotit další faktory. Endsley [98] je uvádí spolu s údaji o procentech chyb, zjištěných rozbory selhání v letecké dopravě. Tyto údaje jsou obsaženy v Tabulce 2 Přílohy A.

Uvedený přehled taxonomie lidských chyb není zdaleka vyčerpávající, existuje více různých třídění. Uvedli jsme ty nejpodstatnější, které představují milníky ve vývoji principů, teorií i praktických postupů k hodnocení lidské spolehlivosti. Na základě uvedených prací Rasmussena, Reasona a Endsleye lze vytvořit obecný model fungování operátora složitého technologického zařízení, v němž je možno vyznačit uzlové body emergentní vzhledem k chybám člověka.

Rasmussen [81] je autorem generického modelu činnosti operátora, který nazval podle grafického znázornění modelem schodů (stepladder model) či přesněji přeloženo štaflí. Je to model lidské činnosti, zejména postupu, kdy se má vyřešit nějaká porucha procesu. Znázorňuje různé etáže, kterými má pracovník procházet, když se snaží zvládnout poruchu procesu. V Obraze 1 (Příloha B) je znázorněn postup činnosti operátora při řešení výkyvu nějakého parametru, který signalizuje poruchu.

Model obsahuje devět postupných kroků:

1 ALERT = podnět pro zahájení zkoumání
2 OBSERVE = určení toho, co je abnormální
3 IDENTIFY = diagnóza stavu systému
4 IMPLICATIONS = důsledky stavu systému
5 GOAL = stanovení cíle
6 PLAN = plánování úspěšného postupu
7 SELECT / FORMULATE = výběr a formulace akcí
8 EXECUTE = provedení akce
9 FEEDBACK = zpětná vazba o účinku akcí

V oblasti činnosti řízené dovednostmi jsou celkem čtyři bloky, dva na vzestupné cestě a dva na sestupné. Činnost je zahájena tím, že operátor vnímá nějakou informaci (například hlášení poplachu), která signalizuje odchylku od normálu (ALERT) a zjišťuje, o jakou odchylku se jedná (OBSERVE). Jde-li o situaci, která se nevymyká běžným stavům (tj. je operátorovi známá) a je jednoduchá, pak ihned provede nápravnou akci (EXECUTE), která je v takové situaci obvyklá a pozoruje její účinek (FEEDBACK).

Není-li však povaha problému ihned zřejmá, pak je nezbytné provést diagnózu. V této oblasti jsou dva bloky. Blok IDENTIFY znamená provedení diagnózy, tj. posouzení systému na základě symptomů, což je činnost řízená naučenými pravidly. Toto posouzení se děje podle algoritmu <jestliže> je symptom A, <pak> jeho příčinou je B. Z tohoto kroku pak vyplývají tři možné cesty: 1) Je-li diagnóza těsně spjata s nutnou akcí (vzhledem k tomu, že tato situace se často opakuje), pak operátor přechází na blok EXECUTE, tj. vykonání akce. 2) Není-li žádoucí akce ihned zřejmá, pak je třeba volit postup na blok SELECT/FORMULATE,

v němž je nutno použít akčního pravidla <jestliže> nastala situace B <pak> udělej C, tj. volba vhodné akce. Poté se vrací do oblasti dovedností tím, že zvolenou akci provede a dozví se její účinek. 3) Třetí možností je, že operátor není schopen situaci řešit ihned, protože si není jistý jejími důsledky pro bezpečnost anebo výrobu. V takovém případě je třeba, aby operátor použil svých znalostí procesu. Oblast činnosti řízené znalostmi představují tři bloky. Nejprve musí operátor posoudit situaci z hlediska možných následků toho, v jakém stavu systém je (IMPLICATIONS), tj. posoudit vývoj a předvídat důsledky toho, co se stalo, tedy to, co se může stát. Zde mohou opět nastat dvě možnosti: 1) Neexistují-li alternativní cíle, pak může operátor vkročit přímo do bloku SELECT/FORMULATE. 2) Je-li nutné uvážit dva či více možností vývoje systému, pak v bloku CÍLE operátor zhodnotí cílový stav, k němuž budou směřovat jeho další akce. Například jestliže posouzení systému naznačuje, že by mohlo dojít k riziku výbuchu, pak bude nejpravděpodobnějším cílem co nejrychlejší zastavení procesu. Jestliže na druhé straně bude pouze znehodnocena zpracovávaná dávka, pak cílem může být dokončení procesu výroby této dávky a její smíchání s jinou, aby byla dodržena požadovaná kvalita

Cílem (GOAL) je zabránit těmto důsledkům, respektive je zvládnout. Na základě těchto úsudků je třeba vytvořit plán nápravy (PLAN). Jeho obsahem je například rozhodnutí, zda dávka vyžaduje chlazení, jak toho dosáhnout a jaká obchvatová potrubí jsou k dispozici pro provedení tohoto plánu. Po provedení těchto myšlenkových operací pak se vrací do oblasti řízené pravidly, volí algoritmus <jestliže> nastala situace B <pak>proveď C, tj. volí druh zásahu a na základě svých dovedností jej provede a sleduje účinek.

Tímto způsobem je možno analyzovat konkrétní činnost operátora složitého technologického zařízení a hodnotit možnosti, jakých chyb se může v jednotlivých fázích dopustit. Analýza je založena na Reasonově citovaném modelu GEMS.

V bloku ALERT jde zejména o chyby typu „kiks“, zejména o přehlédnutí signálu, jeho nepovšimnutí. Operátor signál buď nepostřehne, anebo postřehne pozdě. Jde o nedostatek percepce (signál není vnímán, anebo je postřehnut se zpožděním), který může mít další příčiny:

- Signál není zjevně patrný, jeho objevení není operátorovi přímo zjevné, operátor musí provádět určité kroky, aby jej objevil.
- Signál je špatně detekovatelný, neboť je zahlcen v řadě podobných signálů. Podle teorie detekce signálů je obtížné oddělit signál od šumu.
- Operátor signál nepostřehne, protože v dané chvíli je zaměstnán jinými činnostmi. V daný moment má vysokou pracovní zátěž.
- Intenzita signálu je slabá, například u sluchových podnětů nízká hlasitost.

V bloku OBSERVE jde jak o „kiksy“, tak o omyly. Blok „observe“ znamená v kognitivní teorii to, že předmět vnímání je postřehnut (blok „alert“), ale musí být začleněn do mentální soustavy pomocí interpretace jeho významu, tj. vyhodnocení.

Rozhodovací algoritmus: jeden signál (informace) → jedna odpověď (akce).
Chyby v této oblasti mohou být následující:

Operátor sice signál postřehne, ale nesprávně zhodnotí jeho význam (podcení jej nebo přecení). V důsledku toho reaguje nesprávně, provede chybnou akci (v bloku EXECUTE), aplikuje chybné pravidlo.

Operátor signál nezačlení správně do své mentální soustavy (chybný mentální obraz reality), nepochopí jeho význam, v důsledku toho na signál nereaguje. Neporozumění významu signálu může mít více příčin:

a) vliv očekávání (vidí nebo slyší to, co očekává). Častým problémem je to, že lidé mají neadekvátní model toho, co je očekáváno a poté interpretují všechna vnímaná vodítka do tohoto modelu, což vede k úplně nesprávné interpretaci situace. Jdeo obecná očekávání toho, jak fungují části systému, která mohou být použita místo skutečných dat. Spolehnutí na habituální očekávání jak se bude systém chovat a nikoliv využití skutečných dat, i když jsou k dispozici.

b) je zaměstnán jinými úkoly – přetížení, v důsledku toho na danou informaci zapomene.

Operátor si neuvědomí, že může jít o kombinaci dalších možných odchylek v procesu a uplatní zkratkovitě pravidlo pro zacházení s jednou informací signalizující poruchu, aniž bere do úvahy další signály. Vynechá tudíž kroky, nutné k diagnóze stavu systému (nepřejde do bloku IDENTIFY).

V bloku IDENTIFY jde typicky o omyly vzhledem k tomu, že jde o uplatňování pravidel diagnostiky. O možných chybách zde platí totéž, co v předchozím odstavci, zejména body o nesprávném mentálním modelu reality a o tom, že operátor zkratkovitě použije nesprávné pravidlo. Operátor potřebuje posoudit další informace k tomu, aby si vytvořil správný obraz situace. Jelikož se na jednu obrazovku nevejdou všechny potřebné informace, musí si je aktivně vyhledávat. V panelovém uspořádání mohl operátor jedním pohledem zjistit, o jakou situaci jde (na analogových sdělovačích postačí poloha ručičky k poznání odchylky) a měl přehled o stavu všech relevantních zařízení (tj. čerpadel, ventilů, tlaku, průtoku, servomotorů apod.). Rozhodovací algoritmus: více signálů (informací) → diagnóza stavu systému → více možných odpovědí (akcí) → rozhodnutí (výběr alternativní odpovědi) → provedení akce.

Možné příčiny chyb:

Způsob vyhledávání informací je komplikovaný, v důsledku toho se prodlužuje doba, nutná k vytvoření správného mentálního modelu situace. To může mít za následek, že se operátor dostane do stresového stavu, který jej ovlivní natolik, že si může počínat zbrkle, zkratkovitě a situaci vyhodnotí chybně.

Operátor přehlédne určitou podrobnost, nevšimne si jí v důsledku následujících možných příčin:

- kognitivní tunelové vidění = pracovník se snaží hledat informace, které potvrzují jeho původní hypotézu o stavu procesu a zanedbává informace, které ji nepotvrzují,
- zapouzdření (encystment) = pracovník ulpívá na detailech a ignoruje důležité informace,
- tématické tuláctví (vagabonding) = pracovníkovy myšlenky těkají z jedné věci na druhou, přičemž s každou z nich se zabývá pouze povrchně
- zkratkovitý výběr pravidla = pracovník vybere to pravidlo, které se v minulosti opakovaně osvědčilo, bylo nejčastěji používáno, ignoruje další možnosti,
- polarizace myšlení = tendence vysvětlovat problém jedinou globální příčinou a ne kombinací více příčin,
- hypervigilance při stresu – panika vede k narušenému myšlení. Člověk nepoznává možné alternativy a váže se na urychlený přístup, který se zdá, že nabízí bezprostřední řešení.

Blok IMPLICATIONS předpokládá, že situace je natolik komplikovaná, že operátor

nevystačí s naučenými diagnostickými algoritmy (pravidly) a musí se uchýlit ke svým znalostem. Jde o složitou diagnostiku, v níž se uplatňuje jak důkladná diagnóza toho, co se stalo a co je příčinou současného stavu, tak posouzení toho, jak a k čemu se systém vyvíjí (trendu vývoje systému), tj. jaké důsledky pro systém může mít současný stav. Vhled do situace ovlivňuje rozhodování, což pak dále opět má vliv na provádění akcí.

Rozhodovací algoritmus: mnoho signálů (informací) → diagnóza stavu systému →hodnocení trendu vývoje systému → hledání strategie dalšího postupu (vytvoření plánu) → více možných odpovědí (akcí) → rozhodnutí (výběr alternativní odpovědi) →provedení akce.

Možné chyby operátora:

- Nepředvídání účinků akcí nebo vývoje stavu systému

Jednotlivci si sice uvědomují to, co se děje, ale nejsou schopni správně předvídat, co to znamená pro budoucnost. Toto je zaviněno:

- chybějícím či špatným mentálním modelem,
- přehnanou projekcí současného trendu,
- špatným udržením více cílů v paměti, což může ovlivňovat uvědomování si situace na všech úrovních.

- Habituálním schématem – lidé se mohou dostat do pasti habituálního schématu, provádět úkoly automaticky, což je činí méně vnímavé vůči důležitým vodítkům prostředí.

Blok GOAL znamená, že po zhodnocení trendu vývoje systému musí operátor určit cíl, k němuž má být systém doveden. V popsaném příkladu byl naznačen rozpor mezi cíli bezpečnosti (zabránit škodám způsobeným havárií systému) a cíli produkce (pokračovat ve výrobě navzdory riskantní situaci). Klasickým případem je havárie v Černobylu 1986. Operátoři prováděli experiment na příkaz nejvyšších politických činitelů, v němž měli zjistit, zda je reaktor schopen dodávat energii za nízkého výkonu, který vede k tomu, že reaktor se ocitá v nestabilním stavu. Vypnuli bezpečnostní ochranná zařízení a vzdor signálům upozorňujícím na nestabilní stav reaktoru pokračovali v experimentu, jehož následkem byla exploze. Tehdejší politické vedení bývalého SSSR naléhalo na provedení experimentu bez ohledu na možné následky.

V tomto ohledu je v normálních politických podmínkách rozhodující postoj vedení podniku. Koncepce „kultury bezpečnosti“ odhaluje vliv tohoto postoje na chování jednotlivých pracovníků a prosazuje hledisko bezpečnosti především, přičemž management musí nalézt rozumnou dělbu mezi snahou o dosažení maximálního zisku a snahou zajistit maximální bezpečnost. Tlak vrcholového managementu se přenáší v hierarchii podniku až na jednotlivé řadové pracovníky.

V bloku PLAN vytváří operátor plán postupu při zvládání nastalé situace. Příčiny chybného plánu byly naznačeny v předchozích blocích: jde o nesprávné posouzení situace a stanovení špatného cíle. Například v popsaném incidentu v Černobylu pokračovali operátoři špatným plánem, který měl udržet činnost reaktoru za krajněnestabilního stavu, i když signály na to upozorňovaly. Chyby tudíž mohou být následující:

- stanovení chybného cíle,
- vytvoření chybného plánu dalšího postupu navzdory tomu, že cíl může být správný.

Jde zpravidla o přehlédnutí podstatných podrobností, jež vedou k nesprávné diagnóze stavu systému.

Blok SELECT/FORMULATE se týká vypracování podrobného plánu činnosti vytvářením řady postupných kroků. Jedná se o řetězec dílčích cílů, jejichž dosažení podmiňuje každý následující krok. Jde o uplatnění akčního pravidla (jestliže nastala situace B, pak udělej C). V této fázi se mohou projevit následující chyby:

- vynechání některého kroku,
- přehození/záměna sledu postupných kroků (dílčí cíle), který znamená porušení algoritmu postupu,
- špatné načasování postupných kroků (příliš brzy nebo příliš pozdě).

V bloku EXECUTE jde o fyzické vykonání plánovaných akcí. Při výkonu činnosti může jít o jak o jednoduché „kiksy“, tak o důsledky chyb na vyšších úrovních v předchozích mentálních operacích:

- záměna ovládače – operátor najede myší na nesprávný ovládač,
- neprovedení nějaké akce, která podmiňuje použití ovládače, například při manipulaci s ovládačem operátor nepřepne režim ovládání z automatiky na manuální operace,
- nedbání zpětné vazby o dosažení dílčího cíle. Může dojít k ukvapenému přechodu na následující krok, když při předchozím ještě nebyl cíl dosažen.

5 Faktory ovlivňující činnost člověka

Zatímco v předchozím výkladu byl popsán psychologický přístup k lidským chybám, systémový pohled se nutně musí zabývat i vnějšími podmínkami, které umožňují či provokují, aby lidská chyba vznikla. V systémovém modelu vzniku chyb existuje základní předpoklad, že chyby vznikají ze spojení tří okolností: (1) vnitřních tendencí k chybám u daného člověka, (2) chyb navozených prostředím, a (3) iniciační události, která spouští chybový sled z této nestabilní situace. Tento sled pak může pokračovat k nehodě, nezasáhne-li nějaká bariéra či proces nápravy. Předchozí úvahy o lidských chybách se zabývaly vnitřními tendencemi člověka činit chyby. V této části jsou popsány faktory, které v kombinaci s těmito tendencemi vytvářejí situaci náchylnou k chybám. Tyto faktory jsou nazývány Performance Influencing factors (PIFs).anebo PSFs (Performance Shaping Factors). Rozdíly v těchto názvech jsou nepodstatné, značí prakticky totéž. Obecně lze faktory ovlivňující činnost definovat jako faktory, které determinují pravděpodobnost chyby či efektivního výkonu lidí.

Je třeba poznamenat, že tyto faktory nelze automaticky spojovat s lidskou chybou. Takové faktory jako kvalita postupů, úroveň časového stresu a účinnost výcviku představují kontinuum od nejlépe uplatnitelného (např. ideálně navržený výcvikový program založený na adekvátní analýze potřeb výcviku) k nejhorším možným (což odpovídá stavu, kdy není žádný výcvik prováděn). Jsou-li tyto faktory k dané situaci optimální, předpokládá se, že též výkon člověka bude optimální. I když jsou PIFs optimální, může však stále docházet k chybám. Je tomu tak pro dva důvody: (1) i v optimálním případě zůstává určitá variabilita výkonu. (2) PIFs odpovídají faktorům designu, operací a údržby, které ovlivňují spolehlivost hardwarového zařízení. Např. spolehlivost čerpadla je ovlivňována řadou faktorů: typ a teplota tekutiny, přítomnost ochranných prvků, problémy dodávky tekutin, efektivnost údržby, podmínky prostředí, operační problémy.

5.1 Aplikace

Systémový pohled předpokládá využití seznamu PIFs v nejméně pěti oblastech: 1) jako prostředku auditu k identifikaci problémových oblastí, 2) při vyšetřování nehod, 3) při kvalitativní predikci možných chyb, 4) při hodnocení operačních podmínek, za nichž jsou úkoly prováděny 5) ve fázi designu.

5.2 Klasifikační struktura faktorů ovlivňujících činnost

Je založena na teorii lidských chyb, která proklamuje, že chyby vznikají z nesouladu mezi požadavky a zdroji. Požadavky na činnost člověka jsou pracovní úkoly, například sledovat panel. Zdroje vystihují povahu lidských schopností k zvládnutí těchto požadavků například percepční dovednosti, myšlení, tělesné akce. Tam, kde požadavky přesahují zdroje, lze očekávat výskyt chyb. Tato teorie je založena na racionálních předpokladech, které byly doloženy řadou experimentálních důkazů. V řadě případů však chybí experimentální doklady. Nicméně následující přehled, převzatý z publikace Guidelines for Preventing Human Error in Process Safety [82], poskytuje dobrou základnu pro praktické uplatňování PIFs v souboru nástrojů pro řízení politiky bezpečnosti.

Model předpokládá při nejmenším tři kategorie: nároky, zdroje, politika. Klasifikační schéma je uvedeno v Tabulce 3 (Příloha A). Dělí PIFs do čtyř hlavních skupin a 12 intermediárních kategorií. Je třeba zdůraznit, že tento seznam nemusí být vyčerpávající. Jiní autoři používají dalších seznamů, avšak zdá se, že předložené klasifikační uspořádání je nejkompletnější.

1. Operační prostředí

1.1 Prostředí pracovního procesu

1.1.1 Četnost nasazení pracovníků

Četnost, s jakou byl úkol v minulosti pracovníkem prováděn, ovlivňuje pravděpodobnost úspěchu. Dovednosti, které nejsou často prováděny (např. při úkolech, které jsou vyžadovány pouze nepravidelně), nemusí být správnězafixovány a výkon se zhorší. Zda toto zhoršení povede k významné chybě, závisí na dalších faktorech (jako např. opakovaný výcvik, podrobné postupy apod.).

1.1.2 Složitost událostí v procesu

Jde například o rozsah operací, které mají být prováděny. Vztahy mezi proměnnými a požadovaná přesnost ovlivňuje výkon lidí. Příklady jsou operace zahájení a ukončení provozu, které obsahují vysoký stupeň složitosti.

1.1.3 Vnímané nebezpečí

Jde o jeden z nejzávažnějších stresorů v mnoha pracovních procesech. Vzniká z neúčinné kontroly a dohledu nad těmito systémy. Navzdory skutečnosti, že moderní závody jsou vybaveny automatickými ochrannými systémy, vždy existuje určitá percepce možného rizika. Závažné nebezpečí může existovat i pro okolí závodu. Prostředí, které je vnímáno jako vysoce nebezpečné, zvyšuje stres pracovníků, což může zhoršovat jejich výkon.

1.1.4 Závislost na čase

Týká se času, který je k dispozici pro zvládnutí události. Je to známý stresový faktor, který ovlivňuje výkon. Časová odpověď systému zařízení a fyzikálních či chemických procesů určuje čas, který je k dispozici pro reakci na incident.

1.1.5 Náhlost vzniku události

Při poruše hraje důležitou roli náhlost jejího projevu. Týká se času, který je nutný k tomu, aby se symptom vyvinul do té míry, že jej mohou pracovníci detekovat. Vyvíjí-li se symptom postupně, je zde určitý prostor pro pracovníky, aby zpozorněli, což jim umožní vyvinout správný mentální model stavu procesu. Jestliže se nepříznivá situace vyvíjí extrémně pomalu, nemusí být detekována, zejména tehdy, vyvíjí-li se po více než jednu směnu.

1.2 Fyzické pracovní prostředí

Obecně platí, že špatné prostředí vede k anxietě a únavě, což může vést k chybám.

1.2.1 Hluk

Účinky hluku závisí mezi jiným na charakteristikách hluku samotného a na povaze prováděných úkolů. Intenzita a frekvence hluku determinují rozsah „maskování“ různých akustických klíčů, např. auditivních alarmů, verbálních zpráv apod. Trvání expozice hluku ovlivňuje únavu. Na druhé straně účinky závisí též na typu úkolu. Provádění jednoduchých rutinních úkolů nemusí podléhat vlivu hluku a často též zlepšuje výkon v důsledku zvýšené bdělosti člověka. Výkon obtížných úkolů vyžaduje vyšší stupeň kapacity zpracování informací, což zhoršuje výkon. Úkoly vyžadující značnou pracovní paměť jsou horší. Poulton [83] vysvětluje tyto účiky tím, že „vnitřní řeč“ je maskována hlukem – „nemůžete se slyšet“. Při úkolech během neobvyklých postupů, mentálních počtech apod., může hluk maskovat vnitřní smyčku vyvolání z paměti, což zpomaluje práci a člověk je pak náchylnější k chybám. Jiný účinek hluku při monitorování a interpretaci velkého počtu informačních zdrojů je „zúžení rozsahu pozornosti“. Lidé kontrolující panely se v hlučném prostředí snaží koncentrovat na nejzřejmější aspekty situace, se kterými jsou dobře obeznámeni a nevnímají jakékoli nové rysy situace. Dále může permanentní vystavení hluku znemožňovat příležitosti k sociální komunikaci a činit práci nudnější.

1.2.2 Osvětlení

Kromě fyzického diskomfortu iritace může špatné osvětlení navozovat chyby při čtení značek na ventilech a přístrojích na kontrolním panelu. Přímé či odražené oslnění může vést k dalším problémům – vyhnout se oslnění může pracovníkovu pozornost odvést od předmětu práce.

1.2.3 Teplotní podmínky

Často bývají chyby vynechání něčeho důsledkem práce v nepříznivých klimatických podmínkách. Chlad ovlivňuje kontrolu svalů, snižuje obratnost a sílu. Zkušenosti a praxe způsobují to, že činnost je založena hlavně na dovednosti a proto i resistentnější k zhoršujícím vlivům teploty – začátečníci bývají extrémní teplotou více ovlivňováni.

1.2.3 Atmosférické podmínky

Mnoho pracovních činností se odehrává v prostředí, v němž jsou lidé vystaveni prachu, plynům, párám apod. Osobní ochranné prostředky bývají obvykle překážkou pro rychlý pracovní výkon a pokusy provádět práci rychle mohou vyústit do chyb.

1.3 Rozvrh práce

1.3.1 Pracovní doba a přestávky na oddech

- Poruchy spánku

Výzkumy prokázaly jasný pokles psychologických a behaviorálních výkonů. Zhoršují se zejména: úkoly delší než 30 minut, málo nové a málo zajímavé či podnětné, složité. Spánková deprivace vede též k zhoršení paměti. K zotavení postačí jedna či dvědalší noci spánku. Účinky chronické spánkové deprivace byly zkoumány poměrně méně. Dosud je málo známo o vztazích mezi velikostí deficitu spánku, míry akumulace, množstvím a načasováním optimálního zotavovacího spánku. Studie o částečné deprivaci spánku ukazují, že lidé mohou snášet nespavost a dodržovat úroveň své výkonnosti, jestliže spí kratší dobu než normálně – limit se zdá být okolo 4 až 5 hodin denně. Závisí to však na pravidelnosti – lidé s nepravidelnou dobou spánku mívají větší potíže. V podmínkách akutní deprivace spánku se objevuje častěji „mikrospánek“, který je málo účinný pro zotavení.

- Dlouhá pracovní doba a únava

Zkrácení pracovní doby je prospěšné pro produktivitu práce. Překročení 8hodinové práce vedlo k nižší produktivitě, vyšším absencím a větší nehodovosti. Novější studie však toto problematizují – hledají se alternativní řešení, např. zkrácení pracovního týdne při 12hodinovém dni. Pokusy Bartletta [84] s piloty přispěly k závěru, že únava přispívá k tunelovému vidění, dále bylo zhoršeno časování akcí a schopnost anticipovatsituace. Účinky únavy na dovednou aktivitu znamenají ústup na dřívější stadia učení.

Závěry:

- Ve většině studií byli zkoumáni mentálně a tělesně zdraví mladí lidé – málo je známo o účincích na starší lidi
- K únavovým jevům při dlouhé denní pracovní době dochází po 4 dnech
- Málo je známo o kumulativních účincích mimopracovní aktivity a dlouhé pracovní době

Strategie unaveného pracovníka:

- Pomalejší tempo práce
- Pečlivější kontrola práce
- Používání více taháků paměti
- Spolehnutí na spolupracovníky
- Provádění méně kritických úkolů

1.3.2 Rotace směn a noční práce

Noční práce byla studována z hlediska dvou aspektů: porušení cirkadiánních rytmů a účinky na rodinný život. U cirkadiánních rytmů se prokázala shoda stavu bdělosti s tělesnou teplotou. Pro psychické funkce obsahující více složitějších kognitivních prvků, kde je důležitá pracovní paměť se vzorec účinků mění: paměť má protichůdné poklesy a vrcholy než tělesná teplota.

2. Charakteristika úkolů

2.1 Design prostředků

2.1.1 Umístění, přístup

Pracovníci si často stěžují, že například čerpadla bývají nepřístupná. Nouzová čerpadla by měla být vždy snadno přístupná, jiná, která jsou obsluhována řídce (jednou do roka apod.) mohou být mimo dosah. Při této frekvence je rozumné žádat po pracovníkovi, aby použil žebříku. Dosah se má týkat nejméně 95 % populace.

2.1.2 Označení: Vyžaduje to též častou kontrolu

2.1.3 Osobní ochranné prostředky

Normy pro jejich používání jsou vydávány řídicími orgány. Přehled ergonomických aspektů podali Moran a Ronk [85].

2.2 Design kontrolních panelů

Kontrolním panelem se rozumí řídicí místnost, v níž jsou soustředěny sdělovací a ovládací prostředky – interface člověk-stroj. Standardní učebnice ergonomie (např. Salvendy [86]) obsahují podrobné údaje k designu.

2.2.1 Obsah a relevance informací

Prvotní otázkou je, jaké informace jsou zapotřebí. Příliš málo informací zvyšuje míru dedukcí, které musí pracovník dělat k předvídání stavu parametrů, které nejsou přímo zobrazeny. To je zejména důležité v nouzových situacích. Na druhé straně příliš mnoho redundantních informací může přetížit pracovníka. Je proto nutné aplikovat některou z metod úkolových analýz a to tak, abychom pomocí řízených rozhovorů s vybranými pracovníky zjistili, kolik a jaké informace bude potřebovat.

Dalším faktorem designu je relevance informací. Tento princip je často porušován při zavádění počítačových systémů, kde bývá mnoho informací potřebných pro počítačové odborníky či výrobní manažery, které se pletou do informací potřebných k bezpečnému řízení provozu. Je potřeba určitý druh strukturování a priorizace pro různé uživatele systému.

2.2.2 Identifikace sdělovačů a ovládačů

Tento bod bývá označován jako kódování: označením nálepkou, barvou, tvarem, umístěním, velikostí. Je třeba uvážit pečlivě vztah mezi sdělovačem a ovládačem. Běžným problémem v mnoha podnicích je nedostatek informací pro limity tolerance pro různé kritické parametry. Pracovníci potřebují vědět, jak rychle se parametr pohybuje ke svým limitům tolerance, aby rozuměli urgentnosti situace.

2.2.3 Kompatibilita s očekáváním uživatelů

Týká se podobnosti mezi směrem fyzického pohybu ovládače anebo sdělovače a očekáváním pracovníka. Je třeba vzít v úvahu populační očekávání, například zesílení ve směru pohybu ručiček hodin, zeslabení obráceně proti pohybu. Za normálních okolností to nemusí tolik vadit, ale za mimořádných to může vést k chybám, jak o tom svědčí incident v TMI: otevření ventilu bylo signalizováno rozsvícením kontrolky, zhasnutí signalizovalo

zavření ventilu. V důsledku poruchy elektrického vedení však při jeho uzavření sice došlo k zhasnutí signálky, ale ne k uzavření ventilu. Po dvou hodinách došlo k úniku radioaktivního chlazení z reaktoru.

2.2.4 Seskupování informací

Týká se prostorového uspořádání. Obecně platí, že parametry procesu funkčně spjaté mají být též blízko sebe. Vnímá se to jako větší pravděpodobnost, že daná chyba vede k vzorci symptomů, které lze snadněji interpretovat, než jako náhodnou distribuci informací. Porušení tohoto pravidla nemusí vést k chybám, ale brzdí výkon. Příklad: Porucha regulátoru páry v turbině zavinila vzrůst profilu vysokého tlaku ve třech kondensátorech. Pracovníci si nevšimli vzrůstu tlaku ve všech třech kondenzátorech – byly použity dva dvoukanálové snímače namísto jednoho tříkanálového, a navíc třetí kondenzátor byl na panelu umístěn na odlišném místě, než ty první dva. To vedlo k nižší pravděpodobnosti, že jakákoli odchylka bude detekována pomocí normální strategie kontroly spojených subsystémů.

2.2.5 Přehledné uspořádání kritických informací a poplachových upozornění

Se vzrůstající složitostí závodů může být velmi užitečný přehled sdělovačů kritických informací o procesu a poplachových hlášeních. Několik badatelů obhajuje koncepci integrovaného displeje, který může být konstruován na systémech založených na počítačích. Různé radiální škály jsou adjustovány tak, že normální operace je zobrazována normálním geometrickým tvarem, zatímco odchylky naznačují poruchy. Tento typ displeje je založen na lidské schopnosti „poznávání vzorce“ a může podporovat včasnou detekci abnormálních stavů.

2.3 Pracovní pomůcky a postupy

Se vzrůstem složitosti závodů je zřejmé, že není možné se spoléhat výlučně na dovednosti a paměť pracovníků k výkonu práce. Pracovní pomůcky a postupy jsou metody zamýšlené ke snížení nároků na pamatování si postupů a odkazů, jakož i snížení množství nutného rozhodování. Používá se: tokových grafů, kontrolních seznamů, rozhodovacích tabulek standardních operačních instrukcí a postupů při haváriích.

2.3.1 Kritéria pro výběr pracovních pomůcek

Pro výběr vhodné metody k podpoře pracovníkům je třeba uvažovat o charakteristikách úkolu a typu podpory. Postupové diagramy a rozhodovací tabulky např. nabízejí stručnou organizaci informací a pracovní kritéria, požadovaná k provádění diagnózy chyb a plánován úkolů. Kontrolní seznamy jsou vhodnější pro úkoly, které obsahují sled kroků, který je nutno si zapamatovat. Postupy poskytují instrukce krok za krokem, jak a kdy provádět různé úkoly, které obsahují požadavky na paměť, kalkulace, přesnost a obtížné rozhodování. Standardní operační instrukce bývají obvykle určeny pro kritické úkoly, obsahující změny v operačních podmínkách závodu jako zahájení či odstavení provozu anebo změny paliva pro rafinační pece. Havarijní postupy jsou poskytovány pro úkoly obsahující diagnostiku selhání, stabilizaci a odstranění abnormálních podmínek.

Důležitou otázkou je, jak mnoho mají být požadavky práce podporovány pracovními pomůckami a postupy oproti výcviku. Nahrazují-li pomůcky výcvik, může být pracovník příliš vázán na ně a tak být vulnerabilní v situacích, když pomůcky obsahují chyby anebo jestliže dojde k nepředvídatelným situacím. Na druhé straně přílišné přetěžování pracovníka informacemi a dovednostmi při výcviku může v dlouhodobé perspektivě vést k poklesu výkonu. K určení rozsahu pomůcek oproti výcviku je nutno kalkulovat investice do obojího. Obecně

platí, že pracovní pomůcky a postupy jsou užitečné pro úkoly prováděné zřídka anebo vyžadují složitou logiku, např. diagnostické pomůcky. Lze je použít i v situacích zahrnujících dlouhé a složité sledy akcí, a kde odkazy na tištěné instrukce nenarušují práci. Výcvik má být určen pro úkoly, které jsou prováděny často, vyžadují složité manuální dovednosti, závisí velmi na týmové práci či obsahují nepředvídatelné podmínky. Tyto úvahy lze přímo vztáhnout na klasifikaci skill-, rule- and knowledge.

2.3.2 Jasnost instrukcí

Zahrnuje jak jazyk a formát instrukcí. Poukazuje se na čtyři způsoby zlepšení srozumitelnosti technické řeči:

- vyhýbat se používání více než jedné akce v jednotlivém kroku postupu
- používat jazyk stručný ale srozumitelný uživatelům
- používat aktivního způsobu (např. “otoč spínač 12A”, nikoli “spínač 12A má být otáčen”)
- vyhnout se složitým větám, obsahujícím více než jedno negativum

Příkladem nedostatku jasnosti instrukcí může být incident v jednom podniku, kde operační instrukce požadovala, aby ventil A byl otočen do polohy „manuálně zavřená poloha“. Pracovník to interpretoval, že má ventil zavřít, čímž zablokoval přívod paliva.

Formát postupu je důležitý. V některých situacích je lepší použít vývojového diagramu nebo rozhodovací tabulky než textu.

2.3.3 Úroveň popisu

Málo informací není vhodné pro začátečníka, příliš informací zase pro zkušeného pracovníka. Příkladem může být chyba, ke které došlo nedostatkem podrobností. Mistr na denní směně před odchodem z pracoviště dal noční směně pokyn o čištění reaktoru a napsal: „vmíchejte 150 litrů roztoku dusičnanu po dobu 4 hodin“. Nesdělil jim však, že musí nejdříve naplnit reaktor vodou, neboť to již dávno předtím dělali. Noční směna splnila příkaz, avšak bez vody. V důsledku toho se vyvinula prudká reakce a reaktor explodoval.

2.3.4 Kvalita kontrol a varování

Kontrola kritických parametrů a varování před riskantními podmínkami má být výrazně odděleno od ostatního textu, aby nebylo přehlédnuto.

2.3.5 Podpora při diagnostice chyb

Je užitečné poskytnout pracovníkům nějaká vodítka, jak provádět diagnózu při odchylkách od normálního provozu.

2.3.6 Kompatibilita s operačními zkušenostmi

(1) Postupy neodpovídají způsobům, jakým je práce skutečně prováděna: Postupy bývají často vypracovány při prvním provozu a bývají pak zřídkakdy revidovány k zapracování změn hardware anebo operačního režimu. Navíc bývají často napsány na základě systematické analýzy úkolů, jak jsou vnímány pracovníky či jiným personálem, kteří je mají používat. Odstranění těchto potíží: umožnit, aby pracovníci, kteří budou na zařízení pracovat, byli aktivně zapojeni do jejich vypracování. Aktualizace je nutná.

(2) Informace v postupech jsou správné, ale nejsou zpracovány způsobem použitelným na pracovišti. Často jsou uloženy v kancelářích. Pro některé se zdají zbytečné: např. úkoly založené na dovednostech, které provádějí zkušení pracovníci. Některé však bývají nutné, např. hledání závad či diagnóza. Podrobné postupy bývají potřebné v neobvyklých situacích, zejména pak tehdy, kdy není možné ponechat způsob řešení na samotném pracovníkovi. Je třeba sladit vypracované postupy s obsahem výcviku.

(3) Není dostatečně rozlišeno mezi postupy jakožto normami a instrukcemi k provádění úkolu. Forma normy nebývá vhodná jako účinná operační instrukční pomůcka.

(4) Pravidla a postupy se netýkají jedinců anebo situací. Jde-li o situace, kde neplatí normální postupy, je nutno je pečlivě definovat a kontrolovat proaktivní vývinem “pravidel”, které explicitně stanoví hranice platných podmínek.

(5) Uživatel nerozumí zásadnímu myšlení v nich obsaženému, a proto provádí alternativní akce, které vedou k dosažení téhož účelu, ale provádí se snadněji.

2.3.7 Frekvence aktualizace

Instrukce k používání jsou často dodávány od výrobců zařízení, nemusí odpovídat praxi vzhledem k častým změnám technologie Je důležité je často aktualizovat, neboť rychle zastarávají.

2.4 Výcvik

Výcvik operačních pracovníků plní více funkcí: schopnost vykonávat práci, používat nové zařízení, reagovat na mimořádné události, udržovat dovednosti se zavedením automatizace, efektivně pracovat v týmu. Výcvik mimo práci a při práci: lze tyto formy vzájemně doplňovat.

2.4.1 Konflikt mezi požadavky bezpečnosti a produkce

Následující incident ilustruje důležitost toho, aby tento konflikt byl vysvětlen při výcviku. V rafinérské peci byl zpozorován rozdíl mezi dvěma hořáky: hořák A se jevil dobrý, kdežto hořák B byl nestabilní. Postup naznačuje dvě možnosti: a) udržet anebo snížit produkci zavřením ventilu hořáku B a současně zlepšit stabilitu hořáku A, b) odstavit pec a vyfoukat ji vzduchem. Výcvik musí zdůraznit hlediska bezpečnosti. Naneštěstí pracovník volil alternativu a) a došlo pak k výbuchu pece.

2.4.2 Výcvik v používání nového zařízení

I když se nové zařízení podobá starému, je nezbytné zaškolit pracovníky v jeho používání. Příkladem zanedbání je nehoda v jednom podniku, kde pracovník údržby prováděl demontáž nového čerpadla, které se lišilo od dosavadních. Neprovedl danou operaci, na níž nebyl zvyklý. Došlo k úniku páry, která zasáhla jeho oči.

2.4.3 Praxe ve zvládání nezvyklých situací

Dovednosti v řešení situací lze osvěžovat v opakovacím výcviku. Užitečné jsou výcvikové simulátory. Techniky učení diagnostickým dovednostem popisuje Embrey [99]. Jedna z klasických reakcí na nezvyklou situaci je, že se lidé vracejí k dříve naučeným dobře vytvořeným zvykům a strategiím, které mají určitou podobnost s novou situací, avšak které jsou zcela nevhodné. Takové strategie se dříve osvědčily anebo byly zdůrazňovány v hava-

rijních postupech nebo při výcviku. Lidé se musí naučit jak zůstat, i při změnách podmínek a přehodnotit tak své původní hypotézy. Jiné typy lidských chyb při mimořádných podmínkách byly popsány v předchozí kapitole.

2.4.4 Výcvik v používání havarijních postupů

Výcvik je důležitý pro to, aby pracovníci mohli aplikovat naučené postupy správně a to i za časového tlaku. Při výcviku je nutno cvičit situace vstupu či přechodu k jiným postupům, požadavky bezpečnosti-produkce a reakci automatizovaných ochranných systémů.

2.4.5 Výcvik v práci s automatizovanými systémy

Jakýkoli výcvikový kurs musí uvádět možná rizika, která vyvstávají ze situací, když se pracovníci snaží odstavit automatický systém. Stejně však je třeba upozornit jakékoli případy, kdy se pracovníci přehnaně spoléhají na dobrou práci těchto systémů anebo jim nevěří bez správné kontroly. Užitečnou strategií k překonání těchto problémů je „křížová kontrola“ přístrojů měřicích stejné nebo funkčně svázané parametry, např. teplotu a tlak.

2.4.6 Vývoj výcvikového programu

V praxi se v podnicích málo využívá analýz úkolů k definování nutných mentálních a tělesných dovedností. Místo toho je obvyklý výcvik při práci, který však je málo účinný. Je zde nebezpečí, že se nováčci naučí nevhodným či dokonce nebezpečným praktikám. Proto je nezbytné, aby výcvikový program byl založen na podrobných a systematických postupech, které obsahují tato stadia.

3. Charakteristiky operátora

Ačkoli mnohé z individuálních faktorů mohou ovlivňovat lidské chyby, v praxi je pouze velmi málo kontrolovaných studií, který poukazují na tento vztah.

3.1 Zkušenosti

3.1.1 Úroveň dovedností

Při nácviku dovedností existují tři stádia jejich úrovně. 1) První stádium jsou obecné znalosti principů fyziky a chemie. 2) Při další praxí v podniku dochází ke kompilování znalostí do formy praktického „know-how“ ve formě pravidel, pomocí nichž lze řešit problémy. 3) Po značných zkušenostech nastupuje stadium dovedností, které vyžadují nejméně pozornosti a paměti.

3.1.2 Zkušenosti se stresovými událostmi v procesu

Lze je získat při praxi v práci a pomocí simulátorů. Oba typy mají svá pro a proti. Při simulátorech lze vykonávat větší kontrolu probíhajícího procesu a operační tým může těžit z dobře připravených instrukčních metod. Použití simulátoru však postrádá stresový faktor plynoucí z možné katastrofy. Nicméně je problémem, zda se lidé mohou učit efektivně při stresu. Nejlepší je kombinace obou způsobů.

Ve studiích více autorů se zjistilo, že lidé, kteří úspěšně zvládli mnoho dřívějších stresových zkušeností, podávají lepší výkon za stresu než lidé bez těchto zkušeností. Avšak z těchto studií není zřejmé, jaký druh postojů a dovedností lidé ve stresu získávají. Lze se domnívat, že vyvinou generické strategie řešení problémů, zůstávají pozorní na měnící se podmínky systému a trvale vyhodnocují své pracovní domněnky. Ve svých pracovních postojích mohou získat větší sebedůvěru, že mohou zvládnout neočekávané situace a vykonávat tak větší emocionální kontrolu a uchovat dobré pracovní vztahy se svými kolegy.

3.2 Osobní faktory

Přehled stavu poznání běžných praktik při výběru pracovníků na místa kontroly procesu uvedl Astley et al. [87]. Jeho závěrem je, že základna pro výběr různých testů a výběrových pomůcek bývá často povrchní. Téměř neexistuje měření výkonu, které by mohly naznačit, které testy jsou validní pro předpověď výkonu. Personalisté málokdy očekávají, že výběr lidí jim umožní překonat špatný výcvik anebo design práce. Výběr pokládají jako něco, co by se mělo dělat dobře a uvážlivě, aby se dosáhlo co nejlepšího řešení. Neočekávají, že výběr sám o sobě by mohl řešit operační problémy.

3.2.1 Motivace

Motivace pracovníků chovat se při práci bezpečným způsobem je důležitým prvkem. Problém jak má toho management podniku docílit, však doposud nebyl dostatečně prozkoumán. Ukazuje se například, že bezpečnostní kampaně zpravidla pouze snižují ochotu pracovníků referovat o nehodě, než aby významně snižovaly výskyt nehod. Motivace strachem se ukázala méně účinná než obecné výzvy. Nepříjemné věci obvykle ovlivní postoj, ale ne chování, zpravidla utvrzují postoj těch, kteří jsou již přesvědčení zastánci předkládaných argumentů, například nekuřáci. Ukázalo se například, že používání OOPP je nejvíce ovlivňováno nikoli kampaněmi, ale hraním rolí při školicích akcích.

3.2.2 Riskantní jednání

Koncept sklonu k nehodám vychází ze statistických šetření. Na základě nehod v muniční továrně v průběhu 1. světové války se ukázalo, že určitá malá část dělníků měla více nehod, než by se dalo očekávat vlivem náhody. Pokusy o vysvětlení tohoto jevu pomocí charakteristik osobnosti měly malý úspěch – buď vysvětlovaly pouze malou část variance (20 %), anebo faktor relevantní v jednom případě byl irelevantní v dalších případech. Shaw a Sichel [88] uzavírají, že existuje pouze slabá statistická evidence tohoto rysu.

Verhaegen et al. [89] provedli studie tří skupin pracovníků: a) „aktivní“skupina – byli účastni nehod, b) „pasivní“ skupina – byli pouze nevinnými účastníky nehod, c) kontrolní skupina nebyli spojeni s nehodami. Byla aplikována série dotazů zaměřených na: 1. míru rizikového chování, 2. vnímaná rizika práce, 3. používání OOPP, 4. diskomfort při nošení OOPP, 5. pozitivní postoj vůči oddělení bezpečnosti, 6. percepce, že nehody jsou svou povahou nahodilé. Výsledky ukázaly, že jsou rozdíly mezi skupinami v bodech 1,2,5. Aktivní skupina měla významně vyšší skóre v míře rizikového chování ve srovnání s oběma dalšími skupinami. Aktivní a pasivní skupina měla pozitivnější postoj vůči odd. bezpečnosti (asi proto, že při vyšetřování s ním přišli do styku). Výsledky naznačují pozitivní vztah mezi percepcí rizika, riskantním chováním a zvýšenou pravděpodobností nehod.

3.2.3 Teorie homeostázy rizika (RHT – Risk Homeostasis Theory)

Teorie byla vyvinuta původně pro oblast chování řidičů. Podle ní míra nehod není určována úrovní skutečného rizika, ale úrovní rizika přijatelného pro jednotlivce v dané situaci. Teorie naznačuje, že lidé přizpůsobují své riskantní chování tak, aby udržovali konstantní úroveň vnímaného rizika. Zavedou-li se zlepšená bezpečnostní opatření (např. lepší ochrana), pak se lidé budou chovat riskantnějším způsobem tak, aby udržovali svou navyklou úroveň rizika.

Teorie vyvolala velké diskuse. Mnohé z nich se týkaly zlepšení bezpečnostních podmínek, které by takto mohly být neúčinné. Oponenti též poukazovali na to, že lidé špatně odhadují velikost rizika a tak nejsou s to modifikovat své chování podle objektivních změn možností rizika. Mnozí namítali, že teorie byla vyvinuta pro chování řidičů a že v jiných podmínkách je její uplatnění sporné. Diskuse se týkaly např. toho, zda zavedení bezpečnostních pásů bylo kompenzováno riskantnějším chováním řidičů. Přenesení teorie do podmínek bezpečnosti na podniku je problematické.

3.2.4 Lokus kontroly (locus of control)

Znamená tendenci člověka připisovat příčiny událostí, které se mu stanou, buďsobě (vnitřní, internal) nebo vnějším okolnostem (externím). Výzkumem se zjistilo, že „internálové“ inklinují k hledání informací o problému a pokoušejí se ho kontrolovat sami. Externálové předpokládají, že problém je mimo jejich bezprostřední kontrolu a pokoušejí se hledat pomoc u svých kolegů. V mimořádné situaci se očekává, že internálové odpovídají lépe, protože věří, že jejich akce ovlivní to, co se děje, kdežto externálové cítí, že jejich akce nemají vliv na to, co se děje. Doklady o lepším výkonu internálů při mimořádné události v jaderné elektrárně zjistil Gertman [100].

3.2.5 Emoční kontrola

Roger a Nesshoever [90]definují tuto vlastnost jako tendenci zabránit emocionálním reakcím během krize. Škála pro měření tohoto konceptu má čtyři faktory:

- Příprava– zabývání se minulými událostmi
- Emocionální inhibice – tendence skrýt emoce
- Kontrola agresivity – tendence zabránit agresivním reakcím
- Vlídná kontrola – tendence neříkat rozčilující věci

Emoční kontrola udržuje dobrou komunikaci v týmu zejména v dobách, kdy tým obdrží negativní zpětnou vazbu o svém výkonu.

3.2.6 Typ osobnosti A resp. B

Typ B je relaxovaný, nespěchá, převládá u něj uspokojivý přístup k životu a k práci, kde snaha po úspěchu plyne po proudu života a ne proti němu. Typ A charakterizuje snaha po úspěchu, zaobírá se časem a úspěchem i proti proudu prostředí, je neklidný, má trvalé pocity že je pod tlakem (Friedman a Rosenman [91]). Typ A se pokládá za méně efektivní při stresu než typ B. Vzhledem k bezpečnosti práce nejsou doklady o rozdílném vlivu a chování.

3.3. Tělesný stav a věk

Murrell [92] uvádí čtyři biologické změny spojené s věkem:

- Pokles zrakové ostrosti a rychlosti diskriminace, která se týká velikosti detailu schopnosti vnímat jemné škály.
- Pokles kapacity zpracovávat informace na kontrolním panelu.
- Pokles pracovní paměti, ovlivňující množství informací, které lze podržet po dlouhou dobu.
- Tendence k větší manuální variabilitě, ovlivňující výkon v úkolech, kde tempo diktuje stroj, zejména v manufakturní výrobě.

Tyto vlastnosti jsou výsledkem biologických změn zapříčiněných věkem. Úroveň zkušeností však může tyto efekty potlačovat. Pokračující praxe v určité práci může vést k tomu, že tyto věkové rozdíly zmizí. Navíc mohou starší lidé vyvinout účinnější metody práce a tak minimalizovat nároky práce. Griew a Tucker [93] zjistili, že ve strojní dílně starší lidé dosahovali týchž výsledků pomocí menšího počtu kontrolních pohybů než lidé mladší.

4 Organizační a sociální faktory

4.1Týmová práce a komunikace

Zvyšující se složitost postupů v moderních podnicích vyžaduje týmovou práci. Výcvik týmů je stále důležitější pro bezpečnou a účinnou práci.

Následující PIFs hrají kritickou roli v kolektivním úsilí a komunikaci:

4.1.1 Rozdělení pracovní zátěže

Určuje míru přetížení nebo nedostatečné zátěže pro každou osobu. Je známo, že spolehlivost se snižuje, mají-li lidé příliš mnoho či příliš málo práce. Následující incident popisuje nevhodné rozdělení zátěže. Mistři občas bývají přetíženi. Byl hlouben příkop pro potrubí a svářeči pracovali na dvou místech. Práce začala v 8 hod. ráno. Ve 12 hod. mistr přikázal odstranit zaslepení, aniž se byl podívat na místo. Potrubí sice bylo prázdné, avšak několik litrů oleje v potrubí zůstalo. Olej se vylil na svářecí místo a byl zapálen. Následkem požáru jeden svářeč byl zemřel. Přetížení jinými úkoly znemožnilo mistrovi jít se podívat na místo.

Na druhé straně, při nedostatečné zátěži si pracovníci neuvědomují příliš změny podmínek. Ke zvýšení úrovně aktivity při monitorovacích pracích lze předepsat úkoly navíc, jako např. výpočet spotřeby paliva, životnost katalyzátoru, účinnost pece apod.

4.1.2 Jasnost odpovědností

Odpovědnost musí být jasně specifikována jak pro každodenní úkoly, tak pro mimořádné události. Rozlišuje se: role „ambiguity“ = nedostatečné informace o roli při práci. Odráží se v tom nejasnost o cílech práce, o očekáváních kolegů a o rozsahu a odpovědnosti v práci. Role „conflict“ značí, že jde o současný výskyt dvou či více souborů tlaků, takže splnění jednoho činí potíže při plnění dalších (Kahn et all. [101]). Například manažer instruuje pracovníka, aby provedl určitou akci, která je v rozporu s instrukcemi, které tento dostal od svého mistra.

4.1.3 Komunikace

Následující dva incidenty popisují selhání komunikace (lidé si navzájem neřeknou to, co je zapotřebí). Kletz [94] uvádí následující příklady: 1) Personál laboratoře byl požádán o analýzu atmosféry v tankeru (zejména o to, zda je přítomen uhlovodík). Ti tomu rozuměli tak, že mají zjistit, zda je přítomen kyslík. Po analýze telefonicky hlásili, že nebyl žádný detekován. 2) Mistr údržby byl žádán, aby se podíval na poruchu čerpadla chladicí vody. Aby předešel poškození stroje, rozhodl, že je nutno ihned snížit rychlost. Neřekl to však ihned operačnímu týmu. Chladicí voda vytekla, proces byl narušen a v chladiči se objevila trhlina.

4.1.4 Autorita a vedení

Skupiny mívají svou neformální strukturu statusu, která se od formální může lišit. V každodenní práci to bývá obtížné zjistit, avšak při mimořádných situacích může neformální struktura způsobit rozdílnou interpretaci situace a stavové problémy mohou vytvářet potíže v tom, čí mínění je třeba respektovat. Způsob, jak týmy zacházejí s nesouhlasem, je kritický. Výkon může být brzděn tím, co bylo nazváno „jalový odpor“. Jednotlivec s vysokým smyslem kompetence vyžaduje svobodné vyjádření své schopnosti. Není-li to uznáno a je-li postaven do subordinační pozice, výkon se velmi zhorší tendencí a dotyčný člověk může ukázat, „jak to mohlo být lepší, kdyby se to udělalo podle mne“.

4.1.5 Skupinové plánování a orientace

V mimořádné situaci tým musí věnovat určitý čas plánování správné strategie jak zvládnout situaci a jak přidělit odpovědnost jednotlivým členům. Není to snadné, neboť většina reakcí na stres směřuje k zanedbání plánování a vtrhnout se „na věc“, což může mít katastrofální následky.

4.2 Politika managementu

Politika managementu má všepronikající vliv na aktivity jednotlivců na všech úrovních podniku.

4.2.1 Zájem managementu

Zájem managementu je dominantním faktorem ovlivňujícím bezpečný výkon práce. Musí se projevovat hmatatelně a nejen pouze obhajováním jako součástí vyjádření cílů podniku. Skutečný zájem je demonstrován řadou ukazatelů: linioví vedoucí v každém oddělení musí být odpovědní za bezpečnost. Bezpečnostní funkce v poradenské a auditové roli musí být zřetelnou podnikovou funkcí a ne v žádné jiné skupině, kde je její důležitost rozpuštěna. Otázky bezpečnosti by měly být pravidelně zahrnovány do rozhodování operací podniku a členové vrcholového managementu by měli pravidelněnavštěvovat pracoviště a udržovat denní kontakt s liniovými vedoucími a pracovníky. To zajišťuje, aby politiky deklarované vrcholovým vedením byly skutečně implementovány na operační úrovni. Jiná demonstrace zájmu managementu jsou zdroje vydávané na funkci bezpečnosti ve srovnání s výrobou.

Všeobecnou politiku bezpečnosti v organizaci je třeba proaktivně a trvale hodnotit. Je k dispozici několik systémů: (1) ISRS (International Safety Rating System) poskytuje rozsáhlý audit aktivit managementu na poli bezpečnosti. (2) Další evidenci zájmu o proaktivní budování bezpečnosti je používání extenzivního cvičení „what-if“ a simulací k určení slabých míst. Existence takových cvičení naznačuje aktivní zkoumání schopnosti bezpečnosti.

4.2.2 Nebezpečí kultury „knihy pravidel“

Mnohé podniky se domnívají, že systém pravidel bezpečnosti je neotřesitelný. Existence takové kultury „knihy pravidel“ předpokládá, že postup podle pravidel zaručí, že se nebudou stávat nehody. To je založeno na domněnce, že rigidní soubor pravidel pokryje všechny problémy, a že nikdy nebude zapotřebí, aby jedinci interpretovali tato pravidla na neočekávané situace. Každé pravidlo však občas potřebuje podobnou interpretaci a tato potřeba musí být uznána a zabudována do systému. Ačkoli pravidla a postupy jsou nezbytným a skutečně podstatným aspektem bezpečnosti, musí být pravidelně revidována a aktualizována ve světle zpětné vazby z operačních zkušeností.
Naneštěstí podobné zpětnovazebné smyčky se časem stávají méně efektivní a proto musí být pravidelně revidovány, nejlépe nějakou třetí nezávislou institucí.

4.2.3 Přehnané spolehání na metody technické bezpečnosti:

Aby bylo dosaženo vysoké úrovně bezpečnosti pro vysoce rizikový průmysl, bývají často používány prediktivní techniky hodnocení jako: CPQRA (chemical process quantitative risk analysis), FMECA (failure modes effect and criticality analysis) a další. Je však třeba je doplnit dvěma dalšími: 1) explicitní uznání, že lidské i technické chyby je třeba modelovat a hodnotit se zvláštním důrazem na „vyšší „ úrovně lidských funkcí jako jsou chyby v diagnóze a v rozhodování. Chyby tohoto typu mají podstatný vliv na bezpečnost rizikových systémů vzhledem k jejich schopnostem překonat technické ochrany. 2) Je též nutno uvědomovat si, že jakákoli prediktivní technická analýza systému je založena (obvykle implicitně) na předpokladech o tom, jak bude závod fungovat, jaký druh systému zajištění kvality bude fungovat atd. Tyto předpoklady se vztahují k lidským aspektům systému jak například je podnik řízen, a operační filosofii vzhledem k bezpečnosti proti finančnímu profitu. Jsou-li tyto předpoklady nesprávné (tj. mohlo dojít k změně v politice managementu), pak technická analýza nemusí již déle být platná. Proto je nezbytné explicitně stanovit předpoklady ve světle možných změn v politice a praxi podniku. Je zapotřebí též efektivního systému hlášení o incidentech, aby byly odhaleny zdroje rizik, které nejsou pokryty v analýze bezpečnosti.

4.2.4 Organizační učení

Bylo konstatováno, že „organizace, které se nemohou učit z minulosti, jsou odsouzeny opakovat své chyby v budoucnosti“. To znamená nejen vyvodit závěry ze specifických případů, ale též učit se identifikovat základní příčiny chyb a poučovat se ze skoronehod. Skoronehody bývají daleko četnější než skutečné nehody a poskytují včasné varování o základních problémech, které dříve nebo později povedou k nehodě. Existuje několik důvodů, proč se podniky nepoučí ze zkušeností. Zprávy o nehodách se téměř vždy soustřeďují na to, co se stalo, než na to, proč se to stalo. Tím vzniká malá možnost identifikovat vracející se základní příčiny, Toto lze pozorovat tam, kde existují efektivní systémy hlášení, ale není jim věnována pozornost ze strany managementu, anebo tam, kde sice jsou rozpoznány základní příčiny, ale je nesprávně kladen důraz na profit oproti nákladům na bezpečnost a pokračování výroby. Jinou četnou chybou je kultura obviňování, která brání jedincům sdělovat informace o skoronehodách.

5.3 Variabilita lidské činnosti v normálních a mimořádných situacích

Obecně platí, že jakékoli nedostatky v kvalitě PIFs mohou za mimořádných stavů maximalizovat negativní účinky na činnost, neboť lidé pracují pod tlakem, aby získali informa-

ce, interpretovali jejich implikace pro bezpečnost a správně rozhodovali co nejrychleji, než dojde k vážným důsledkům. Za stresu se objevují četné jevy, jako je rigidita řešení problémů a polarizace myšlení, které mohou změnit účinky PIFs, neboť činí pracovníka vulnerabilnějším k chybám. Je proto nezbytné porozumět tomu, jak se lidé chovají za podmínek velkého stresu, aby bylo možno zhodnotit roli každé PIF.
V mimořádných situacích se mohou objevit tyto obecné charakteristiky:

zvysoce riskantní prostředí,
- velký časový tlak,
- vysoká zátěž úkoly, složitost úkolů,
- nezvyklé podmínky procesu,
- velký hluk zaviněný poplachem,
- dlouhá pracovní doba k dokončení úkolu.

Míra v jaké určitá kombinace podobných „operačních environmentálních faktorů“ bude pracovníky vnímána jako stresová, závisí na zdrojích, jako je kvalita kontrolního panelu, postupů, výcviku, organizačních a sociálních faktorů a konečně i individuálních charakteristik pracovníků. Konfrontace těchto stresových faktorů se zdroji „coping“ ovlivňuje začátek stresu pracovníka. Situace nejsou stresové pouze tím, že je přítomna řada externích stresorů, nýbrž protože jsou jako takové vnímány pracovníkem.

Definice toho, co je to stresor, je též důležitá. Externí stresory vyvstávají z operačního prostředí. Nedostatky v designu kontrolního panelu, postupech, výcviku a problémy v oblasti týmové práce a managementu bezpečnosti též mohou vést ke stresu. Takové stresory mohou způsobovat konfliktní či víceznačné informace, přetížení pracovníka, konflikt mezi bezpečností a produkcí, nejasnosti v roli členů týmu a špatnou komunikaci. To může na oplátku negativně ovlivňovat lidskou spolehlivost. Kvalita těchto PIFs určuje, zda mají pozitivní nebo negativní účinky. Pracovníci jsou ve stresu tehdy, když pociťují, že jejich zdroje nedostačují k zvládání mimořádné situace.

Při studiích činnosti za stresu a vyskytujících se chybách byly použity tři přístupy.

(1) Laboratorní studie, které zkoumaly účinky pouze jednoho externího stresoru (např. hluku či horka) na relativně jednoduché úkoly, např. výběrovou reakci.
(2) Analýza skutečných nehod. Studie provedli například: Kletz [94], Reason a Mycielska [95]. Podobné analýzy závisí na úrovni podrobností poskytovaných ve zprávách o nehodách – tyto retrospektivní zprávy závisí na přesnosti paměti a též na „racionalizaci zpětného pohledu“.
(3) Použití simulátorů bývají doprovázeny potížemi pro vysokou nákladnost provádění podobných studií.

Kontogiannis a Lucas [96] uvádějí přehled těchto přístupů. Provedli klasifikaci kognitivních jevů, které se vyskytují za vysokého stresu. Klasifikaci uvádíme v Tabulce 4 (Příloha A). Klasifikace byla provedena po zkoumání řady nehod z různých průmyslových odvětví. Kognitivní jevy ilustrují praktickým způsobem psychologické mechanismy, které urychlují chyby za stresu. Mohou též vysvětlovat, proč role PIFs se liší za normálních a mimořádných situací v závislosti na souboru kognitivních jevů, které jsou do hry přivedeny. Protože tyto jevy jsou pro každého jedince jedinečné, lze zjistit větší rozdíly v lidských výkonech za mimořádných situací. Konečně: klasifikace kognitivních jevů je užitečná při zarovnání těch aspektů PIFs, které hrají větší roli v lidském výkonu za stresu. Například „seskupování informací“ a „přehled kritických parametrů“ jsou dva aspekty designu kontrolního panelu, který lze optimalizovat ke snížení pravděpodobnosti, že pracovník vyvine „kognitivní tunelové vidění“. S ohledem na design zařízení může též kontrola specifikace vstupních a výstupních podmínek podnítit pracovníka k tomu, aby uvažoval o alternativních hypotézách.

MODEL SYSTÉMOVĚ-TEORETICKÉHO MODELOVÁNÍ A PROCESŮ HAVÁRIÍ

V této kapitole o systémovém přístupu k haváriím uvedeme jeden z modelů havárií založený na teorií systému, který je známý pod označením STAMP - System Theory Accident Modeling and Processes (Systémově-teoretické modelování a procesy havárií). Tento model odráží koncept bezpečnosti, podle kterého k haváriím, resp. k událostem s těžkými ztrátami, dochází tehdy, když vnější poruchy, selhání komponent nebo dysfunkční interakce mezi podsystémy a komponentami systému nejsou adekvátně kontrolovány. Stručněřečeno, havárie jsou výsledkem nedostatečné kontroly, nebo dohledu nad bezpečnostními pravidly během vývoje, konstrukce a provozu systému.

Bezpečnost v systémovém pojetí je problémem kontroly a je řízena celou strukturou kontroly včleněnou do adaptivních socio-technických systémů. Cílem struktury kontroly bezpečnosti je kontrola dodržování bezpečnostních nařízení, opatření a pravidel během celého životního cyklu každého konkrétního socio-technického systému.

V tomto smyslu vyžaduje porozumění vzniku havárie, aby bylo určeno, proč byla struktura kontroly bezpečnosti neefektivní. Zabránění vzniku havárií v budoucnosti vyžaduje návrh struktury kontroly tak, aby byl zajištěn dohled nad plněním bezpečnostních omezení. Proto nejdůležitějším základním pojmem v přístupu STAMP není událost, ale omezení, kterými se jí mělo předejít.

Systémy jsou v přístupu STAMP chápány jako vzájemně provázané komponenty, které jsou udržovány ve stavu dynamické rovnováhy zajišťované zpětnovazebními regulačními obvody. Na systém není pohlíženo jako na statický výtvor, ale je chápán jako dynamický proces, který se kontinuálně přizpůsobuje tomu, aby plnil své cíle a reagoval na své vlastní změny a změny okolí. Původní projekt musí zajišťovat nejen splnění náležitých omezení chování systému z hlediska jeho bezpečného provozu, ale musí zaručovat, že tyto limity nebudou omezeny ani při změnách a jimi vyvolaných adaptačních procesech. Havárie se potom považují za důsledky trhlin (děr, nedostatků) procesů zahrnujících interakce mezi lidmi, společenskými a organizačními strukturami, inženýrstvím a komponentami systémů. Proces vedoucí k havárii může být popsán pomocí terminologie funkcí adaptabilních zpětných vazeb, které selhaly při zachování bezpečnosti, když došlo ke změnám chování systému během provozu.

Dovolíme si na tomto místě udělat krátkou poznámku k termínu adaptabilních zpětných vazeb. Jakýkoli model havárií, který zahrnuje sociální systém a selhání člověka, musí vysvětlovat adaptaci. Lze prohlásit, že opravdu konstantní je pouze tvrzení, že není nic, co by konstantní zůstávalo navždy. Systémy i organizace soustavně podléhají změnám tím, že se přizpůsobují lokálním tlakům a krátkodobým výrobním a nákladovým cílům. Lidé se přizpůsobují svému okolí (adaptují se, nebo se s ním asimilují), nebo mění své okolí tak, aby lépe sloužilo jejich úmyslům. Doprovodným znakem možnosti systémů a lidí přizpůsobovat se aktuálním trendům, je zvyšování pravděpodobnosti toho, že bezpečnostní ochrany budou časem systematicky degenerovat, obzvláště tehdy, když se tlaky na snižování nákladů a zvyšování produktivity stanou dominantními prvky rozhodování. Tehdy začnou redundance a jiná opatření pro zvýšení ochrany před chybami člověka degenerovat, protože se pracovní praktiky adaptují na zvyšování efektivnosti v daném pracovním prostředí. Podle

Rasmussena [57] není tato adaptace nahodilá, ale procesem optimalizačním, který je řízen vyhledávacími strategiemi a proto je predikovatelný a potenciálně kontrolovatelný.

Podobnému procesu “degenerace“ podléhají často i struktury kontroly bezpečnosti, což vysvětluje pozorování, že havárie v komplexních systémech často obsahují “migraci“ systému směrem ke stavu, kde už i malá odchylka (ať už ve fyzickém zařízení, nebo v chování operátora), může vést ke katastrofě. Tato migrace bývá často vyvolána normálním úsilím mnoha zaměstnanců vynakládaným v rámci jejich každodenní práce, odpovídající shora stanovenému požadavku na větší produktivitu a menší náklady. Takto jsou položeny základy pro budoucí havárii už mnoho let před jejím vznikem. K degradaci bezpečnostní rezervy dochází v systémech obvykle často bez toho, že bychom se pro to rozhodli. Je to jednoduše výsledek plynulého postupu přijímaných úprav/změn, které pomalu přivedly podnik směrem k situaci, kdy už i běžná chyba může vést k velké havárii.

Místo definování managementu bezpečnosti v termínech prevence chyb/selhání komponent, je v přístupu STAMP management bezpečnosti definován jako soustavná kontrola, jejímž úkolem je určovat nevyhnutelná omezení pro chování systému vůči bezpečnostním změnám a požadovaným adaptacím. Při používání přístupu STAMP můžeme havárie pochopit pomocí otázek typu: „Proč kontroly, které byly stanoveny, haváriím nezabránily, nebo aspoň nezjistily změny, které vedly k havárii?“, tj. pomocí identifikace bezpečnostních omezení, které byly porušeny a zjištěním, proč kontrola nebyla adekvátní potřebě dohledu nad bezpečnostními omezeními. Např. pochopení havárie v Bhópálu vyžaduje nejen jednoduché určení toho, proč údržbáři nezaslepili příslušné potrubí, ale hlavně to, proč kontroly, které byly nainstalovány v zařízení za účelem prevence úniku nebezpečných chemikálií a zmírnění následků takového případného úniku (snímače, měřící zařízení, havarijní signalizace, chladiče, apod.), nesplnily svůj účel.

V teorii systémů je kontrola vždy spojena s nařizováním omezení a požadavků. Namísto chápání havárií jako výsledku iniciační události v sérii událostí vedoucích ke zničení/škodě nebo úrazu, jsou havárie považovány za výsledek chybějících omezení, které nebyly zadány v konkrétním systému na každé příslušné úrovni (technické, manažerské, nebo dozorové). Bezpečnostní omezení specifikují ty vztahy mezi systémovými proměnnými, které vytvářejí bezpečné stavy systému. Příkladem takového bezpečnostního omezení na fyzikální úrovni je oznámení: „Před vstupem do této místnosti musí být vypnut proud“. Kontrolní procesy, které zajišťují splnění tohoto omezení, vymezují chování systému tak, aby udávané omezení nemohlo být porušeno.

Omezení (proti selháním) jsou obzvlášť užitečná při vysvětlování a prevenci havárií vyvolaných těmi chybami projektu (konstrukčními), které souvisí se softwarem a chováním operátorů. Proč vlastně hrají omezení/požadavky kladené na projektování složitých systémů, jejichž funkčnost je podstatně závislá na počítačích, takovou významnou roli? Počítač je úžasně výkonný a užitečný proto, že je nezávislý na fyzikálních omezeních elektromechanických zařízení. To je jeho předností i kletbou. Nancy Levesonová nazývá tuto skutečnost “kletbou flexibility“ [40]. Fyzikální zákony zajišťují základní sebekontrolu při projektování, konstrukci a modifikaci systémů a také kontrolují jejich komplexnost. U softwaru jsou limity toho, čeho je možné dosáhnout jiné, než limity toho, čeho je možné dosáhnout úspěšně a bezpečně. Limitující faktory se mění ze strukturální integrity a fyzikálních zákonitostí reálných materiálů a mechanismů na limity našich intelektových schopností. Je možné, dokonce lehké, vypracovat software, kterému nemůžeme rozumět tak, abychom mohli určit, jak se bude chovat za všech okolností, proto musíme konstatovat, že můžeme vytvořit software, který překračuje intelektové limity člověka. Výsledkem toho jsou havárie způsobené intelektovou neříditelností interaktivně komplexních a úzce vzájemně se ovlivňujících komponent a subsystémů, které dovolují nepozorovatelně vniknout potencionálně nebezpečným inter-

akcím mezi nimi během vývoje zařízení/systému. Řešení tohoto problému inženýry spočívá v zabezpečení stejné disciplinovanosti tvorby softwaru, jakou zajišťuje příroda svými zákonitostmi při konstrukci elektromechanických zařízení. Bezpečnost, tak jako každá jiná kvalita, musí být obsažena v projektu systému tak, aby obsahovala, nebo dohlížela na bezpečnostní omezení systému kontrolováním jeho komponent a jejich interakcí. Pokud plní úlohu kontroly bezpečnosti software, potom musí reprezentovat, ba přímo být projektem systému. Software, jemuž je svěřena kontrola bezpečnosti, přispívá k haváriím tím, že nezahrnuje některé požadavky na omezení chování, nebo tím, že přímo navede chování systému na porušení stanovených omezení.

STAMP poskytuje mnohem lepší popis toho, jak software způsobuje havárie, než popis modelů chyb a částečně vysvětluje, proč většina softwarem vyvolaných havárií pochází z chybných požadavků na objednávaný software a ne z chyb při programování. Primárním problémem bezpečnosti při počítači ovládaných systémech nejsou “chyby“ softwaru, ale nedostatek potřebných omezení na chování softwaru.

Softwarové vysvobození z předcházejících omezení kladených fyzikálními zákony má vliv i na výkon supervize a kontrolu automatizovaných systémů člověkem a na design interface mezi operátorem a řízeným procesem. Cook [12] tvrdí, že pokud kontrolu a řízení přednostně prováděla mechanická zařízení ovládaná lidmi z pracovišť v těsné blízkosti ovládaných strojů, bylo senzorické vnímání stavu zařízení a procesu možné cestou přímé fyzikální zpětné vazby, jakou byly např. vibrace, zvuk, nebo teplota. Sdělovače byly přímo spojeny s řízeným procesem a v podstatě tvořily jeho fyzikální prodloužení. Touto cestou zabezpečovaly bohatý zdroj informací o procesech a stavech strojů.

Nástup elektronických řídicích a informačních systémů umožnil řídit technologické procesy z mnohem větších vzdáleností (fyzických i mentálních), než čistě mechanické ovládače. Toto zvětšení vzdálenosti však zároveň znamená, že operátoři ztratili mnoho přímých informací o procesu a stavech zařízení tím, že už nemohou přímo pozorovat zařízení svými smysly. Návrháři systému proto musí syntetizovat a poskytnout operátorům mentální obraz o stavu procesu a zařízení. Významným novým zdrojem chyb projektu se stal požadavek pro projektanty určit předem, jaké informace bude operátor v rozličných situacích muset mít, aby mohl bezpečně ovládat technologický proces. Jestliže projektanti nepředvídali předem nějakou významnou situaci, ke které může dojít, pak ani nepředvídali, jaké informace bude operátor u ní potřebovat a nemohli je proto v projektu zabezpečit.

Projektanti taktéž musí zabezpečit zpětnou vazbu mezi zásahy operátorů a mezi jakoukoliv poruchou, ke které může dojít. Kontrola a řízení prováděné pomocí elektromechanických zařízení nebo softwarem, nemusí mít žádoucí efekt na proces a operátoři o tom nemusí vůbec vědět. Havárie mohou být odstartovány nesprávnou zpětnou vazbou. Takovou byla např. havárie v TMI, kde operátor dal povel k otevření armatury a zpětná vazba mu oznámila, že daná armatura je otevřená, i když ve skutečnosti tomu tak nebylo. V tomto případě, tak jako i některých dalších případech, zpětná vazba signalizovala jen to, že bylo aktivní napájení pohonu elektroarmatury, ale ne, že je skutečně otevřená. Elektronické řídící systémy uvolňují omezení na konstrukci systému tím, že dovolují větší funkčnost, ale zároveň i vytvářejí větší možnosti omylů, ať už projektantů nebo operátorů, které předtím neexistovaly, nebo byly mnohem méně pravděpodobné u čistě mechanických řídících systémů. Pozdější zavádění počítačů a digitálních řídících systémů přineslo další výhody a odstranilo mnohem víc omezení při projektování řídících systémů, čímž se však zvětšila možnost chyb/selhání.

To hlavní, co jsme chtěli tímto úvodním pohledem na otázky systémového přístupu k bezpečnosti říci, můžeme shrnout následovně: „Systémově-teoretický přístup k bez-

pečnosti, jakým je i STAMP, považuje bezpečnost za otázku kontroly. Havárie se stávají tehdy, když selže komponenta/zařízení, působí vnější poruchy a/nebo vzniknou disfunkční interakce mezi komponentami včetně funkcí managementu, které nejsou vhodně ošetřené. Místo, aby byly havárie považovány za výsledek iniciační události v sérii událostí vedoucích ke zničení/poškození zařízení, resp. k úrazu, jsou havárie chápány jako výsledek interakcí mezi komponentami, které porušují systémové bezpečnostní omezení. Pokud se efekty disfunkčních interakcí a nedostatečného dozoru bezpečnostních omezení přímo odrážejí v událostech, neadekvátní kontrola bezpečnostních omezení se v nich odráží jenom nepřímo, přesto, že je způsobuje. Úlohou systémových inženýrů, resp. inženýrů systémové bezpečnosti, je identifikovat všechna konstrukční a projektová omezení, která jsou nevyhnutelná pro trvalé udržování bezpečnosti systému a také zajistit, aby celý projekt systému včetně jeho sociálních a organizačních aspektů (a nejen fyzických), byl orientován na udržování jeho bezpečnosti.

6.1 Systémově-teoretické modelování a procesy havárií - STAMP

V předcházejících částech této studie jsme popsali systém jako hierarchickou strukturu, ve které každá úroveň ukládá určitá omezení aktivit/chování nižší úrovně, což znamená, že omezení, resp. jejich absence na vyšší úrovni dovolují kontrolovat chování na nižší hierarchické úrovni. Systémově-teoretický model havárií, místo dekompozice systému a příčin havárie na komponenty jeho struktury a tok událostí, popisuje systémy a havárie v termínech hierarchických úrovní kontroly založené na zpětnovazbovém mechanismu. Výklad modelu takové hierarchické kontroly v přístupu STAMP je uveden v následující části.

Model kontroly bezpečnosti v socio-technických systémech v rámci STAMP

Socio-technické systémy můžeme modelovat jako hierarchické úrovně organizace s kontrolními procesy probíhajícími ve styku mezi úrovněmi za účelem kontroly aktivit na nižších úrovních. Na každé úrovni může být neadekvátní kontrola způsobena buď chybějícími omezeními, nebo omezeními nedostatečně komunikovanými, resp. omezeními, na které se náležitě nedohlédlo na nižší úrovni a taktéž neadekvátně zabezpečenými funkcemi zpětné vazby o plnění/dodržování omezení na nižší úrovni při zajišťování bezpečnosti.

Ideu modelování socio-technických systémů pomocí teorie systémů využili pro rozbory havárií už Rasmussen [57]. Pro přístup STAMP byl vybudován model kontroly, který vychází z vyšších úrovní modelu vypracovaného Rasmussenem a přidává k nim strukturu kontroly pro vývoj/projektování systému.

Struktura kontroly pokračuje směrem dolů od koncepce až na úroveň technické realizace systému.

Generický model kontroly bezpečnosti v přístupu STAMP má dvě základní hierarchické struktury kontroly, jednu pro vývoj systému a druhou pro jeho provoz, které jsou vzájemně interaktivně provázané. Tak je postaven proto, protože například výrobce letadel má pod svoji bezprostřední kontrolou jen systém vývoje a výroby letadla, bezpečnost však zahrnuje stejně vývoj jako i provoz letadla a nemůže být úspěšně završena ani v jedné z těchto částí izolovaně. Používání systému je částečně závislé na své konstrukci a výrobě a částečně na efektivní kontrole během samotného provozu. Výrobce musí svým zákazníkům/provozovatelům přesně oznámit předpoklady o podmínkách provozu, pro které byly bezpečnostní analýzy provedeny a poskytnout jim bezpečné provozní předpisy a procedury. Provoz systému naopak poskytuje zpětnou vazbu výrobci o chování systému během jeho životního cyklu.

Mezi hierarchickými úrovněmi každé kontrolní struktury jsou potřebné komunikační kanály směrem dolů pro přenos příkazů od kompetentních (pravomocných) složek pro ukládání omezení na nižší úroveň a zpětnovazební kanály směrem nahoru pro přenos výsledků měření účinnosti splnění uložených omezení na nižší úrovni. Zpětná vazba je rozhodující v každém otevřeném systému ve smyslu zabezpečení adaptabilní kontroly.

Vláda, vrcholové orgány průmyslových odvětví a soudnictví jsou vrcholovými úrovněmi každé části systému kontroly generického modelu pro STAMP. Vládní struktura kontroly nad vývojem a výrobou se může lišit od struktury pro provoz. Náležitá omezení pro každou strukturu kontroly a pro každou hierarchickou úroveň se mohou lišit, ale všeobecně se skládají z projekčních a metodických omezení, z požadavků na management, z omezení pro výrobní procesy a z provozních omezení.

Na nejvyšší úrovni hierarchie obou částí modelu kontroly bezpečnosti pro STAMP je parlament a státní zákonodárství. Parlament kontroluje bezpečnost přijímáním zákonů a zřizováním úřadů struktury státní regulace. Zpětná vazba o úspěšnosti této kontroly, nebo o potřebě dalších kontrolních mechanismů je podávána ve formě zpráv pro vládu, podkladů pro jednání parlamentních výborů, lobbystickými skupinami i závěry samotných havárií.

Následující úroveň zahrnuje vládní agentury pro regulaci, průmyslová a zákaznická sdružení, odborové svazy, pojišťovací společnosti a soudy. Omezení generovaná na této hierarchické úrovni a zasílaná obchodním společnostem a podnikatelským firmám jsou obvykle formulována jako politiky, regulace, certifikáty, standardy/normy a trestní sankce (pokuty). Pokud je v dané oblasti ustanoven odborový svaz, může i on vydávat svoje požadavky na bezpečnost při výrobě a provozu a na kolektivní vyjednávání.

Management společnosti přijímá standardy/normy, regulační opatření a jiné všeobecné kontrolní omezení pro podniky a přenáší je do formulování specifických podnikových politik a standardů. Mnohé společnosti mají definovanou všeobecnou politiku bezpečnosti (což je požadováno zákonem ve Velké Británii) a také i detailní standardy. Zpětnou vazbu dostávají ve formě zpráv o výrobě, o stavu provozních zařízení, o odhadech rizik a hlášení o poruchách. Model STAMP je představen v Obraze 2 (Příloha B).

Ve struktuře kontroly bezpečnosti ve výrobních a vývojových podnicích (viz Obraz 2, Příloha B) určuje management vlastní politiku bezpečnosti pro podnik a vybírá, resp. upravuje, adekvátně standardy/normativy pro svoje produkty. Vyšší úroveň kontrolního procesu zajišťuje jen všeobecné cíle a omezení a každá nižší úroveň k nim může přidávat detaily ve smyslu akceschopnosti stanovených všeobecných cílů a omezení, které vytvářejí bezprostřední lokální podmínky a cíle bezpečnosti.

Postup je tedy takový, že pokud vládní nebo podnikové standardy vyžadují provedení analýzy nebezpečí, musí mít konstruktéři a tvůrci dokumentace (provozních předpisů a uživatelských manuálů) pod kontrolou analýzy konkrétních nebezpečí, pomocí nichž stanoví specifická omezení pro konstrukci a provoz vyvíjeného systému. Navržená omezení, která jsou považována za nevyhnutelná pro kontrolu možných nebezpečí souvisejících s určením vyvíjeného systému, jsou postoupeny odborným útvarům (implementers and assurers) zodpovědným za technické řešení, které zabezpečí, že identifikovaná nebezpečí budou v systému pod kontrolou ve smyslustanovených/požadovaných omezení. Úspěšnost (správnost) navržených technických řešení se potvrzuje testovacími protokoly, revizními zprávami a případně dalšími analýzami nebezpečí. Na konci vývojového procesu jsou výsledky analýz nebezpečí a dokumentace bezpečnostně významných vlastností projektu pro jejich kontrolu včetně potřebných zdůvodnění použitého řešení odevzdány útvaru/odborníkům pro údržbářský servis produktu, aby byly použity při zajišťování plnění účelu (poslání) systému a k jeho dalšímu potřebnému vývoji.

Podobný proces mezi hierarchickými úrovněmi kontroly probíhá i v části modelu pro strukturu kontroly bezpečnosti provozu. Navíc jsou mezi těmito dvěma kontrolními strukturami vzájemné interakce dané nutností přenosu bezpečnostních omezení přijatých při projektovaní systému do provozních postupů a procedur a potřebou získávání poznatků o funkčnosti systému, jeho selháních, potřebných úpravách a změnách.

Rasmussen upozorňuje, že vlastní kontrola na každé úrovni má být prováděna podle přesně stanovených nařízení a instrukcí, nebo může být určen volněji, pouze cíli, aniž je jednoznačně stanoveno, jak jich má být dosaženo. Současné trendy od managementu formou dozoru (dohledu) a příkazů k managementu formou porozumění podstaty věci (chápání) se odrážejí diferencováním úrovní zpětnovazební kontroly, které jsou nad nižšími úrovněmi a změnou od managementu předepisování kontroly k managementu určování cílů tak, aby tyto byly na každé hierarchické úrovni interpretovány a plněny v souladu s lokálními podmínkami. Pokusy delegovat pravomoc rozhodovat a řídit prostřednictvím cílů, vyžaduje explicitní formulaci hodnotových kritérií pro vykonávané činnosti a efektivní prostředky komunikace respektovaných hodnot směrem dolů v organizacích i v celé společnosti. Dopad specifických rozhodnutí na každé úrovni na cíle a hodnoty přenášené na nižší úroveň, musí být náležitě a formálně vyhodnocen.

Jak v každém řídícím obvodu, tak i v zpětnovazební kontrole bezpečnosti, může mít dopravní zpoždění toku nařízení a informací o účinnosti jejich splnění vážný vliv na efektivnost této kontroly. Například příprava norem může trvat několik let, což je doba, kdy už mohou výrazně zaostávat za aktuálním stavem technologie a praxe. Na fyzické úrovni systémů mohou být komponenty nové technologie použity v rozličných částech a v rozdílném rozsahu (tzv. asynchronní evoluce řídící struktury). To byl případ sestřelení vrtulníku armády USA vlastními stíhačkami v severním Iráku v r. 1994, když pilot stíhačky používal rádio, se kterým se nemohl spojit se starším typem rádia ve vrtulníku.

Všeobecně jedinou cestou, jak se vypořádat s dopravními zpožděními v řídících obvodech, je přenést odpovědnost na nižší úrovně, kde je eliminováno zpoždění při získávání informací, nebo zpětnovazebních údajů z měřících kanálů. V obdobích rychle se měnících technologií dopravní zpoždění nevyhnutelně vyžaduje, aby shora přicházející omezení byla modifikována na nižších úrovních tak, aby odpovídala konkrétní situaci. Překonání zpětnovazebního zpoždění si na nejnižších úrovních může vyžádat předběžný typ kontroly pro nastolení kontroly nad probíhající činností.

Musíme ještě připomenout, že kontrolní struktury bezpečnosti socio-technických systémů se na všech hierarchických úrovních setkávají se stresujícími faktory, jakými jsou rychle se měnící technologie, konkurence, boj o trh, změny postoje veřejnosti a dozorových orgánů k bezpečnosti a jiné, které byly popsány v první kapitole této studie. Tyto tlaky mohou vyvolat potřebu nových procedur, nebo kontrolních mechanismů na to, aby se zjistilo, že požadovaná bezpečnostní omezení nejsou přehlížena.

6.2 Modely pro řízení procesů

Kromě ukládání omezení a hierarchických úrovní kontroly bezpečnosti obsahuje přístup STAMP ještě třetí základní prvek, kterým jsou modely pro řízení procesů. Všeobecně platí, že každý regulátor, ať už je to člověk, nebo automat, nevyhnutelně potřebuje model systému, nebo procesu, který řídí, aby ho mohl řídit efektivně. Prvním extrémem takovýchto modelů jsou ty, které obsahují pouze jednu nebo dvě proměnné, jako je to např. v modelu jednoduchého termostatu, ve kterém se využívá pouze okamžitá teplota a žádaná hodnota teploty. Druhým extrémem jsou komplexní modely s velkým počtem snímaných proměnných

a nastavených hodnot, které jsou potřebné pro řízení složitých systémů, jako např. letecký provoz, nebo jaderné elektrárny.

Nezávisle na tom, zda je model pro řízení systému zabudován do logiky automatického regulátoru, nebo zda je mentálním modelem operátora, musí zpracovávat stejné informace: požadované vztahy mezi systémovými proměnnými, údaje o okamžitém stavu systému provozu, limitní nastavení a způsoby, jakými je možné měnit stavy zařízení a změny procesů. Řídící modely se využívají pro určování potřebných řídících zásahů a manipulací a aktualizují se pomocí různých forem zpětné vazby. Je důležité mít na zřeteli, že model řízeného procesu je vyžadovaný na každé úrovni hierarchické struktury kontroly a ne pouze na nejnižší technické úrovni.

V dnešních složitých technologiích bývají regulátory řídících obvodů nejčastěji mnohonásobnou kombinací lidí-operátorů a automatických regulátorů. Počítače, které jsou běžnou komponentou regulačních a řídících obvodů, se mohou nacházet na více místech v celé struktuře obvodu. Mohou působit například jako inteligentní podpora rozhodování pro operátora bez přímého přepojení na ovládací jednotku zařízení. I v takovémto případě musí software počítače modelovat řízený proces, protože ho řídí nepřímo, ba dokonce přesnost/validnost modelování může být pro celý řídící obvod kritická. Citlivým místem regulátorů kombinovaných z operátorů a automatických regulátorů je rozhraní člověka a zařízení tvořené oznamovači informací, displejů, havarijních hlášení, neboť je prostředkem synchronizace mentálního modelu operátora a modelu automatického regulátora a jakýkoliv nedostatek v této synchronizaci může vést k systémovým haváriím.

Havárie, obzvlášť systémové, jsou často důsledkem nesrovnalostí mezi modely operátora a automatického regulátoru a aktuálním stavem řízeného procesu. Dále mohou systémové havárie vést k neadekvátní koordinaci mezi několika regulátory a operátory, včetně neočekávaných postranních efektů přijatých rozhodnutí/zásahů, nebo konfliktní řídící zásahy. Obzvlášť kritická při koordinaci je nesprávná komunikace.

Dodáváme, že modely řídících procesů jsou stejně důležité i pro fázi vývoje a výroby systémů. Projektanti při své práci musí používat model samotného vyvíjeného systému a také i modely procesů vlastního projektování.

6.3 Klasifikace faktorů havárií pomocí STAMP

Po uvedení tří principiálních prvků modelu STAMP (omezení, hierarchická struktura kontroly a modely procesů) můžeme odvodit klasifikaci faktorů havárií pro tuto metodiku. V přístupu STAMP jsou havárie definovány v termínech porušení bezpečnostních omezení, které mohou být způsobeny selháním/poruchou prvku v systému, vlivy okolí a disfunkčními interakcemi mezi prvky (ať už funkčními nebo poškozenými). V každém řídícím obvodu, na každé hierarchické úrovni socio-technické struktury kontroly pro danou část systému, vyplývá nebezpečné chování buďz nepřítomnosti, nebo neadekvátnosti omezení na proces na nižší úrovní, nebo neadekvátního uplatňování/předsazování omezení.

Protože každý prvek řídícího obvodu kontrolní struktury může přispívat k neadekvátnímu prosazování bezpečnostních omezení, začneme odvozovat klasifikaci faktorů havárií prozkoumáním každé komponenty všeobecného řídícího okruhu kontrolní struktury a ohodnocením jejího potenciálního příspěvku. V řídícím okruhu může regulátor, resp. kompetentní orgán, provést neadekvátní, nebo nesprávný řídící zásah včetně chybného zpracování poruch nebo odchylek, nebo kontrolní zásah může být nesprávně proveden ovládacími mechanismy obvodu. Tyto všeobecné faktory platí na každé úrovni socio-technické struktury

kontroly, jen jejich interpretace se budou lišit v závislosti na hierarchické úrovni.

V Tabulce 5 (Příloha A) je uvedena klasifikace nedostatků kontroly bezpečnosti, které vedou k systémovým nebezpečím a haváriím.

Pro každý z těchto faktorů, všude tam, kde do kontrolní činnosti vstupuje člověk, nebo organizace, je nevyhnutelné, aby bylo hodnocení jeho příspěvku provedeno v kontextu s tím, jak bylo dáno rozhodnutí pro provedený zásah přijato a s uvážením všeho, co mohlo přijaté rozhodnutí ovlivnit, protože bez toho nebude možné pochopit, jak a proč došlo k nebezpečnému rozhodnutí.

Připomínáme, že havárie způsobené chybami/selháním prvků systému jsou v probírané klasifikaci také zahrnuty. Mohou být způsobeny nesprávnými omezeními ve výrobě, neadekvátním inženýringem (neexistující, nebo nekorektně implementovanou odolností techniky vůči chybám), nesouladem mezi kapacitou jednotlivých prvků včetně člověka a provozními/pracovními požadavky, nezvládnutými poruchami okolí, nedostatečnou údržbou, stárnutím a degradací v čase.

Prevence chyb komponent může být prováděna zvyšováním integrity systému, nebo zvyšováním odolnosti prvků vůči vnitřním a vnějším vlivům, nebo zabudováním bezpečnostní rezervy nebo bezpečnostních faktorů. Také se jim dá vyhnout provozní kontrolou, periodickými inspekcemi a preventivní údržbou, jakož i kontrolami během výroby. Účinky selhání komponent na chování systému mohou být eliminovány, nebo redukovány pomocí vhodných redundancí. Model STAMP překračuje jednoduché svalování viny za havárie na selhání komponent a požaduje, aby byly identifikovány příčiny, kterými se prokáže, proč k danému selhání došlo a proč tím došlo k havárii.

Neadekvátní prosazování bezpečnostních omezení

Neadekvátní kontrola prosazování/uplatňování bezpečnostních omezení může vzniknout buď proto, že nebezpečí a s nimi související omezení nebyly identifikovány (bod 1.1 Tabulky 5), nebo proto, že samotné kontrolní činnosti neadekvátně prosazují stanovená omezení (bod 1.2 Tabulky 5). Neadekvátnost kontrolních činností může být výsledkem chybného algoritmu (stanoveného způsobu) kontroly (bod 1.2.1 Tabulky 5), nekonzistentních nebo nekorektních modelů řídících procesů použitých pro algoritmus kontroly (bod 1.2.2 Tabulky 5), neadekvátní koordinací mezi několikanásobnými regulátory nebo orgány/jednotlivci, kteří přijímají rozhodnutí (bod 1.2.3 Tabulky 5) a neadekvátní nebo neexistující zpětnou vazbou (bod 1.2.4 Tabulky 5).

Neadekvátní kontrolní algoritmy

Kontrolní algoritmy nemusejí být účinné při prosazování bezpečnostních omezení (bod 1.2.1 Tabulky 5) tehdy, když jsou od začátku nesprávně navržené, když se v důsledku změny řízeného procesu stane algoritmus kontroly neadekvátním, nevhodnou změnou samotného algoritmu (např. zásahem údržbáře), nebo různými typy přirozené adaptace člověka, pokud jsou algoritmy kontroly realizované lidmi. V této studii jsme již několikrát poukázali na změny typu asynchronního vývoje, které vedly k mnoha haváriím. Staly se tehdy, když změny některých podsystémů byly pečlivě připraveny, ale jejich účinky na ostatní části systémů, včetně aspektů kontroly bezpečnosti, nebyly dostatečně uvážené. Příčinou asynchronní evoluce může být i poškození (opotřebování) některé z části systému.

Kritickým prvkem při vyhodnocování kontrolních algoritmů je komunikace a to na straně monitorování změn, ke kterým může dojít, jako i jejich oznamování na vyšší hierarchické

úrovni kontroly. Např. proces bezpečnostní analýzy, jehož výsledkem jsou bezpečnostní omezení, vždy zahrnuje určité základní předpoklady o podmínkách provozu (pracovního prostředí). Když se tyto podmínky (prostředí) změní tak, že původní předpoklady už dále neplatí, může to způsobit, že místní kontrola bezpečnosti bude neadekvátní.

Nekonzistentní modely procesů

Výše jsme zdůvodnili to, že efektivní kontrola je založena na validním modelu řízeného procesu. Havárie, obzvlášť systémové havárie, jsou nejčastěji způsobeny nekonzistencí mezi modely, které používá regulátor, resp. kontrolní orgán, při řízení a skutečným stavem procesu (bod 1.2.2 Tabulky 5). Když model regulátoru procesu (ať už mentální model operátora, nebo naprogramovaný model automatu) diverguje od skutečných stavů procesu, potom povel k provedení nesprávného řídícího zásahu odvozeného z této nesrovnalosti může vést k havárii.

Důležité jsou i mentální mapy vývojových pracovníků a konstruktérů. Např. při vývoji softwaru nemusí mentální mapa programátorů o požadovaném fungování systému kopírovat mentální mapy inženýrů (co se dnes běžně nazývá jako chybně stanovené požadavky na software) nebo software může být implantován na jiný počítač, než na který byl původně určen, nebo použit při testování vyvíjeného softwaru, případně mohly nastat změny v řídícím systému. Situace se může stát daleko komplikovanější, když se na regulaci/kontrole podílí více regulátorů, protože každý z nich musí mít konzistentní modely a tyto modely musí být konzistentně společné.

Nejčastější formou nekonzistence je neúplnost modelů provozních procesů, která spočívá v tom, že tyto nepokrývají všechny možné stavy procesů, nebo možné poruchy včetně nezvládnutí, nebo nekorektního zvládnutí poruch komponent. Samozřejmě, že žádné modely nejsou kompletní v absolutním slova smyslu, cílem však je udělat je dostatečně kompletními na to, aby bezpečnostní omezení nemohla být porušovaná při jejich používání.

Termín „kompletní“ zde není myšlen v matematickém slova smyslu, ale více ve významu, že v daném modelu neexistují neurčitosti z hlediska jeho předpokládané aplikace. Specifikace jsou nekompletní, jestliže fungování systému, nebo softwaru není dostatečně přesně určeno, protože požadované fungování při určitých událostech, nebo podmínkách bylo přehlédnuto, nebo je určeno jen volně, tj. připouští více než jednu interpretaci.

Jestliže nejsou rozdíly ve výsledcích dvou programů splňujících stejné požadavky významné pro určitou podmnožinu specifikovaných požadavků, nebo omezení, které se vztahují na bezpečnost, pak neurčitosti, nebo neúplnost (nekompletnost) jsou bezpředmětné přinejmenším pro danou podmnožinu a můžeme říct, že specifikace jsou dostatečně kompletní. Požadované specifikace jsou dostatečně kompletní tehdy, když specifikují bezpečné fungování za všech okolností, ve kterých má být systém provozován. Je jen samozřejmé, že pokud mohou být požadovány specifikace dostatečné pro určitý systém, nemusí dostačovat pro jiné systémy.

Souhrnem můžeme konstatovat, že modely procesů mohou být nekorektní hned od začátku, nebo se mohou stát nekorektními v důsledku neexistující, nebo chybné zpětné vazby, nepřesným měřením resp. vlivem neuvažovaného dopravního opoždění v řídících obvodech.

Neadekvátní koordinace mezi regulátory a tvůrci rozhodnutí

V situacích, kdy se na regulaci/kontrole podílí současně více regulátorů (lidí nebo automatů), mohou být jednotlivé řídící zásahy neadekvátně koordinovány (bod 1.2.3 Ta-

bulky 5) v důsledku neočekávaných postranních efektů přijatých rozhodnutí, nebo zásahů, případně konfliktních kontrolních činností. Velmi důležitou roli přitom sehrávají chyby komunikace. Leplat zdůvodňuje, že havárie jsou mnohem pravděpodobnější tam, kde se oblasti regulace/kontroly procesu, resp. procesů jednotlivými regulátory, překrývají, případně mají společné hraniční oblasti návazností, resp. kompetenčního dosahu [38]. V těchto případech existuje vysoký potenciál pro neurčitosti a konflikty mezi nezávislými rozhodnutími. Navíc, odpovědnosti za regulační/kontrolní funkce v hraničních oblastech jsou často nedostatečně definovány. Oblasti překrývání existují tam, kde je regulační/kontrolní funkce plněna kooperací dvou regulátorů, nebo kde dva regulátory působí na stejný stav procesu. Takové překrytí vytváří potenciál pro konfliktní řídicí zásahy (dysfunkční interakce mezi činnostmi regulátorů). Leplat se odvolává na studii z ocelářského průmyslu, ve které se uvádí, že 67 % technických poruch s materiálními škodami se stalo právě v oblastech součinnosti, přičemž tyto představují jen malý podíl na všech prováděných činnostech. Zajímavým případem havárie způsobené “překrytím“, je havárie letadla A320 v Bangáloru (Indie). Během přistání kapitán vypnul svůj automatický letový navigátor a předpokládal, že to udělá i druhý pilot, protože je to doporučená procedura přistávání. Tím by rychlost přistávání byla automaticky regulována. Druhý pilot však kapitánem očekávané vypnutí neudělal, tím se mód automatické kontroly rychlosti nenastavil a naopak už v poměrně nízké výšce se nastavil mód otevřeného klesání, což bylo příčinným faktorem pro pád letadla nedaleko přistávací dráhy.

Neadekvátní, nebo chybějící zpětná vazba

Čtvrtým nedostatkem, který vede k systémovým haváriím je neadekvátní, nebo nepřítomná zpětná vazba (bod 1.2.4 Tabulky 5). Základním principem teorie systémů je fakt, že žádný řídící systém (regulační nebo ochranný) nemůže být lepší než jeho měřící kanály. Vyvstává proto důležitá otázka, zda regulátory, nebo ti, kteří přijímají rozhodnutí, mají potřebné informace o aktuálním stavu kontrolovaného procesu pro dosažení svých cílů. Potřebné informace o aktuálním stavu řízeného procesu musí být soustavně dodávány používaným modelům, jinak v opačném případě se haváriím vyhnout nedá. Zpětná vazba může chybět, nebo může být neadekvátní, protože buď jednoduše nebyla v projektu systému zahrnuta, nebo existují nedostatky v monitorování, zpětnovazebních komunikačních kanálech, v časovém nesouladu (dopravní zpoždění), případně nepřesnosti měřících přístrojů.

Neadekvátní výkon kontrolních činností

Druhou cestou k tomu, aby bezpečnostní omezení mohla být porušena, je existence chyb a nedostatků v kompetenčních kanálech kontrolní struktury shora dolů, tj. v přenosech příkazů a nařízení, nebo při jejich provádění, tj. chyby a selhání ovládačů, nebo jejich prvků. I tady platí, že tyto chyby/selhání mohou být způsobeny nejen provozem těchto zařízení, ale už při jejich vývoji a výrobě.

6.4 Analýza havárií přístupem STAMP

Analýza havárie použitím přístupu STAMP začíná určením struktury kontroly bezpečnosti v daném socio-technickém systému. Havarijní proces je popsán na každé zúčastněné hierarchické úrovni kontrolní struktury v termínech bezpečnostních omezení, která byla porušena a se stanovením, proč byla porušena. Získáme tím více pohledů na havárii v závislosti na perspektivě a úrovni, ze které se na ni díváme.

Prvním krokem je identifikace nebezpečí zahrnutých do analyzované havárie. V dalším kroku se sestrojí hierarchická struktura kontroly bezpečnosti před identifikovanými hrozbami (nebezpečími) a určí se nevyhnutelná omezení pro kontrolu identifikovaných nebezpečí v každé hierarchické úrovni. Následně se postupně identifikují všechna selhání a disfunkční interakce v technologickém procesu a zařízeních, která se vyskytla v jednotlivých událostech tak, jak následovala v časové posloupnosti od bezprostřední havarijní události. Pro každé omezení se určí, proč bylo porušeno – buď proto, že nebylo nikdy stanoveno a kontrolou zabezpečeno jeho prosazování, anebo proto, že způsob prosazování byl neadekvátní. Přitom lze využít Tabulky 5.

Porozumění jakémukoli rozhodnutí přijatému lidmi vyžaduje (přinejmenším) znát informace, které byly k dispozici, i ty, které byly nutné, ale těm, kteří se rozhodovali, nebyly tehdy k dispozici. Dále je nutno znát mechanismy tvarující (ovlivňující chování při rozhodování se ve smyslu kontextu a tlaků na účastníky procesu rozhodování, hodnotové struktury, ze kterých přijaté rozhodnutí vychází a všechny nedostatky mentálních modelů účastníků procesu rozhodování.

Všeobecný popis úloh každé komponenty ve struktuře kontroly bezpečnosti bude obsahovat následující:

- Bezpečnostní požadavky a omezení,
- Kontroly,
- Kontext: Role a odpovědnosti Faktory tvarující chování a okolí,
- Nedostatky v kontrolovaném procesu,
- Dysfunkční interakce, selhání, chybná rozhodnutí a kontrolní činnosti,
- Důvody pro chybné kontrolní činnosti a dysfunkční interakce:
- Nedostatky algoritmu kontroly
- Chyby procesu, rozhraní, nebo mentálních modelů
- Neadekvátní koordinace mezi spolupůsobícími vícerými regulátory
- Nedostatky kompetenčního kanálu
- Nedostatky zpětné vazby.

Jedním z vážných problémů využití přístupu STAMP pro analýzy předcházejících havárií na základě informací, které jsou dostupné v existujících zprávách a hlášeních, je, že většina informací, která jsou nutná pro zkompletování modelu určité havárie pro STAMP, obvykle nejsou v existujících dokumentech obsažena. Je to proto, že většina zpráv a hlášení o haváriích je psána z perspektivy událostmi orientovaných přístupů. Události jsou v nich většinou vždy jasně popsány a zpravidla jedna nebo více z nich je vybrána jako kořenová příčina, přestože nebylo kompletně zanalyzováno, proč se tyto události staly. Navíc, analýzy se většinou zastaví v tom momentu, kdy se objeví někdo, na koho je možné svalit vinu za havárii. Většinou to jsou operátoři, nebo pracovníci údržby. Příležitost získat důležitá poučení pro zlepšení systémů je tím ale ztracena.

6.5 Management a kultura bezpečnosti

Kultura bezpečnosti byla vždy kritickou částí pro dosažení cílů bezpečnosti. Její skutečný význam byl v současnosti podtržen až zprávou vyšetřovací komise pro havárii raketoplánu Columbia. Je v ní doslova uvedeno: „Nárazy úlomků pěny nebyly ani tak jedinou příčinou havárie raketoplánu Columbia, jako jí nebylo poškození těsnících O-kroužků při havárii raketoplánu Challenger. Columbia i Challenger byly zničeny i kvůli chybám v organizaci NASA“.

Očividně nejdůležitějším zjištěním v této zprávě byl nátlak na NASA, aby i proti analýzám bezprostředních poruch dala přednost politickým rozhodnutím a rozpočtovým omezením, které ovlivnily celou strukturu, kulturu i systém bezpečnosti programu raketoplánů, což bylo v konečném důsledku příčinou chybného rozhodnutí.

Co je kultura bezpečnosti? Kultura je množina společně uznávaných norem a hodnot, způsob vidění a interpretace světa a událostí kolem nás (naše mentální mapa) a naše činnosti prováděné v sociálním kontextu. Kultura bezpečnosti je součástí (podmnožinou) kultury, která odráží naše všeobecné postoje a přístupy k bezpečnosti a managementu rizika. Kultura může být organizačně rozdělena do tří rovin: (1) povrchová úroveň představující kulturní artefakty (běžné věci denní potřeby); (2) střední úroveň zahrnující stanovená organizační pravidla, normy, hodnoty a praxi; a (3) často neviditelná, ale určující základová úroveň hlubokých návyků, které ovlivňují naše chování a rozhodování. Je jasné, že změnit kulturu je velmi těžké, protože to vyžaduje změnu všech třech vyjmenovaných úrovní a obtížnost změny na každé další úrovni se progresivně stupňuje.

Management, zdroje, možnosti a kultura jsou vzájemně propleteny a pokus změnit kulturu bez změny prostředí, ve kterém je používána, je dopředu odsouzen k neúspěchu. Také jednoduchá změna organizační struktury (včetně politiky, cílů, poslání, popisu pracovních míst a procedur vztahujících se k bezpečnosti) může krátkodobě snížit riziko, ale povrchní ustanovení, které nezasahují do množiny společných hodnot a sociálních norem s velkou pravděpodobností přestanou být po určitém čase prováděny. Příkladem toho jsou změny a opatření nařízené v NASA po havárii Challengeru, které po čase zdegradovaly až do bodu, kdy stejné tlaky a nerealistická očekávání, které způsobily zničení Challengeru, přispěly i ke zničení Columbie. Dosažení trvalého zlepšení výsledků vyžaduje provést změny v širokém rozsahu, které zabezpečí ochranu před přetrvávajícími vlivy prostředí a tlaky vyvolávajícími postupnou degradaci kultury bezpečnosti v čase a správné reakce na ně.

Společnou trhlinou kultury bezpečnosti nalezenou při vyšetřování velkých havárií je „kultura popření“, pro kterou je charakteristické nerealistické odhadování rizika, a kde prokazatelná rizika a varování jsou přehlížená bez náležitého prozkoumání. Taková kultura popření je obvyklá tam, kde předpoklady, za kterých probíhá provoz, nekorespondují s deklarovanou politikou organizace. Dát praktickou (inženýrskou) podobu kultuře bezpečnosti, nebo jinými slovy, dát do souladu provozní praktiky a hodnoty se stanovenými bezpečnostními hodnotami, vyžaduje v první řadě identifikaci požadovaných organizačních principů a hodnot bezpečnosti a potom nastolení a řízení organizační infrastruktury pro dosažení požadovaných hodnot a jejich dlouhodobé udržování. Pouze hesla a slogany nestačí. Všechny aspekty kultury, které mají vliv na bezpečnost, musí dostat praktickou podobu (inženýring), aby byly v souladu s organizačními principy bezpečnosti. Úspěšné dosažení tohoto souladu vyžaduje pochopení, proč se provozní praktiky v organizaci odklánějí od stanovených principů namísto vytváření vhodných nastavení a zavádění ochran proti budoucím nesouladům.

Nejdůležitější aspekty silné kultury bezpečnosti v sociálních systémech jsou:

- Formální organizační struktura zahrnující bezpečnostní útvary/skupiny a formálně určené bezpečnostní úkoly a zodpovědnosti výkonných pracovníků, manažérů, inženýrů, odborových vedoucích a ostatních. Tato struktura obvykle nebývá statická, spíše je dynamická s konstantně se vyvíjející množinou formálních vztahů.
- Organizační podsystémy, které ovlivňují kulturu bezpečnosti a management rizika, včetně otevřených a mnohosměrných komunikačních systémů, informační systém bezpečnosti pro podporu plánování analýz a procesů rozhodování, systémy odměn, systémy pro výběr a udržování znalostí, dovedností a schopností souvisejících s bezpečností, systémy pro zpracování poučení a zpětnou vazbu z poruch a provozních anomálií a jiných provozních zkušeností, kanály a procedury pro vyjádření obav o bezpečnost a řešení konfliktů.

• Neformální organizační struktury a procesy sociální interakce zahrnující vedení, vyjednávání, řešení problémů, rozhodování se a kolegialitu. Zde máme na mysli především vedení a rozhodování o otázkách bezpečnosti na každé organizační úrovni. Řešení problémů po událostech a provozních anomáliích je důležitou složkou kultury bezpečnosti, obzvlášť jestliže se vztahuje na identifikování a odstraňování kořenových příčin a nehledá pouze běžné příznaky hlubších problémů.

• Individuální schopnost a motivace zahrnující vědomosti, dovednosti, návyky a postoje, skupinová dynamika a více psychologických faktorů, zejména obavy ze vzniku bezpečnostních problémů, učení se z chyb bez obviňování, konání ve prospěch bezpečnostních hodnot apod.

• Bezpečnostní pravidla a procedury včetně hodnot a předpokladů, na kterých je postavena a jasně definována vize systémové bezpečnosti. Vize bezpečnosti musí být rozšířena mezi všemi členy organizace a ne pouze proklamována vedoucími. Často se totiž stává, že mezi vizí bezpečnosti, kterou hlásají vedoucí a vizí rozšířenou mezi řadovými zaměstnanci jsou velké rozdíly.

ZÁVĚR

V první části této studie je popsán změněný postoj veřejnosti k vnímání rizik z provozu moderních technologických zařízení. Rozhodující mírou tuto změnu zapříčinily katastrofální průmyslové havárie z konce minulého století svými dopady, ale i zjištěnými příčinami a mechanismy jejich vzniku. Technická zařízení se stávala vždy většími celistvými komplexy díky novým konstrukčním materiálům a řídící technice. Nástup digitálních řídících technologií vymanil vzájemné ovlivňování a interakce mezi komponenty/částmi zařízení ze zajetí mechanických přenosů a umožnil dosažení tehdy nepředstavitelných konstrukčních a provozních možností. Najednou bylo možné stavět automatické linky na velkovýrobu jakéhokoliv zboží, včetně toxických či explozivních nebezpečných výrobků, létat s velkokapacitními letadly a plavit se na obrovských tankerech. Bohužel, i navzdory veškeré důmyslnosti, s jakou byla tato pozoruhodná technická díla zkonstruována, se mnohá z nich nevyhnula haváriím, jejichž důsledky byly svou hrůzou úměrné velikosti a složitosti těchto děl.

Rozbory přibývajících havárií výrobních a technických komplexů brzy ukázaly, že na rozdíl od předcházejících havárií v průmyslu nebyly vyvolány jednoduchým selháním individuální části/komponent zařízení, ale latentními interakcemi mezi nimi ukrytými ve složitosti celého zařízení, které vedly k procesům s nežádoucími účinky a nebyly eliminovány/redukovány bezpečnostními omezeními. Vždy se ukázalo, že přijatá bezpečnostní opatření byla buď nedostatečná anebo selhala kontrola jejich zavedení a dodržování. Typické příznaky těchto havárií si vynutily specifický přístup, který se začal rozvíjet krátce po 2. světové válce. Jeho teoretickým základem je teorie systémů a předmětné havárie se v ní chápou jako systémové havárie.

V předložené studii jsou popsány hlavní příznaky, kterými se systémové havárie ohlašují. Téměř nikdy k nim nepatřily očividně nebezpečné činy či konstrukční chyby. Většinou to bývá řetězec běžných zanedbání, nedůsledností a ústupků, kterými se továrna, resp. produkt nějakého projektu, dostane do stavu, ve kterém už sebemenší další malá neopatrnost může iniciovat vážnou systémovou havárii. Mnohé z těchto příznaků jsou ve studii ilustrovány na příkladech ze skutečných událostí.

K teoretickým základům systémových havárií důležitých pro porozumění procesů jejich vzniku a rozvoje patří pojem kauzalita. Ve studii je uveden model trojúrovňové hierarchické struktury příčinnosti havárií, jehož autorem je Lewycky. Samostatná část je ve studii

věnována vysvětlení hlavních pojmů všeobecné teorie systémů používaných při rozborech a modelování systémových havárií. Klíčový význam pro systémové havárie má chápání bezpečnosti složitých systémů jako emergentní vlastnosti jejich hierarchické struktury. Celá teorie systémových havárií je vypracovaná na třech pilířích, kterými jsou

(1) nevyhnutelná bezpečnostní omezení ve všech stádiích životního cyklu produktu,

(2) hierarchická struktura úrovní kontroly stanovení a dodržování nevyhnutelných bezpečnostních omezení a

(3) modely řízení provozních resp. produkčních procesů, ať už jsou to matematicko-logické modely automatických regulátorů a ochran, anebo mentální (konceptuální) modely operátorů, konstruktérů a jiných. Pro hlubší porozumění teorie systémových havárií je ve studii popsaný reprezentační přístup k modelování a studiu procesů systémových havárií známý pod zkratkou STAMP, jehož autorkou je přední odbornice na systémové havárie Nancy C. Levesonová.

V závěrečné části této studie jsou popsány tři významné havárie v jaderných zařízeních ve Windscale, na Three Mile Island (TMI) a v Černobylu a jsou uvedeny poznatky ze systémových analýz mechanizmů a příčin jejich vzniku. Ty poukazují na to, že havárie těchto zařízení mají povahu systémových havárií a jejich bezpečnost musí být proto zajišťována ve smyslu emergentní vlastnosti jaderných zařízení jako složitých systémů. Nevyhnutelnost přistupovat k bezpečnosti těchto děl ze strany systémových havárií i v České republice jednoznačně potvrzuje neoddiskutovatelný fakt enormního vzrůstu složitosti (ve všech třech aspektech: bezpečnostních omezeních, hierarchické struktury kontroly a v obou dvou typech modelů řízení) jaderné elektrárny v Temelíně (ETE) vůči blokům jaderné elektrárny v Dukovanech (EDU).

Máme za to, že obsah předkládané studie poskytne užitečné úvodní informace a motivace odborníkům z oblasti lidského faktoru pro vstup do teorie systémových havárií a její aplikaci v naší jaderné energetice.

(Footnotes)

[1] hnutí ve Velké Británii začátkem 19. století, které bylo namířeno proti zavádění strojů do výroby, neboť ty byly považovány za původce nezaměstnanosti.

LITERATURA

(1) Ackoff, Russell L. Towards a system of systems concepts. Management Science, 17(11): 661-671, July 1971.

(2) Adams, E.E. Accident causation and the management system. Professional Safety. October 1976.

(3) Adato, Michelle; KacKenzie, James; Pollard Robert and Weiss Ellyn Safety Second: The NRC and American`s Nuclear Power Plants. Indiana University Press, Bloomington, Ind., 1987.

(4) Ahearne, John F. Nuclear power after Chernobyl. Science, 236: 673-679, May 8, 1987.

(5) Ayres, Robert U. and Rohatgi Pradeep K. Bhopal: Lessons for technological decision-makers. Technology in Society, 9: 19-45, 1987.

(6) Barrett, Richard S. The human equation in operating a nuclear power plant. In David a.L. SiHs, C.P. Wolf, and Vivien B. Shelanski, editors, Accident at Three Mile Island: The Human Dimensions, pages 161-171, Westview Press, Boulder, Colo.,1982.

(7) Boebert, Earl Personal communication.

(8) Bogard, William The Bhopal Tragedy. Westview Press, Boulder, Colo., 1989.

(9) Bond, Pete Heroes in Space. Basil Blackwell Ltd., New York. 1987.

(10) Brown, Michael L. Personal communication from comments on an early version of this manuscript.

(11) Calder, J. Scientific accident prevention. American Labor Legislative Review, I: 14-24, January 1911.

(12) Cook, Richard I. Verite, Abstraction, and Ordinateur Systems in the Evolution of Complex Process Control. 3rd Annual Symposium on Human Intemction with Complex Systems (HICS '96), Dayton Ohio, August 1996.

(13) Farmer, F.R. Quantification, experience, and judgement. In B. H. Harvey. European Major Hazards, pages 51-59, Oyez Scientific and Technical services, Ltd., London, 1984.

(14) Fischhoff, Baruch; Hohenemser, Christoph; Kasperson, Roger and Kates, Robert: Handling hazards. In Jack Dowie and Paul Lefrere, editors, Risk and Chance, pages 161-179, Open University Press, Milton Keynes, United Kingdom, 1980.

(15) Wilde, G.J.S. Evidence Refuting the Theory of Risk Homeostasis? A Rejoinder to Frank P. McKenna. Ergonomics 25: 879-890, 1984.

(16) Kirwan, B. Guide to Practical Human Reliability Assessment. London: Taylor and Francis, 1994.

(17) Frola, F. Ronald and Miller C.O. System safety in aircraft acquisition. Technical report, Logistics Management Institute, Washington, D. C., January 1984.

(18) Gloss, David S. and Wardle, Miriam Gayle Introduction to Safety Engineering. JohnWiley & Sons, New York, 1984.

(19) Griffiths, Richard F., editor: Dealing with Risk: The Planning, Management and Acceptability of Technological Risk. Manchester University Press, Manchester, United Kingdom, 1981.

(20) Haddon, William, Jr. The prevention of accidents. In Duncan W. Clark and Brian

MacMahon, editors, Preventive Medicine, page 595, Little, Brown, and company, Boston, 1967.

(21) Hammer Willie Handbook of System and Product Safety. Prentice-Hall, Inc., Englewood Cliffs, N.1. 1972.

(22) Hammer, Willie Product Safety Management and Engineering. Prentice-Hall, Inc., Englewood Cliffs, NJ. 1980.

(23) Hansen, C.M. Universal Safety Standards. Universal Safety Standards Publishing Company, New York, 1914.

(24) Harriss, R.C.; Hohenemser, C. and Kates, R.W. The burden of technological hazards. In G. T. Goodman and W. D. Rowe, editors, Energy Risk Management, pages 103-138, Academic Press, New York, 1979.

(25) Heinrich, H.W. Industrial Accident Prevention: A Scientific Approach. McGraw-Hill, New York, 1931.

(26) Hornick, Richard J. Dreams-Design and destiny. Human Factors, 29(1): 1] 1-121, 1987.

(27) Checkland, Peter Systems Thinking, Systems Practice. John Wiley & Sons, New York, 1981.

(28) Childs, Charles W. Cosmetic system safety. Hazard Prevention, May/June 1979.

(29) Chisti, Agnees Dateline Bhopal. Concept Publishing Company, New Delhi, India, 1986.

(30) Chris, Johnson The Detection, Reduction and Mitigation of Failure in Safety-Critical Systems, 2000.

(31) Johnson, William G. MORT Safety Assurance Systems. Marcel Dekker, Inc., New York, 1980.

(32) Kemeny, John G. Report of the President's Commission on Three Mile Island (The Need for Change: The Legacy ofTM/). U.S. Government Accounting Office, Washington, D.C., 1979.

(33) Kjellen, Urban A changing role of human actors in accident control-Implications for new technology systems. In Jens Rasmussen. Keith Duncan, and Jacques Leplat, editors. New Technology and Human Error. pages 169-175. John Wiley & Sons, New York. 1987.

(34) Kletz, Trevor My ths of the Chemical Industry. The Institution of Chemical Engineers. Rugby. Warwickshire, United Kingdom, 1984.

(35) Kletz, Trevor Wise after the event. Control and Instrumentation. 20(10): 57-59. October 1988.

(36) Komp, Emory Calamities of technology. Science Digest, pages 50-59, July 1986.

(37) Lagadec, P. States of Emergency. Butterworth-Heinemann, London, 1990.

(38) Leplat, Jacques Occupational accident research and systems approach. In Jens Rasmussen, Keith Duncan, and Jacques Leplat, editors, New Technology and Human Error, pages 181-191, John Wiley & Sons, New York, 1987.

(39) Lerner, Eric Automating U.S. air lanes: A review. IEEE Spectrum, pages 46-51, November 1982.

(40) Leveson, Nancy G. A New Approach To System Safety Engineering, Aeronautics and

Astronautics Massachusetts Institute of Technology, June 2002.

(41) Leveson, Nancy G. SAFEWARE, System Safety and Computers, University of Washington, 1995

(42) Lewycky, Peter Notes toward an understanding of accident causes. Hazard Prevention, pages 6-8, March/April 1987.

(43) Lombardo, Thomas G. TMI: An insider's viewpoint. IEEE Spectrum, pages 52-55, May 1980.

(44) Machol, Robert E. The Titanic coincidence. Interfaces, 5(5): 53-54, May 1975.

(45) Martin, Mike W. and Schinzinger, Roland Ethics in Engineering. McGraw-Hill Book Company, New York, 1989.

(46) Megaw, James How Safe?: Three Mile Island, Chernobyl, and Beyond. Stoddard Publishing Company, Toronto, Ontario, 1987.

(47) Mill, John Stuart A system of logic, ratiocinative, and inductive: Being a connected view of the principle of evidence, and methods of scientific inquiry. J. W. Parker, London, 1943.

(48) Miller, C.O. A comparison of military and civil approaches to aviation system safety. Hazard Prevention, pages 29-34, May/June 1985.

(49) Miller, C.O. The broader lesson from the Challenger. Hazard Prevention, pages 5-7, January/February 1987.

(50) Mostert, Noel Supership. Alfred A. Knopf, New York, 1974.

(51) Neumann, Peter G. Computer-Related Risks. ACM Press, 1994.

(52) Perrow, Charles Normal Accidents: Living with High-Risk Technology. Basie Books, Inc., New York, 1984.

(53) Perrow, Charles The habit of courting disaster. The Nation, pages 346-356, October 1986.

(54) Ned, Franklin The accident at Chemobyl. The Chemical Engineer, pages 17-22, November 1986.

(55) Incident and the Friendly Fire Death of Lt. Laura Piper. Brasseys Inc., 2001.

(56) Ramo, Simon The systems approach. In Ralph M. Miles, Jr., editor, Systems Concepts: Lectures on Contemporary Approaches to Systems, pages 13-32. John F. Wiley & Sons, New York, 1973.

(57) Rasmussen, Jens Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, vol. 27, No. 2j3, Elsevier Science Ltd., 1997, pp. 183-213.

(58) Rogers, William P. Introduction to System Safety Engineering. John Wiley & Sons, New York, 1971.

(59) Rogers, William P. Report of the Presidential Commission on the Space Shuttle Challenger Accident. U .S. Government Accounting Office, Washington, D.C., 1986.

(60) Ruckelshaus, William D. Risk in a free society. Risk Analysis, 4(3): 157-162, 1984.

(61) Ruckelshaus, William D. Risk, science, and democracy. In Theodore S. Glickman and Michael Gough, editors, Readings in Risk, pages 105-118, Resources for the Future, New York, 1990.

(62) Sarter, Nadine and Woods, David How in the world did I ever get into that mode?: Mode error and awareness in supervisory control. Human Factors, Vol. 37, No. 1, November 1995, pp. 5-19.

(63) Schlein, Edgar Organizatianal Culture and Leadership. 2nd Edition, Sage Publications, 1986.

(64) Muhlouse,Alsace-Lorraine Collection of Applicances and Apparatus for the Prevention of Accidents in Factories. Society for the Prevention of Accidents in Factories, 1895.

(65) Stieglitz, William I. Engineering for safety. Aeronautical Engineering Review, February 1948.

(66) Ferry, Ted S. Safety Program Administration for Engineers and Manager. Charles C. Thomas Publisher, Springfield, III, 1984.

(67) U.S.S.R. State Committee on the Utilization of Atomic Energy. The accident at the Chernobyl nuclear power plant and its consequences. Report presented at the AIEA Experts Meeting, Vienna, Austria, August 25-29, 1986.

(68) Verne, L. Roberts Defensive design.Mechanical Engineering, pages 88-93, September 1984.

(69) Vesely, W.E.; Goldberg, F.F., Roberts, N.H. and Haasl, D.P. Fault tree handbook.

(70) Weil, Vivien Case Browns Ferry. In Curd Martin and May Larry Professional Responsibility for Harmful Actions, pages 402-411, Kendall Hunt, Dubuque, Iowa, 1984.

(71) Weinberg, Gerald An Introduction to General Systems Thinking. John Wiley & Sons, New York, 1975.

(72) Wolf, C.P. Some lessons learned. In David L. Sills, C.P. Wolf, and Vivien B. Shelanski, editors, Accident at Three Mile Island: The Human Dimensions, pages 215-232, Westview Press, Boulder, Colo., 1982.

(73) Zebroski, Edwin L. Sources of common cause failures in decision making involved in man-made catastrophes. In James J. Bonin and Donald E. Stevenson, editors, Risk Assessment in Setting National Priorities, pages 443-454, Plenum Press, New York, 1989.

(74) Enhancing Mission Success - A Framework for the Future, A Report by the NASA Chief Engineer and the NASA Integrated Action Team, December 21, 2000.

(75) Military Standard System Safety Program Requirements, MIL-STD-882C, 19 January 1993.

(76) Kirwan, B. An overview of a nuclear reprocessing plant Human Factors programme. Applied Ergonomics, 34: 441-452. 2003

(77) Swain, A.D.; Guttmann, H.E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278. Washington, D.C.: US Nuclear Regulatory Commission. 1983.

(78) Reason, J.: Human Error. Cambridge: Cambridge University Press. 1990.

(79) Rasmussen, J. Skills, rules, knowledge: Signals, signs, symbols and other distinctions in human performance models. IEEE Transactions on Systems, Man, and Cybernetics 13, 257-267,1983.

(80) Endsley, M.R. Situation Awareness and Human Error: Designing to Support Human Performance. Proceedings of the High Consequence Surety Performance, Albuquerque, NM. 1999.

(81) Rasmussen, J. Information Processing and Human-Machine Interaction. Amsterdam: North Holland. 1986.

(82) Guidelines for Preventing Human Error in Process Safety. New York: American Institute of Chemical Engineers. Center for Chemical Process Safety.1994.

(83) Poulton, E. Continous Noise Interferes with Work by Masking Auditory Feedback and Inner Speech. Applied Ergonomics, 7: 79-84, 1976.

(84) Bartlett, F.C. Fatigue following Highly Skilled Work. Proceedings of the Roayl Society (Series B), 131: 247-257, 1943.

(85) Moran, J.B.; Ronk, R.M. Personal Protective Equipment. In G.Salvendy (Ed.), Handbook of Human Factors, New York: Wiley. 1987.

(86) Salvendy G.: Handbook of Human Factors. New York: Wiley. 1987.

(87) Astley, J.; Shepperd, A.; Whitfield, F. A Review of UK and International Knowledge and Practice int the Selecion of Process Control Operators. In E. Lovesey (Ed.) Ergonomics Setting Standards for the 90's Contemporary Ergonomics. London: Francis and Taylor. 1990.

(88) Shaw, K.S.; Sichel, H.S. Accident Proneness. Oxford: Pergamon. 1971.

(89) Verhaegen, P.; Strubbe, J.; Vonck, R.; van der Abeele, J. Absenteeism, Accidents and Risk-Taking. Journal of Occupational Accidents 7: 177-186, 1985.

(90) Roger, D.; Nesshoever, W. The Construction and Preliminary Validation of a Scale for Measuring Emotional Control. Personality and Individual Difference 8: 527-534, 1987.

(91) Friedman, M.; Rosenman, R. „Type A" Behavior and Your Heart. New York: Knopf. 1974.

(92) Murell K. F. H.: Ergonomics: Man in His Working Environment. London: Chapman and Hall. 1965.

(93) Griew, S.; Tucker, W.A. The Identification of Job Activities Associated with Age Differences in the Enginerign Industry. Journal of Applied Psychology 42: 278, 1958.

(94) Kletz, T.A. What went wrong? Case Histories of Process Plant Disasters (3rd ed.), Houston: Gulf Publishing Co. 1994.

(95) Reason, J.; Mycielska, K. Absent Minded? The Psychology of Mental Lapses and Everyday Errors. Englewood Cliffs NJ: Prentice Hall. 1982.

(96) Kontogiannis, T.; Lucas D. Operator Performance Under High Stress: An Evaluation of Cognitive Modes, Case Studies and Countermeasures. Human Reliability Associates, Lancashire UK: Dalton and Wigan. 1990.

(97) Chapanis, A. et al. Applied Experimental Psychology: Human Factors in Engineering Design. New York: Wiley. 1949.

(98) Endsley, M.R. Evaluation of Situation Awareness in Flight Operations Employing Synthetic Vision Systems. Prepared for NASA Langley Research Center. 2000.

(99) Embrey, D.E. Approaches to aiding and training operatprs' diagnoses in abnormal situations. Chemistry and Industry 7: 454-459, 1986.

(100) Gertman, D.I.; Haney, L.N.; Jenkins, J.; Blackman, H.S. Operator Decision Making Under Stress. In G.Johansen, G.Mancini and L. Maftensson (Eds.) Analysis Design and Evaluation of Man-Machine Systems (Proceedings of the 2nd IFAC/IFIP/IFORS Conference, Varese, Italy. 1985.

(101) Kahn, R.I.; Wolfe, D.M.; Quinn, R.P.; Snoek, J.D.; Rosenthal, R.A. Organizational Stress: Studies in Role Conflict and Ambiguity. New York: Wiley. 1964.

(102) Technical Report NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D. C., 1981.

PŘÍLOHA A -TABULKY Tabulka 1 - GEMS (Reason 1990)[1]

Úroveň činnosti	Faktory přispívající k chybám
Založené na dovednosti	1. Nedávnost a četnost používání (Recency and frequency of previous use)
	2. Kontrolní signály prostředí (Environmental control signals)
	3. Sdílené vlastnosti schématu
	(Shared schema properties)
	4. Konkurující plány (Concurrent plans)
Založené na pravidle	1. Postoj „Vždy to takto fungovalo“ (Mind-set „It’s always worked before“)
	2. Příhodnost „Preferuje se to, co první přijde pod ruku“ (Availability „The first to come is preferred“)
	3. Zkreslené srovnání „Podobné se vztahuje k podobnému“ (Matching bias „Like relates to like“)
	4. Přílišné zjednodušení, například haló efekt (Oversimplification (e.g. halo effect)
	5. Přehnaná sebedůvěra „Jsem si jistý, že mám pravdu“ (Overconfidence („I’m sure I’m right“)
Založené na znalosti	1.Výběrovost (omezená racionalita) (Selectivity - bounded rationality)
	2. Přetížení pracovní paměti (omezená racionalita) (Working-memory overload)
	3. Sejde z očí, sejde z mysli (Out of sight, out of mind)
	4. Tématické tuláctví a zapouzdření (Thematic vagabonding and encysting)
	5. Vzpomínání / myšlení podle analogie (Memory prompting / reasoning by analogy)
	6. Obnovené zkreslení při srovnávání (Matching bias revisited)
	7. Neúplný či nesprávný mentální model (Incomplete / incorrect mental model)

Tabulka 2 - Taxonomie chyb při SA – údaje z rozboru selhání v letecké dopravě (Endsley 1999)[2]

ÚROVEŇ 1 Selhání správně vnímat informace – 76,3 %

Data nejsou po ruce – 13 %

a) Špatný design systému
b) Selhání komunikace
c) Neprovedení nějakého nutného úkonu (například resetovat výškoměr)

Data jsou, ale jsou obtížně detekovatelná či diskriminovatelná – 11,1 %
Například špatné označení ranveje, nedostatečné osvětlení, překážky výhledu, problémy spojené s hlukem v kokpitu

Data jsou k dispozici, avšak dochází k selhání monitorovat či pozorovat úda je – 35,1 % (největší podíl chyb)

a) Přehlédnutí – nepodívá se na údaje
b) Zúžení pozornosti a vnější rušení, které brání operátorovi vnímat důležité informace – 22,9 %
c) Vysoká zátěž úkolem - i když momentální – brání ve vnímání informací

Informace je vnímána, ale chybně (chybná percepce údajů) – 8,7 %a)
Vliv očekávání (například vidí nebo slyší něco, co očekává)

b) Neporozumění informacím v důsledku rušení jiným úkolem

Výpadek paměti – 8,4 %

Operátor nejdříve určitou informaci vnímá, ale pro mnoho dalších na ni zapomene. Zapomínání bylo nejčastěji spojeno s narušením normální rutiny, vysoké pracovní zátěže a vyrušování.

ÚROVEŇ 2 Selhání správně informace integrovat nebo jim rozumět – 20,3 %

- Chybějící či špatný mentální model – 6,9 %

  Informace je správně vnímána, ale její význam není pochopen. Chybí mentální model, pomocí něhož lze spojit informaci s danými důležitými úkoly. Většinou byly chyby tohoto druhu spojeny s automatizovaným systémem.

- Použití nesprávného mentálního modelu k interpretaci informací – 6,5 %

  Vede k nesprávné diagnóze či porozumění situaci v oblastech, kde je odlišný systém. Častým problémem je to, že lidé mají neadekvátní model toho, co je očekáváno a poté interpretují všechna vnímaná vodítka do tohoto modelu, což vede k úplně nesprávné interpretaci situace.

- Přehnaný spoleh na původní (deafault) hodnoty v mentálním modelu – 6,5 %

  Jde o obecná očekávání toho, jak fungují části systému – tato očekávaná data mohou být použita místo skutečných. Spoleh na habituální očekávání jak se bude systém chovat a ne využití skutečných dat, i když jsou k dispozici.

Jiné - 2,3 %

Například operátor jednoduše neporozumí významu vnímaných informací a jejich vztahu k operačním cílům, anebo několik informací není správně integrováno. To může být způsobeno omezením pracovní paměti anebo některými dalšími neznámými kognitivními chybami.

ÚROVEŇ 3

Nepředvídání budoucích akcí nebo stavu systému – 3,4 %

Jednotlivci si sice uvědomují to, co se děje, ale nejsou schopni správně předvídat to, co to znamená pro budoucnost. Je to zaviněno:

- Chybějícím či špatným mentálním modelem – 0,4 %
- Přehnanou projekcí současného trendu – 1,1 %
- Jiným

Důvod pro nesprávné předvídání je málo zřejmý. Mentální projekce situace do budoucna je velmi náročný úkol, v němž lidé bývají obecně nedostateční.

OBECNĚ

Špatné udržení více cílů v paměti – to může ovlivňovat uvědomování si situace na všech úrovních

Habituální schéma – lidé se mohou dostat do pasti habituálního schématu, provádět úkoly automaticky, což je činí méně vnímavé vůči důležitým vodítkům prostředí.

Tabulka 3 - Klasifikační struktura výkon ovlivňujících faktorů(Center for Chemical Process Safety 1994)[3]

1. Operační prostředí

1.1 Prostředí pracovního procesu

1.1.1 Četnost nasazení lidí

1.1.2 Složitost událostí v procesu

1.1.3 Vnímaná nebezpečí

1.1.4 Závislost na čase

1.1.5 Náhlost vzniku událostí

1.2 Fyzické pracovní prostředí

1.2.1 Hluk

1.2.2 Osvětlení

1.2.3 Teplotní podmínky

1.2.4 Atmosférické podmínky

1.3 Rozvrh práce

1.3.1 Pracovní doba a přestávky na oddech

1.3.2 Rotace směn a noční práce

2. Charakteristika úkolů

2.1 Design prostředků

2.1.1 Umístění / přístup

2.1.2 Označení

2.1.3 Osobní ochranné prostředky

2.2 Design kontrolních panelů

2.2.1 Obsah a relevance informací

2.2.2 Identifikace sdělovačů a ovládačů

2.2.3 Kompatibilita s očekáváním uživatelů

2.2.4 Seskupování informací

2.2.5 Přehledné uspořádání kritických informací a poplachových upozornění

2.3 Pracovní pomůcky a postupy

2.3.1 Kritéria pro výběr pracovních pomůcek

2.3.2 Jasnost instrukcí

2.3.3 Úroveň popisu

2.3.4 Kvalita kontrol a varování

2.3.5 Podpora při diagnostice chyb

2.3.6 Kompatibilita s operačními zkušenostmi

2.3.7 Frekvence aktualizace

2.4 Výcvik

2.4.1 Konflikt mezi požadavky bezpečnosti a produkce

2.4.2 Výcvik v používání nového zařízení

2.4.3 Praxe ve zvládání nezvyklých situací

2.4.4 Výcvik v používání havarijních postupů

2.4.5 Výcvik v práci s automatizovanými systémy

2.4.6 Vývoj výcvikového programu

3 Charakteristiky operátora

3.1 Zkušenosti

3.1.1 Úroveň dovedností

3.1.2 Zkušenosti se stresovými událostmi procesu

3.2 Osobní faktory

3.2.1 Motivace

3.2.2 Riskantní jednání

3.2.3 Teorie homeostázy rizika

3.2.4 Lokus kontroly

3.2.5 Emoční kontrola

3.2.6 Osobnosti typu A resp. B

3.3 Tělesný stav a věk

4 Organizační a sociální faktory

4.1Týmová práce a komunikace

4.1.1 Rozdělení pracovní zátěže

4.1.2 Jasnost odpovědností

4.1.3 Komunikace

4.1.4 Autorita a vedení

4.1.5 Skupinové plánování a orientace

4.2 Politika managementu

4.2.1 Zájem managementu

4.2.2 Nebezpečí kultury “Knihy pravidel“

4.2.3 Přehnané spoléhání na prvky technické bezpečnosti

4.2.4 Organizační učení

Tabulka 4 - Individuální a kognitivní jevy za stresu (Kontogiannis a Lucas 2000)[4]

Jev	Charakteristika
Kognitivní vyhnutí se (Cognitive avoidance)	Může mít řadu forem. Např. člověk je selektivněnepozorný na ohrožující známky a vyhýbá se myšlení o nebezpečí pomocí aktivit, které odvádějí pozornost. Jiná forma: svalení odpovědnosti (passing the buck) – spoleh na jiného, že rozhodne.
Zesílení konformity ve skupině (Reinforced group conformity)	Tendence skupiny chránit souhlas tlakem na nesouhlasící členy a filtrováním vnějších informací, které mohu narušit jednotu skupiny.
Zvýšené rizikové chování (Increased risk taking)	Jednotlivci tendují chovat se riskantněji ve skupiněnež o samotě. Byla navržena různá vysvětlení, zejména iluse, že kontrolovaný systém je nezranitelný, dále rozložení odpovědnosti za jakýkoli možný problém, přítomnost přesvědčivých osob, které zastávají rizikovou pozici a zvýšená familiarizace problému v diskusích.
Zabývání se minulostí (Dwelling in the past)	Skupina za stresu tenduje koncentrovat se na vysvětlování faktů, které byly již překonány pozdějšími událostmi
Tendence k přílišné kontrole situace (Tendency to overcontrol the situation)	Lidé tendují k přílišné kontrole situace, než aby delegovali odpovědnost
Strategie „uvidíme“ (Adopt a „wait and see“ strategy)	Jak se důsledky krize stávají kritičtější, lidé se více zdráhají přijmout bezprostřední rozhodnutí a čekají na redundantní informace
Dočasná mentální paralýza (Temporary mental paralysis)	Krátkodobá neschopnost využít informací, které jsou k dispozici Je to pravděpodobně zaviněno náhlým přepojením nízké stimulace na vysokou za doby krize.
Snížení rozsahu pozornosti (Reduced concentration span)	Soustředění, tj. schopnost napřít pozornost na požadavky, se za stresu snižuje
Kognitivní „tunelové vidění“ (Cognitive „tunnel vision“)	To je známo jako „zakotvení hypotéz (hypothesis anchoring), pracovník se snaží hledat informace, které potvrzují jeho původní hypotézu o stavu procesu a k zanedbávání informace, které ji nepotvrzují

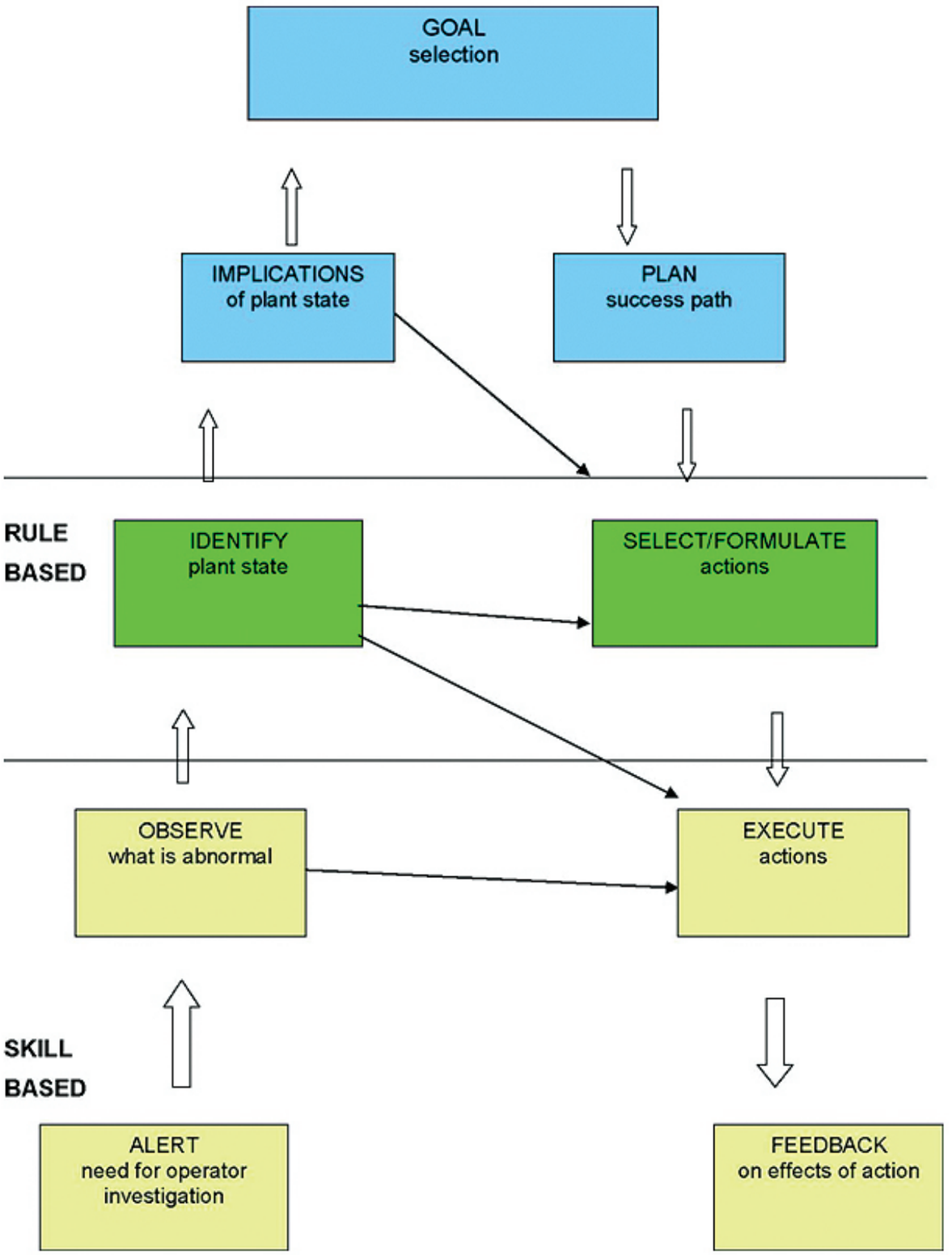
Rigidita řešení problému (Rigidity of problem-solving)	Tendence používat nevyhovující řešení, která nejsou nejúčinnější
Polarizace myšlení (Polarization of thinking)	Tendence vysvětlovat problém jednou globální příčinou než kombinací příčin
Zapouzdření a tématické tuláctví (Encystment and thematic vagabonding)	Tematické tuláctví se týká případů, v nichž člověkovy myšlenky těkají z věci na druhou, s každou z nich zachází povrchně. Zapouzdření nastává tehdy, když se témata nabubřují a člověk se zabývá detaily, zatímco důležité věci jsou ignorovány
Stereotypní kontrola (Stereotype takeover)	Ústup k habituálnímu či předpogramovanému způsobu chování v minulosti v podobné situaci, která se však v určitém ohledu liší
Hypervigilance	Panika vede k narušení myšlení. Člověk nepoznává možné alternativy a zavírá se na urychlený přístup, který se zdá, že nabízí bezprostřední řešení.

Tabulka 5 - Klasifikace nedostatků kontroly bezpečnosti vedoucí k systémovým nebezpečím

1. Neadekvátní prosazování bezpečnostních omezení kontrolou
1.1 Neidentifikování nebezpečí
1.2 Nedostatečné, neefektivní nebo neprovedené kontrolní činnosti pro identifikovaná nebezpečí
1.2.1 Navržený algoritmus procesu kontroly neprosazuje nebezpečí • nedostatky při vytváření procesu kontroly • změny procesu bez odpovídajících změn v algoritmu (asynchronní vývoj) • nekorektní úpravy/přizpůsobení
1.2.2 Modely procesu jsou nekonzistentní, neúplné a nekorektní (chybí připojení) nedostatky v procesu jejich tvorby •nedostatky v procesu jejich aktualizace
1.2.3 Neadekvátní koordinace mezi regulátory a tvůrci rozhodnutí (v překrytích resp. na hranicích oblastí působení)
1.2.4 Neadekvátní, nebo chybějící zpětná vazba: -vynechaná v návrhu (projektu) systému -nedostatky v komunikaci -dopravní zpoždění -neadekvátní systém sběru informací -není bráno v úvahu dopravní zpoždění a nepřesnosti měření
2. Neadekvátní výkon kontrolních činností
2.1 nedostatky v komunikaci
2.2 Neadekvátní chování ovládačů
2.3 Časová zdržení

PŘÍLOHA B - OBRAZY MODELŮObraz 1 - Model schodůčinnosti podle Rasmussena (1986)[5]

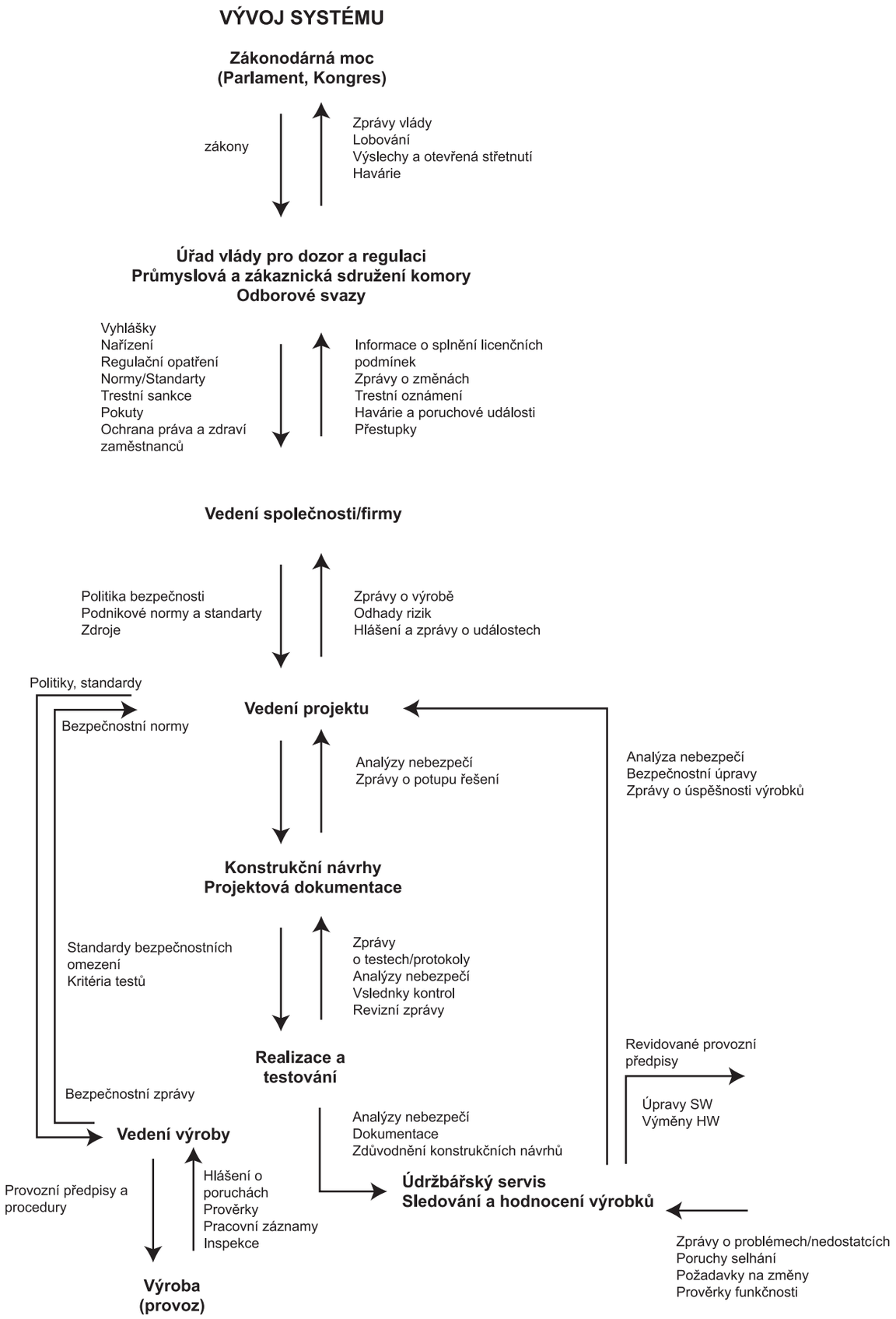
KNOWLEDGE BASE



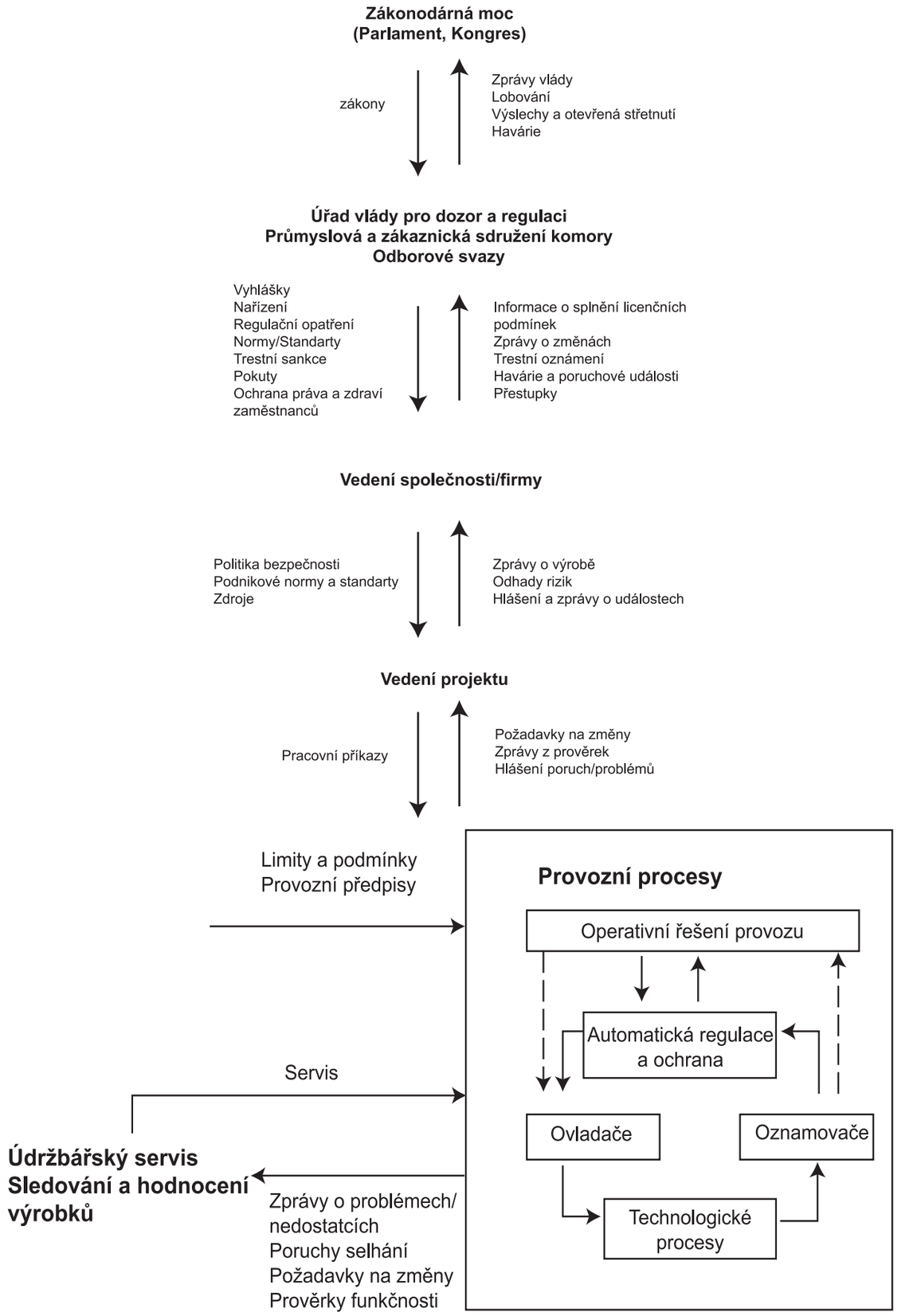
Vysvětlivky

Žluté bloky = činnost založená na dovednostech
Zelené bloky = činnost založená na pravidlech
Modré bloky = činnost založená na znalostech
Prázdné šipky = předpokládaný postup činnosti
Úzké plné šipky = zkratka

Obraz 2 - Model STAMP



VÝVOJ SYSTÉMU



PŘÍLOHA C - VYBRANÉ HAVÁRIE V JADERNÝCH ELEKTRÁRNÁCH Z POHLEDU SYSTÉMOVÉ BEZPEČNOSTI

Havárie na reaktoru Windscale

Charakteristika reaktoru Windscale a průběh havárie

Reaktor Windscale se nachází na pobřeží Cumberland ve Velké Británii a byl prvním britským produkčním reaktorem. Byl postaven na výrobu plutonia a proto se liší od reaktorů, které se používají k průmyslové výrobě elektrické energie. Je to grafitem moderovaný a vzduchem chlazený typ reaktoru. Chlazení je řešeno jako průtokové, což znamená, že chladící vzduch je vháněn do aktivní zóny a z ní přímo vyfukován do ovzduší. Protože jakákoliv částečka/znečištění vzduchu by se mohla stát radioaktivní, byly na reaktoru Windscale nainstalovány filtry vzduchu před jeho vstupem do aktivní zóny.

V původním projektu nebyly filtry ve výstupu chladícího vzduchu do atmosféry navrženy. Přidány byly dodatečně tehdy, když se při výstavbě reaktoru zjistilo, že se takové výstupní filtry používají na stejných typech reaktorů v USA. Svědčí o tom i umístění těchto filtrů ve výšce přibližně 130 m nad zemí. Všeobecně byly přijímány jako zbytečnost, až i hloupost.

V grafitech moderovaných reaktorů působí efekt tzv. Wignerovy energie, která se v grafitu kumuluje. Tento jev se stal známým až po postavení reaktoru Windscale. Naakumulovaná energie se za jistých okolností uvolní jako tepelná energie. Když k tomu dojde neočekávaně nebo nekontrolovatelně, může dojít k nárůstu teploty grafitu nad povolené meze a k tavení paliva.

Popis havárie

Dostupné informace o havárii reaktoru Windscale, které v této části uvedeme, jsou převzaty ze zprávy autora Megaw [46]. V září r. 1952 došlo k spontánnímu uvolnění Wignerovy energie v odstaveném reaktoru Windscale. Teplota grafitu rostla, ale nedosáhla nebezpečné úrovně a ani nedošlo k žádnému poškození. Po této poruše bylo nařízeno pravidelné kontrolované odvádění tepla z Wignerovy energie. Prováděnou proceduru popisuje Megaw jako odvádění Wignerovy energie pomocí zvýšení teploty grafitu nad normální hodnotu dočasným provozem reaktoru bez průtoku chladícího vzduchu. Když se uvolnění tepla z Wignerovy energie odstartovalo, reakce jeho tvorby byla schopna se samostatně udržovat a personál odstavil reaktor. Celý postup musel být prováděn velmi opatrně vzhledem k dopravnímu zpoždění kapacitního jevu ohřevu grafitu. Pokud by se reaktor odstavil příliš rychle, nevzrostla by teplota grafitu dostatečněvysoko. V opačném případě by při opožděném odstavení reaktoru mohlo dojít k roztavení paliva. Až do podzimu r. 1957 byla uváděná procedura provedena mnohokrát a byla považována za čistě rutinní úkol.

Dne 7. října 1957 bylo spuštěno odvádění Wignerovy energie z reaktoru Windscale. Inženýrovi, odpovědnému za provedení této procedury , se zdálo, že celá reakce skončila příliš rychle. Nevěděl totiž, že termočlánky na měření tepla nebyly nainstalovány v nejteplejších částech aktivní zóny. Operátoři provedli druhé nahřátí grafitu poměrně velkou rychlostí a pravděpodobně způsobili poškození obalu palivových elementů a oxidaci palivové náplně. Přístroje neindikovaly nic zvláštního až do odpoledne

10. října, kdy přišla výstražná signalizace o úniku radioaktivity. Vizuální prohlídkou přes průzor se v 16.30 hod. toho dne zjistilo, že v aktivní zóně jsou rozžhavené palivové elementy a přes druhý otvor vyšlehly plameny.
Vše, na co si jen dokázali vzpomenout, bylo použito na uhašení plamenů, ale nic nebylo účinné. Kolem půlnoci se rozhodli, že zkusí uhasit oheň v reaktoru vodou, protože všechno ostatní selhalo. Pro minimalizování pravděpodobnosti parní exploze byla voda nalévána do reaktoru nespojitě v malých dávkách. Vodu začali nalévat do reaktoru druhý den ráno v 8.55 hod. a nalévání skončili 12. října odpoledne v 15.10 hod. Tehdy už byla aktivní zóna zchlazená, ale různé druhy radioaktivních prvků byly vypouštěny do atmosféry, roznášeny větrem a usazovaly se v půdě kolem budovy reaktoru. Radioaktivní materiály velmi nízké koncentrace zasáhly Belgii v pozdních hodinách 2.října a Frankfurt pozdě odpoledne 12. října. Do 15. října byly atmosférou zaneseny do Norska.

Bezprostřední úkoly provozu představovala kontrola dávek ozáření zaměstnanců a ochrana zdraví obyvatelstva v blízkosti reaktorového zařízení. Muži, kteří pracovali u reaktoru, nosili ochranné oděvy a respirátory a doba, během které byli vystavení záření, byla kontrolována. Hlavním rizikem byly malé děti, které pily mléko od krav pasoucích se na trávě, kontaminované jódem 131. Mléko z oblasti 200 mil ve směru větru od reaktorového zařízení bylo zlikvidováno i přesto, že nemuselo být zdravotně závadné po zpracování na sušené mléko, sýr, nebo čokoládu a tříměsíčním skladování těchto výrobků (tj. po době rozpadu jódu 131). Ministerstvo zemědělství rozhodlo s ohledem na veřejné mínění mléko zlikvidovat.

Celkově byly zlikvidovány 2 milióny litrů mléka. Farmářům byly ztráty nahrazeny a Megaw ve své zprávě píše, že bylo úsměvné, že najednou začaly krávy poškozených farmářů produkovat enormní množství mléka. Pod kontrolou byly i vzorky vody a jiných výrobků, ale žádné významné nebezpečí nebylo zjištěno.

Existují kontroverzní názory na to, zda uváděné dodatečně namontované výstupní filtry vzduchu (Cockcroftovy filtry pojmenované podle muže, který je dal nainstalovat) byly nebo nebyly účinné. Někteří lidé byli přesvědčeni, že filtry zachytily velké množství jódu 131 a zabránily tomu, aby havárie přerostla v katastrofu. Jiní prohlašovali, že tyto filtry zachytily jen malé množství jódu 131. Po 25 letech speciálního výzkumu účinkůradiace udává zpráva britského úřadu pro ochranu před jaderným zářením, vydaná v r. 1982, odhad 20 úmrtí na rakovinu štítné žlázy. Dodatečně bylo oznámeno, že vzhledem k získaným informacím o uniklých radioaktivních materiálech se původní odhad zvyšuje na 33 úmrtí. Toto číslo je horní odhad a skutečný počet je pravděpodobně nižší, ba dokonce rovný 0 [46].

Daleko jasnějším výsledkem havárie reaktoru Windscale bylo zničení důvěry veřejnosti s ohledem na potenciální nebezpečí jaderných elektráren a tehdy převažujícího názoru, že technologie zvítězí nad vším. I přestože byla zřízena komise pro vyšetřování této havárie, byla oficiální zpráva z tohoto vyšetřování zveřejněna až po 20 letech z důvodů ochrany jaderného průmyslu. Jako odpověď na obavy veřejnosti před nebezpečím jaderných zařízení byla na Jaderném dozoru Velké Británie zřízena sekce bezpečnosti a spolehlivosti, která měla odpovídat za bezpečnost jadrných zařízení.

Vzhledem k rozhodnutí, že doplnění požadovaných bezpečnostních zařízení by bylo příliš nákladné, byly po této havárii oba reaktory ve Windscale trvale odstaveny a izolovány. Trvalo víc než 10 let, než se začalo s demontáží havarovaného reaktoru.

Příčinné faktory havárie

U této havárie hrál bezpochyby významnou roli nedostatek znalostí o jaderných reaktorech spolu se sebeuspokojením a důvěrou v jejich bezpečnost. Tento fakt je nesmírně důležitý jednak proto, že hrál rozhodující roli u havárií v TMI a v Černobylu a také i proto, že s ním nikdo v tak vysoce vědecky fundovaném průmyslu nepočítal. Mnoho operátorů

a jiných zaměstnanců propadlo sebeuspokojení po mnoha letech prakticky bezporuchového provozu reaktoru. Podrobnější analýza příčinných faktorů této havárie není možná z důvodů nedostatku veřejně přístupných informací.

Havárie v jaderné elektrárně Three Mile Island (TMI)

TMI se nachází 10 mil jižně od Harrisburgu, kde jsou postaveny dvě jaderné elektrárny TMI-1 a TMI-2, jejichž společný instalovaný elektrický výkon je 1700 MW, což stačí k zásobování asi 300 000 domácností. Obě elektrárny jsou ve spoluvlastnictví společností Pensylvni Electric Company, Jersey Central Power & Light Company a Metropolitan Edison Company (Met Ed). Obě elektrárny provozovala společnost Met Ed. Všechny uvedené společnosti patří společnosti General Public Utilities Corporation, elektrárenské holdingové společnosti se sídlem v New Jersey.

Charakteristika JE Three Mile Island a průběh havárie

Ve středu 28. března 1979 se ve 04 hod. ráno zastavilo několik čerpadel kondenzátu a napájecí vody na. Zpráva Kemenyho komise, která vyšetřovala havárii v TMI, konstatovala, že série událostí způsobená selháním zařízení, chybami v pracovních procedurách a chybami personálu a způsobila po eskalaci uváděného výpadku čerpadel na do té doby nejhorší havárii v jaderném průmyslu USA [33].

Aktivní zóna reaktoru JE TMI-2 obsahuje přibližně 100 tun uranového paliva (uranový oxid) ve tvaru malých válcových palet s průměrem asi 1,3 cm a vysokých asi 2,5 cm, které jsou vkládány do tzv. palivových tyčí dlouhých přibližně 4 m. Plášť palivové tyče, který tvoří tzv. palivový povlak (pokrytí), je vyroben ze zirkoniové ocele Zircaloy-4, která velmi dobře vede teplo a má dobrou propustnost neutronů. Aktivní zóna reaktoru TMI-2 obsahuje 36 816 takových palivových tyčí.

Pro řízení štěpné řetězové jaderné reakce v reaktoru TMI-2 se využívá 69 řídících tyčí, které jsou vyrobeny z materiálu s vysokou schopností pohlcovat neutrony. Když se tyto tyče zasunou do aktivní zóny reaktoru, štěpná řetězová jaderná reakce se přeruší a zůstane blokována. Operátor reaktoru řídí výkon reaktoru pomocí počtu zasouvaných řídících tyčí a hloubkou jejich zasunutí do aktivní zóny. Na pohonných mechanismech pro pohyb řídících tyčí jsou tyče připevněny elektromagneticky. V případě potřeby havarijního (okamžitého) odstavení reaktoru se po stlačení havarijního tlačítka přeruší proudový obvod s elektromagnetem a tyče se volným pádem zasunou do aktivní zóny (tzv. scram reaktoru).

Hlavním nebezpečím provozu JE je možné uvolnění velkého množství radioaktivního materiálu naakumulovaného v palivu během jeho hoření. Všechen tento radioaktivní materiál se za normálních okolností nachází v palivových tyčích. Poškození povlakůpalivových tyčí může způsobit únik tohoto radioaktivního materiálu do chladící vody v reaktoru a tato voda se může v případě poškození dalších ochranných bariér JE, tj. tlakové nádoby reaktoru a ochranné obálky budovy reaktoru (kontejnmentu), dostat do okolí/životního prostředí JE. Uváděné tři bariéry - povlaky palivových tyčí, tlaková reaktorová nádoba a kontejnment - jsou základními bezpečnostními ochranami před únikem radioaktivního materiálu z aktivní zóny reaktoru. Povlaky palivových tyčí jako první zadržují radioaktivní materiál v palivových tyčích. Druhou bariérou k zabránění úniku radioaktivního materiálu po jeho případném uvolnění z palivových tyčí v důsledku poškození palivových povlaků je tlaková reaktorová nádoba s uzavřeným chladícím okruhem reaktoru. Tlaková reaktorová nádoba na TMI-2 je vysoká přibližně 13 m a hloubka její stěny je ~ 23 cm. Je obložena dvěma oddělenými betonovými a ocelovými těsněními s celkovou šířkou ~ 3 m, které pohlcují radioaktivní záření

a neutrony emitované z aktivní zóny reaktoru. Nakonec je toto vše vloženo do kontejnmentu vysokého ~ 60 m postaveného ze zpevněné betonové konstrukce s šířkou stěny ~ 1,3 m, který je poslední, tj. třetí bariérou zabraňující úniku radioaktivního materiálu z paliva do okolí JE.

Při provozu tlakovodních reaktorů je velmi důležité, aby chladící voda protékající aktivní zónou byla pod mezí sytosti, tj. pod bodem teploty varu vody při daném tlaku. Při havárii spojené se změnami tlaku v reaktorové nádobě dochází k porušení této nevyhnutelné podmínky a chladící voda v tlakové nádobě vře. Vařící voda může mít výrazně nižší chladící účinek na palivové tyče než voda podchlazená, nemusí však být ještě příčinou poškození palivových povlaků důsledkem jejich přehřátí. Problémy s přehřátím a možným poškozením palivových povlaků nastanou po varu vody a "obnažení" (tj. nezaplavení vodou) aktivní zóny v reaktoru resp. její části.

Obnažení aktivní zóny způsobuje dva problémy. Prvním je, že teplota palivových povlaků může v důsledku ztráty chlazení palivových tyčí narůst až na hodnotu (~ 1204 °C), při které dochází k reakci vody se zirkoniem, a následnému poškození palivových povlaků a produkci vodíku. Druhým problémem je nárůst teploty samotného uranového paliva až na hodnotu jeho tavení (~ 2870 °C). Roztavením paliva se může uvolnit velké množství radioaktivních materiálů. Kdyby došlo k roztavení většího množství paliva, mohlo by se přetavit přes dno tlakové nádoby reaktoru a uvolnit tím obrovské množství radioaktivních materiálů do budovy kontejnmentu.

Pro provoz bloku JE TMI-2 jsou nejdůležitější tato hlavní zařízení:

- primární okruh (s reaktorem, aktivní zónou, kompenzátorem objemu a chladícími okruhy s hlavními cirkulačními čerpadly chladící vody)
- parní generátor (ve kterém se vaří voda sekundárního okruhu pomocí tepla odváděného z reaktoru a vyrábí se pára pro turbínu)
- sekundární okruh (s turbínou, která pohání generátor na výrobu elektrické energie, s kondenzátorem páry vystupující z turbíny a čerpadly pro kondenzát a napájení vody do parogenerátorů).

Stručný funkční popis hlavních částí bloku tlakovodní JE, který je uveden v závorkách, zároveň i vysvětluje výrobu elektrické energie v JE.

Ráno 28. března 1989 vypadla napájecí čerpadla vody do parogenerátorů při 97% výkonu reaktoru. Výpadek napájecích čerpadel znamenal přerušení proudu vody do parogenerátorů a následně jejich vysušení a znemožnění produkce páry. Proto byla turbína odstavena automatickými ochranami. To se stalo v prvních dvou sekundách havárie.I přesto, že reaktor byl odstaven automatickou havarijní ochranou 8 sekund po výpadku prvního napájecího čerpadla, nárůst tlaku v reaktorové nádobě dále pokračoval. Vývoj tepla v aktivní zóně reaktoru pokračuje i po jeho odstavení zasunutím řídících tyčí v důsledku jaderných reakcí, které probíhají v radioaktivních materiálech ve vyhořelém palivu. Je to tzv. zbytkové teplo, jehož velikost je přibližně 6 % výkonu reaktoru v době po havarijním odstavení reaktoru. Toto zbytkové teplo musí být z reaktoru bezpodmínečněsoustavně odváděno, aby nedošlo k přehřátí aktivní zóny a následnému poškození povlaků palivových tyčí. Zabezpečení odvodu zbytkového tepla z reaktoru je proto jednou z prvořadých bezpečnostních funkcí JE. Pro případ výpadku napájecích čerpadel jsou připravena havarijní napájecí čerpadla vody do parogenerátorů, která se spouštějí automaticky při výpadku normálních napájecích čerpadel. Ve 14. sekundě průběhu havárie si operátor na blokové dozorně (dále BD) všiml, že havarijní napájecí čerpadla jsou v činnosti. Nepostřehl však dvě světelné signalizace, které oznamovaly, že armatury potrubí přívodu vody od havarijních napájecích čerpadel do parogenerátorů jsou zavřené. Stalo se to proto, že jedno ze světel bylo tehdy překryté žlutou údržbářskou vývěskou a nikdy se nezjistilo, proč bylo druhé varovné světlo přehlédnuto.

Vysušování parogenerátorů (tj. odpaření vody, která v nich zůstala po přerušení napájení) způsobilo snížení odvodu tepla přiváděného chladící vodou z aktivní zóny a tím zvýšení její teploty. Zvýšená teplota chladící směsi v reaktoru způsobila nárůst hladiny v kompenzátoru objemu a zároveň i tlaku v reaktorové nádobě. To aktivovalo otevření pojistného ventilu na kompenzátoru objemu pro zkorigování vzniklého přetlaku. Pojistný ventil, který byl pro tento účel nainstalován, zapracoval správněa z reaktoru začala přes otvor pojistného ventilu vytékat parovodní směs přes potrubí vedoucí od pojistného ventilu do speciální barbotážní nádrže umístěné na podlaze v budově kontejnmentu.

Po havarijním odstavení reaktoru a otevření pojistného ventilu začal tlak v primárním okruhu klesat. Pojistný ventil se měl zavřít ve 13. sekundě při poklesu tlaku na hodnotu (~15,4MPa), ale protože se zasekl, zůstal otevřený. Světelná signalizace na příslušném panelu v BD, která indikovala, že elektrický proud v obvodu pojistného ventilu byl přerušený, dovolila nesprávně operátorům předpokládat, že se pojistný ventil zavřel. Ve skutečnosti se tento pojistný ventil zasekl v otevřené poloze po dobu až 2 hodin a 22 min. a umožňoval unikání chladící směsi z reaktoru, čímž byla iniciována havárie se ztrátou chladící směsi - LOCA (Lost Of Coolant Accident).

V prvních 100 minutách havárie vytekla více než jedna třetina objemu chladící směsi v primárním okruhu přes otevřený pojistný ventil. Pokud by se pojistný ventil uzavřel tak, jak byl projektován, nebo kdyby si operátoři na BD uvědomili, že pojistný ventil se zasekl a zůstal otevřený a uzavřeli by zajišťovací armaturu na potrubí u pojistného ventilu a znemožnili by tak únik chladící směsi z primárního okruhu, nebo kdyby nechali v provozu čerpadla vysokotlakového havarijního chlazení, byla by havárie na TMI jen malou provozní událostí.

Operátoři na BD byli tehdy vyškoleni tak, aby při vzniku havárie reagovali rychle a prakticky bez přemýšlení dopředu připravenými zásahy na iniciační havarijní signály. V průběhu několika minut po prvním havarijním signálu na BD následně přišla kaskáda asi 100 alarmových signálů. Operátoři reagovali rychle, tak jak byli vycvičeni pro havarijní odstavení turbíny reaktoru. Později jeden z operátorůřekl vyšetřovací komisi o své reakci na lavinu alarmů toto: „Byl bych nejraději vyhodil celý panel s havarijní signalizací. Nedával nám žádnou užitečnou informaci.“.

Na BD byl povolán směnový mistr, který tehdy dohlížel na údržbářské práce na speciálním čistícím zařízení kondenzátu používaném v bloku TMI-2. Tyto údržbářské práce v čističce spočívaly ve vyplavování hrudek vytvořených z umělohmotných kuliček, používaných k odstraňování rozpuštěných minerálů v napájecí vodě, které zůstávají zachyceny v potrubí, kterým se vypouštějí z čističky. Na vyplavování zachycených hrudek se používala směs vody a vzduchu. Později se ukázalo, že přes jeden vadný ventil na čističce pronikla voda do rozvodu vzduchu pro ovládání ventilů v čističkách, což způsobilo poruchové otvírání a zavírání ventilů. Tato chybná činnost ventilůpravděpodobně způsobila výpadek napájecích čerpadel, který vedl k havárii. Uváděný problém s únikem vody do ovládacího vzduchu ventilůčističek se vyskytl nejméněvakrát před havárií na TMI-2. Je možné s jistotou říci, že kdyby společnost Met Ed napravila předcházející problémy s čističkami, nebylo by nikdy došlo k nešťastné posloupnosti událostí z 28. března 1979 [33].

Při zaseknutém pojistném ventilu tlak chladící směsi v primárním okruhu neustále klesal a hladina se v kompenzátoru objemu prakticky ztratila. V 13. sekundě havárie spustil operátor čerpadlo pro doplňování vody do primárního okruhu. Ve 48. sekundě se začala zvyšovat hladina v kompenzátoru objemu, tlak ale dále klesal.

Po jedné minutě a 45. sekundě od začátku havárie se parogenerátory vysušily, protože přívod vody od havarijních napájecích čerpadel byl zablokován už uváděnými uzavřenými armaturami. Voda v primárním okruhu se ještě více ohřála a svojí expanzí způsobila další zvýšení hladiny v kompenzátoru objemu.

Po dvou minutách vývoje havárie, když hladina vody v kompenzátoru objemu neustále stoupala, došlo k náhlému výraznému poklesu tlaku. Tehdy byla automaticky spuštěna vysokotlaká havarijní čerpadla, která začala do reaktoru dodávat přibližně 3785 litrů chladící směsi za minutu. Podle hladiny v kompenzátoru objemu operátoři usuzovali, že je v reaktoru dostatek chladící směsi. Tlak však nadále klesal a teplota chladící směsi se ustálila.

Asi dvě a půl minuty po startu vysokotlakých havarijních čerpadel operátor jedno z nich odstavil a na druhém zredukoval průtok na méně než 379 litrů za minutu. Udělal to proto, protože byl naučen, že se hladina kompenzátoru objemu má udržovat na nominální hodnotě a nesmí se připustit zaplnění kompenzátoru objemu vodou (tj. vytvořit tzv. “tvrdý okruh“). U tvrdého okruhu se velmi těžko reguluje tlak chladící směsi v primárním okruhu a hrozí nebezpečí poškození hlavních cirkulačních čerpadel.

Kemenyho komise konstatovala, že klesající tlak dohromady s konstantní teplotou chladící směsi v primáru po spuštění vysokotlakových havarijních čerpadel musely upozornit operátory, že došlo k LOCA havárii a bezpečnost vyžaduje, aby vysokotlaká havarijní čerpadla byla v provozu. Jeden z operátorů přes to všechno komisi řekl: „Rapidní zvyšování hladiny v kompenzátoru mě vedlo k přesvědčení, že dodávka chladící směsi vysokotlakovými havarijními čerpadly je nadbytečná a že dostali bychom se rychle na tvrdý okruh“.

Meze sytosti dosáhla chladící směs v reaktoru asi za pět a půl minuty od počátku havárie. V reaktoru se začaly formovat parní bubliny a začaly z něho vytlačovat vodu. Hladina v kompenzátoru objemu se tím opět zvýšila. Pro operátory to bylo pouze potvrzení toho, že v reaktoru je stále dost vody. Vůbec si neuvědomovali, že voda v reaktoru vře a mění se v páru. Skutečná bilance doplnění a úniku chladící směsi z primárního okruhu byla taková, že unikalo větší množství chladící směsi, než bylo doplňováno. Operátoři tak začali vypouštět chladící směs z reaktoru přes potrubní systém pojistných ventilů.

V 8. min. někdo zjistil, že do parogenerátorů nepřitéká žádná voda z havarijních doplňovacích čerpadel. Operátor se podíval na kontrolní signální světla, která indikují, zda jsou armatury na trasách čerpadel havarijního napájení parogenerátorů otevřené nebo zavřené. Jeden pár těchto armatur, které se automaticky otvírají po dosažení plného průtoku havarijních napájecích čerpadel, byl otevřený. Druhý pár armatur, nazývaných “dvanáctky“, o kterých se běžně předpokládá, že jsou vždy otevřené, kroměspecifických testů havarijních napáječek, byl zavřený. Operátor otevřel oběřady těchto armatur a voda začala natékat do parogenerátorů plným proudem.

Vědělo se, že již uváděné “dvanáctky“ armatury byly zavřené dva dny před tím (26.března) z důvodů provedení rutinních testů připravenosti havarijních napájecích čerpadel. Vyšetřování Kemenyho komise nezjistilo příčinu, proč byly tyto armatury zavřeny ještě v 8. minutě vývoje havárie. Vyšetřovatelé konstatovali, že nejpravděpodobnějším vysvětlením jsou následující možnosti (1) armatury nebyly po testech dne 26.března opět otevřeny, (2) armatury byly po provedeném testu otevřené, ale operátoři je na BD omylem zavřeli v prvních chvílích havárie, nebo (3) armatury byly po testech omylem zavřeny z řídícího štítu mimo BD. Ztráta havarijního napájení parogenerátorů na 8 minut neměla významný vliv na začátek havárie, přispěla však ke zmatku a odpoutání pozornosti operátorů, když se snažili pochopit příčinu hlavního problému s reaktorem.

Kemenyho komise uvedla, že během prvních dvou hodin havárie operátoři nezjistili nebo nedokázali rozpoznat význam více věcí, které je musely upozornit na to, že mají otevřený pojistný ventil a že došlo k LOCA havárii. Jednou z nich byla vysoká teplota potrubí od pojistného ventilu, kterým vytékala chladící směs z primárního okruhu. Havarijní provozní předpis stanoví, že hodnota 93°C teploty potrubí indikuje, že pojistný ventil je otevřený. Druhý havarijní předpis zase stanoví, že když teplota potrubí dosáhne 55°C, pojistný ventil propouští a musí se zavřít. Operátoři dosvědčili, že teplota potrubí byla běžně vysoká,

protože buď pojistný ventil, nebo některé jiné armatury mírněpropouštěly (netěsnily). To byl důvod, proč operátoři přehlédli význam této teploty. Vedoucí směny řekl komisi, že vysokou teplotu potrubí považoval za důsledek jeho zahřátí při otevření pojistného ventilu, protože věděl že se pojistný ventil otevřel a že může trvat nějakou dobu, než potrubí vychladne na teplotu nižší než je nastavená hodnota signalizace.

Ráno v 04 hod. 11 minut havarijní signalizace oznamovala vysokou hladinu vody ve sběrné jámě budovy kontejnmentu, což je příznakem úniku chladící směsi, nebo porušení integrity primárního okruhu. Voda smíšená s parou vycházela z počátku z otevřeného pojistného ventilu do barbotážní nádrže umístěné na podlaze budovy kontejnmentu. Po jeho přeplnění (prasknutí ochranné membrány) začala voda téct do sběrné jámy. Tato voda byla mírně kontaminovaná. Ze sběrné jámy byla přečerpávána do nádrže umístěné v blízké budově pomocných systémů.

Dalším faktem, který Kemenyho komise označila za jasný signál pro operátory, že došlo k LOCA havárii, byl nárůst teploty a tlaku v budově kontejnmentu. To, že si toho operátoři nevšimli, označila komise za vážný nedostatek v jejich přípravě.

Přibližně 5 min. po signalizování přítomnosti vody ve sběrné jámě kontejnmentu, měl jeden z operátorů telefonát z budovy pomocných systémů, vněmž mu oznámili, že jeden z přístrojů ukazuje výšku hladiny víc než 1,9 m ve sběrné jámě kontejnmentu. Když si operátor tuto informaci prověřil v počítači, dostal stejnou odpověď. Doporučil potom vypnutí dvou čerpadel na přečerpávání vody ze sběrné jámy do budovy pomocných provozů. Nevěděl však, odkud voda do sběrné nádrže teče a chtěl zabránit tomu, aby byla voda, která mohla být radioaktivní, přečerpávána ven z budovy kontejnmentu. Oběčerpadla vody ze sběrné jámy byla vypnuta okolo 04.39 hod. Tehdy už bylo nejméně30 m^3 nízkoradioaktivní vody přečerpáno do budovy pomocných systémů. Od začátku havárie v té době uplynulo pouze 39 minut.

Tehdy už vedoucí pracovníci a experti přišli na TMI-2. Vrchní šéf útvaru technické podpory, který byl telefonicky vyrozuměn, že na bloku mají výpadek turbíny, dosvědčil, že to co našel, vůbec neodpovídalo tomu, co očekával. Řekl: „Cítil jsem, že jsme se octli v opravdu neobvyklé situaci, protože jsem ještě nikdy neviděl, aby hladina kompenzátoru objemu vystoupila a udržovala se tak vysoko a současně tlak chladící směsi v primárním okruhu stále klesal. Tyto dva parametry se vždy chovaly stejně.“. Posádka BD s tím úplněsouhlasila. Havárii později popisovali jako kombinaci událostí/jevů, které předtím nikdy nezažili, ať už v provozu, nebo při výcviku na simulátoru.

Krátce po páté hodině začala čtyři hlavní cirkulační čerpadla chladící směsi v primárním okruhu silně vibrovat. Vibrace byly způsobeny čerpáním parovodní směsi, což byla další nepoznaná indicie toho, že chladící směs v reaktoru vře. Operátoři se obávali, že nebezpečné chvění může poškodit čerpadla nebo cirkulační potrubí. Vedoucí směny a jeho sloužící operátoři na BD, přesně podle výcviku, vypnuli dvě cirkulační čerpadla v 05.14 hod. a později po 27 min. vypnuli i zbývající dvě cirkulační čerpadla.

Okolo 06.00 hod. radiační alarmový signál uvnitř budovy kontejnmentu potvrdil fakt, že přinejmenším několik palivových článků má porušené povlaky a unikají z nich radioaktivní plyny do chladící směsi primárního okruhu. V důsledku úniku chladící směsi, který byl větší než doplňování, se obnažil vrch aktivní zóny a přehřál se až na teplotu, při které dochází k reakci páry se zirkoniem, při které se uvolňuje vodík. Část tohoto vzniklého vodíku pronikla do kontejnmentu přes zaseknutý pojistný ventil a barbotážní nádrž a zbytek zůstal v reaktorové nádobě.

Zaseknutý pojistný ventil na kompenzátoru objemu byl uzavřen v 06.22 hod. po dvou hodinách a 22 minutách od té doby, co se po otevření zasekl a neuzavřel se. Únik chladící směsi byl zastaven a tlak se začal zvyšovat, ale destrukce aktivní zóny pokračovala. Z ne-

známých příčin nenaběhlo havarijní vysokotlaké čerpadlo ani po další hodině. Do té doby byla zaznamenán rostoucí úroveň radiace v budově kontejnmentu i v budově pomocných systémů a všechny sledované údaje ukazovaly, že víc než 2/3 výšky aktivní zóny jsou bez chladící směsi a palivo je přehřáto na teplotu od 1930°C do 2200°C. V 06.54 hod. spustil operátor jedno z hlavních cirkulačních čerpadel, ale po 19 min. ho musel pro velké vibrace odstavit. Radiační havarijní signalizace začaly přibývat a v lokalitě JE musela být vyhlášena havarijní situace. Tímto aktem se rozběhla posloupnost činností vyžadovaných havarijním plánem včetně vyrozumění státních a dozorových orgánů. Později, když byly evidovány další havarijní radiační signály, byla vyhlášena všeobecná havarijní situace.

Čtyři hodiny po začátku havárie byla budova kontejnmentu izolována, což kromějiného znamená, že se armatury na potrubích pro přečerpávání chladící směsi z budovy kontejnmentu do budovy pomocných provozů zavřely. Tyto armatury se zavřou automaticky, ale operátor je může z BD otevřít. Ve skutečnosti otevřeny byly a radioaktivní chladící směs i nadále přitékala do budovy pomocných systémů, odkud některé radioaktivní materiály unikly do okolí JE.

Podle projektu TMI-2 má být budova kontejnmentu izolován po dosažení určité hodnoty tlaku. Pro snižování tlaku páry vnikající do budovy kontejnmentu z primárního okruhu používali operátoři sprchový a ventilační systém kontejnmentu. NRC vydala v
r. 1975 nová kritéria pro izolování budov kontejnmentů na JE. Na TMI-2 měli povolený provoz kontejnmentu podle původních kritérií. Kemenyho komise konstatovala, že opožděné izolování kontejnmentu způsobilo pouze malý rozdíl průběhu havárie.

Operátoři se znovu pokusili aktivovat čerpadla havarijního chlazení reaktoru v 08.26 hodin a pomocí čerpadel udržovat určitý průtok chladící směsi v reaktoru. Aktivní zóna byla tehdy ještě stále obnažená a bylo zjevné, že se ji podaří zaplavit čerpadly havarijního chlazení až okolo 10.30 hod.

Tehdy už byly instrukce havarijního plánu plněny v okolí JE. Práce personálu na BD se zkomplikovala a stala se těžší, protože pracovníci v JE museli začít používat ochranné masky. Obzvlášť obtížnou se stala komunikace mezi pracovníky.

Odpoledne, ve 13.50 hod., zaslechli na BD výbuch. Byl to výbuch vodíku uvnitřbudovy kontejnmentu, což si ale ještě dlouho nikdo neuvědomil. Zvuk byl chybněpovažován za efekt ventilace. Tlakový pík na záznamu z počítače byl komentován jako možná chyba měření.

V pátek, 30. března 1979, se už havárií na TMI-2 zabývali experti jaderného průmyslu ze všech zemí. V ten den vznikla obava z možné exploze vodíkové bubliny v reaktoru. Někdo zNRC přišel s teorií (která se nakonec ukázala jako chybná), že radiace v reaktoru může způsobit rozklad vody na vodík a kyslík a přivodit tak explozi, která by mohla roztrhnout tlakovou nádobu reaktoru. Tyto obavy se ukázaly jako nepodložené, ale i tak se celý týden se mnohé laboratoře a vědci pokoušeli poskytnout radu pro řešení tohoto problému.

Škody způsobené popsanou havárií včetně dekontaminace budov se odhadovaly až do výšky 1,86 miliard dolarů, přičemž v této sumě nebyly zahrnuty ztráty ve výrobě.

Efekt ohrožení zdraví okolního obyvatelstva havárií byl zanedbatelný, protože pouze velmi malé množství radioaktivního materiálu se dostalo mimo JE. Guvernér státu Pensylvánie vyzval dne 30. března 1979 k evakuaci dětí a těhotných žen žijících v blízkosti TMI. Tuto radu mnozí uposlechli. Kemenyho komise konstatovala, že hlavní zdravotní efekt z havárie byl mentální stres obyvatelstva. Mnohem vážnější byl dopad havárie na veřejné mínění obyvatelstva vůči jadernému průmyslu, kde se projevil výrazný pokles důvěry veřejnosti v jadernou energetiku a v dozorový orgán nad její bezpečností.

Příčinné faktory havárie - druhá úroveň

Příčinné faktory havárie TMI rozebereme v tomto bodu studie podle výše uváděného tříúrovňového modelu kauzality havárií. První úroveň – průběh a hlavní události havárie, byla popsán. V následujícím textu se budeme zabývat druhou úrovní zjišťující podmínky a okolnosti, za jakých havárie proběhla.

Největším pozitivem při havárii TMI-2 bylo zachování celistvosti kontejnmentu i přes explozi vodíku v něm, čímž zůstala převážná část radioaktivních materiálů uvnitřbudov JE. Na druhé straně však mnoho zásahů operátorů k havárii přispělo negativně. Operátoři TMI-2 nebyli nikdy školeni pro řešení následků zaseknutí pojistného ventilu kompenzátoru objemu a instrukce pro chování se v této situaci nebyly v havarijních provozních předpisech uvedené. Také nebyli speciálně připravováni na nebezpečí vzniku varu v reaktoru, přestože fyzika tohoto jevu jim byla všeobecně známa. Vedení společnosti Met Ed nepovažovalo vření chladící směsi v reaktoru za zvlášť nebezpečné a přestože se taková událost ve společnosti přihodila asi rok před havárií TMI-2, nebylo její skutečné nebezpečí - obnažení aktivní zóny - operátorům zdůrazněno. Když došlo při havárii ke vzniku varu v chladící směsi, operátoři nerozpoznali jeho význam a neprovedli rychle nápravné zásahy. K tomu všemu neměli operátoři správné informace o teplotách v potrubí vedoucím od zaseklého pojistného ventilu.

Kemenyho komise konstatovala, že většina operátorů a ostatních zaměstnanců, kteří se podíleli na zvládnutí havárie, nerozuměli úplně provozním principům zařízení JE. Jejich výcvik a příprava kladly nedostatečný důraz na základní pochopení fyziky reaktoru a principy jeho bezpečného provozu.

Navíc se ukázalo, že simulátorový výcvik operátorů ve společnosti B&W neobsahuje výcvikové scénáře pro havárie s vícenásobnými poruchami. Výcvikový simulátor nebyl principiálně schopný zreprodukovat podmínky a události, kterým byli operátoři vystaveni při havárii. Simulátor nedokázal simulovat událost se zvyšující se hladinou v kompenzátoru objemu a současným poklesem tlaku chladící směsi v primárním okruhu.

Mnohé z provozních a havarijních předpisů používaných na TMI byly neadekvátní včetně těch, které byly připravené pro zvládnutí LOCA havárií a pro provoz kompenzátoru objemu. Kemenyho zpráva konstatovala, že nedostatky v těchto pracovních postupech mohly zmást operátory a být příčinou jejich chybných zásahů. Zpráva dále poukázala na to, že analýzy havárií s malými úniky, které provedli ve společnosti B&W v r. 1978 byly na Met Ed chybně interpretovány a potom i chybnězavedeny do havarijních provozních předpisů pro tento typ havárie. Provozní předpisy měly navíc i formální chyby (překlepy apod.) a schválení platné revize nebylo provedeno v souladu s platným postupem v Met Ed.

Členové Kemenyho komise konstatovali, že schopnost personálu TMI-2 identifikovat potrubí a armatury byla nižší než je běžný průmyslový standard. V osmé hodině havárie personál potřeboval 10 min. času pro lokalizování tří armatur v budověpomocných provozů při vysoké úrovni radiace.

Opakující se problémy s čističkou kondenzátu nebyly na TMI-2 odstraněny a jak jsme již výše uvedli, právě ty byly pravděpodobnou příčinou spuštění havárie. Společnost Met Ed také neodstranila nedostatky zařízení pro monitorování radiační situace, které zjistil audit NRC měsíc před havárií.

BD na TMI-2 byla nevhodně navržena z hlediska zvládnutí havarijních situací. Její projektanti systematicky nevyhodnotili vypracovaný návrh, aby se prokázalo, zda vyhovuje havarijním podmínkám. Řešení BD bylo nesprávné prakticky ve všem: v rozmístění přístrojů a signalizaci na panelech, v obsahu displejů, v prostorovém řešení pracovišť a pod. Nebylo divu, že operátoři dělali chyby, protože jim k tomu konstrukce BD přímo napomáhala. Zásadními nedostatky, které jsme již uvedli výše, byla lavina havarijních oznámení

v prvních minutách havárie a chybějící funkční seskupení validních parametrů. Jeden z členů Kemenyho komise byl doslova zděšený z toho, že podstatné parametry pro havarijní situaci nebyly seskupeny dohromady, ale obrazněřečeno, byly roztroušeny po všech panelech a v některých případech byly i špatněčitelné. Dalším závažným nedostatkem byla chybějící informace o měření hladiny v reaktorové nádobě. Výrobce B&W se oficielně vyjádřil, že přímé měření hladiny by mohlo být nespolehlivé a příliš drahé. Několik měřících přístrojů selhalo, nebo bylo mimo rozsah měření, protože přístroje nebyly dimenzovány pro takové hodnoty, kterých bylo dosaženo během havárie. Počítač, který zaznamenával údaje během havárie, se v jednom momentu zahltil informacemi a důležité údaje nebyly zaznamenány. Sám John Kemeny se o BD na TMI vyjádřil, že zaostávají nejméně 20 let za vývojem.

K již uváděným nedostatkům provozních předpisů patřila i nedostatečná kontrola (verifikace) provádění testů připravenosti. Po havárii byly zjištěny vážné nedostatky při provádění radiační kontroly zařízení prostorů. Údržbářský personál byl vzhledem k provozním úsporám zredukován a v době havárie byl údržbáři přepracováni Blok měl značný počet neplánovaných odstávek a více zařízení nebylo provozu schopné. Prohlídkou záznamů o zařízeních zpětně za šest měsíců se zjistilo, že mnoho jednotlivých částí zařízení, ve kterých probíhaly havarijní události, mělo velmi špatnou údržbu, kdy se jednotlivé části zařízení náležitě neopravovaly (snímač hladiny v kompenzátoru objemu, spalování vodíku, vypínače doplňovacích čerpadel, čistička kondenzátu). I přes známé problémy s čističkou zjistila inspekce na TMI-1, že na armaturách by-pasu (odtoku čističek pro jejich odstavení při údržbě) visí bórové stalaktity delší než 30 cm a z podlahy pod nimi rostou z unikající chladící směsi bórové stalagnity.

Příčinné faktory havárie - třetí úroveň

Na této úrovni rozebereme omezení, která měla zabránit vzniku havárie.

Přehlížení varovných signálů

Podobné události na jiných JE ukázaly počáteční problémy a potřeby operátorůmít jasné instrukce pro zvládnutí takových událostí, k jakým došlo na TMI-2. Některé z nich (např. události na JE Davis-Besse) jsme již v této studii uvedli. Po události z dubna 1978 na TMI si operátoři managementu stěžovali na problémy BD, k žádným nápravám však nedošlo.

Zajištění ovladatelnosti reaktoru

Reaktor TMI-2 je podobně jako reaktor RBMK v Černobylu mimořádně citlivý na poruchy. To je dáno malým objemem primární chladící směsi v porovnání s ostatními reaktory v USA a poddimenzovaným kompenzátorem objemu. Tyto vlastnosti způsobují rychlé reakce na poruchy a stěžují ovládání reaktoru. Hlavním ekonomickým ukazatelem provozu jaderného reaktoru je poměrný palivový objem, který má za následek velmi rychlou sekvenci událostí zejména při LOCA haváriích, na které nemohou operátoři reagovat. Pro dostatečné statistické ujištění, že takovýto reaktor je pod kontrolou i při LOCA haváriích, jsou nainstalovány redundantní bezpečnostní systémy. Tyto systémy činí systém složitější, což zvyšuje pravděpodobnost, že operátor může zasáhnout nevhodně. Ve zprávě se uvádí, že by bylo vhodnější zvýšit o několik procent investiční náklady na konstrukci reaktoru, aby operátor v poruchových/havarijních situacích nemusel vykonat žádný zásah v prvních 30 min. jejich vývoje.

Nedostatečná pozornost věnovaná lidskému faktoru

Uvedli jsme již výše, že projektanti BD na TMI-2 nevěnovali dostatečnou pozornost interakci člověk-stroj v situacích rychlých změn stavů zařízení a nepřehledných provozních podmínek při haváriích. Potřeby operátorů na BD pro zvládnutí pomalu se rozvíjejících LOCA havárií s malým únikem byly na TM1-2 úplně ignorovány pravděpodobně proto, že se projekt koncentroval pouze na velké LOCA havárie, při kterých není čas na významnější zásah operátorů.

Při zhodnocení úlohy, kterou sehráli operátoři v průběhu havárie, se Kemenyho komise zdržela jednoduchého obvinění operátorů a pouze zdůraznila, že jejich chování bylo způsobeno více faktory (nedostatky v přípravě, v provozních předpisech, chyby organizace při nezabezpečení vhodného poučení z předchozích havárií, chyby BD [33].

Po havárii TMI-2 se začala lidskému faktoru v jaderném průmyslu věnovat velká pozornost. Barrett to komentoval prohlášením, že jaderný průmysl prokazatelněrozpoznal důležitost výběru operátorů, jejich tréninku, motivace a procesu získávání licencí tak, jako i návrhem BD z hlediska komunikačních nároků, ergonomie a kognitivního inženýrství [6]. Naneštěstí se s tímto prohlášením neztotožňují všichni odborníci (např. Hornick [27]).

Sebeuspokojení

Kemenyho zpráva vyzdvihuje fakt, že v jaderném průmyslu všeobecně převládl pocit nemožnosti vzniku velké havárie a tento pocit pronikl i do dozorových orgánů vlády USA. Vznikl proto, že za celé roky nedošlo v jaderném průmyslu k žádné události s dopadem na zdraví obyvatelstva. Důvěra v bezpečnost jaderných elektráren postupněpřerostla do přesvědčení. Toto je důležité si uvědomit, když chceme pochopit, pročmnohé kroky, které mohly zabránit havárii TMI-2 nebyly provedeny. Kemenyho komise vyjádřila své přesvědčení, že tento postoj musí být změněn na takový, který říká, že jaderná energie je ve své přirozenosti potenciálně nebezpečná, a proto si musíme při ní soustavně klást otázky, zda je stále pod bezpečnostním dohledem a zda tento dohled je dostatečný k zabránění velkých havárií.

Za další projev sebeuspokojení a podcenění rizika radiační havárie je třeba považovat skutečnost, že elektrárna TMI byla neadekvátně projektována z hlediska dekontaminace a čištění zamořených a poškozených částí elektrárny.

Management

Kemenyho zpráva zdůrazňuje závažné nedostatky managementu TMI-2. Směnový mistr nemohl adekvátně plnit svou úlohu dohledu na probíhající údržbářské práce, protože byl zavalený administrativní prací, která nesouvisela s výkonem dohledu. Na bloku se neprováděla systematická kontrola stavu zařízení a otevření/zavření armatur při střídání směn. Dohled nad postupy kontroly (surveillance procedures) připravenosti zařízení byl nedostatečný a byly zjištěny nedostatky v systému zajištění kvality a v systému kontroly. Revizí poruchových hlášení z TMI-2 se zjistilo, že neobsahují opakované chyby typu „omissions“ (přehlédnutí, vynechání), že mnohé události nebyly dostatečně analyzovány a byla přijímána nevhodná nápravná opatření. Na TMI-2 nebyla zřízena pracovní skupina odpovědná za zjištění a napravení potenciálních bezpečnostních problémů, na které upozorňovali zaměstnanci. Nakonec zpráva uvádí, že vedení JE dovolilo provozovat elektrárnu s vědomím více slabých míst v práci operátorůBD.

Konečnou odpovědnost za projekt elektrárny TMI měla společnost GPU Service Corporation (GPUSC), jejíž představitelé připustili, že neměli vhodné experty nebo zkušenosti v některých oblastech. Po dostavění odevzdala GPUSC elektrárnu společnosti Met Ed. Tato neměla dostatečné znalosti, zkušenosti a personál na adekvátní provoz a údržbu elektrárny.

Odpovědnost za rozhodnutí managementu byla rozdělena mezi management na lokalitě TMI a vedení společnosti Met Ed a GPUSC. GPUSC si uvědomila začátkem r. 1977, že je žádoucí, aby odpovědnost za provoz elektrárny měla jedna organizace. Externí audit managementu, který byl proveden na jaře v r. 1977 doporučil zpřehlednit a přehodnotit úlohy GPUSC a Met Ed při projektování a stavbě nových zařízení, posílit jejich vzájemnou komunikaci a stanovit minimální standardy pro bezpečný provoz JE budovaných firmou GPU. K integraci managementu došlo až po havárii.

Zabezpečení kvality

Společnost Met Ed měla plán zajištění kvality, který splňoval požadavky NRC. Kemenyho zpráva konstatuje, že dřívější požadavky NRC byly neadekvátní. Nebylo vyžadováno, aby programy zajištění kvality byly aplikovány na JE jako celek, ale jen na části/systémy, které byly klasifikovány jako bezpečnostně významné. Ani jeden z pojistných ventilů a ani žádná čistička kondenzátu nebyly zařazeny do této kategorie zařízení. Navíc podle Kemenyho zprávy NRC nepožadovala žádnou úroveň nezávislosti revize (od liniového managementu), která je běžná pro programy zajištění kvality v bezpečnostně kritických provozech.

Plán kvality zavedený ve společnosti Met Ed měl podle Kemenyho komise a podle auditu NRC provedeném po havárii taktéž závažné nedostatky. Nezávislý audit provádění procedur pro kontrolu stavu připravenosti zařízení byl požadován jen každé dva roky. Neexistoval žádný plán pro revize těchto procedur a ve skutečnosti ani nebyla provedena žádná revize procedur starších více než dva roky. Našly se vážné nedostatky v hlášeních, analýzách a řešení problémů bezpečnostně významných zařízení a jiných událostí, jejichž vznik požaduje NRC hlásit. Nezávislé posouzení celkového provozu elektrárny bylo minimální.

Nedostatky v procesu schvalování provozních předpisů

Provozní předpisy na TMI-2 nebyly v plném rozsahu překontrolovány experty. Po havárii začala NRC požadovat, aby bezpečnostní útvary na elektrárně povinněpřekontrolovaly provozní postupy a procedury, což před havárií nebylo standardní [4]. Met Ed ani jednou nepožadovala nezávislé posouzení provozních předpisů.

Výcvik personálu

Kemenyho zpráva konstatovala, že ve výcviku a přípravě operátorů byly závažné nedostatky. Absolvovaný výcvik mohl odpovídat normálním provozním podmínkám, avšak přípravě na možné těžké havárie a havárie s více poruchovými událostmi nebyla věnována dostatečná pozornost. Obsah výcvikových programů nezajišťoval, aby operátoři získali dostatečné porozumění reaktorovým systémům.

Představitel firmy B&W zodpovědný za výcvik byl předvolán k výslechu při vyšetřování havárie TMI-2 jako svědek. Byl hrdý na výcvikový program své firmy za posledních 5 let. Když dostal otázku, co považuje za nejdůležitější úspěch, opakoval: „Než jsem přišel, byla většina výcvikových kurzů zabezpečována inženýry z JE. Inženýři však neumí hovořit způsobem, aby jim lidé mohli rozumět. Proto jsem jako prvé pravidlo zavedl, aby žádný inženýr nebyl oprávněn účastnit se výcviku operátorů“. Podstatným zjištěním, které Kemenyho komise našla bylo, že z výcvikových programů pro operátory byla odstraněna všechna teorie a operátoři byli cvičeni pouze na ovládání tlačítek, což stačilo nanejvýš pro normální provoz. Bylo to však v souladu s požadavky NRC a stalo se to všeobecnou výcvikovou praxí. Procvičovaly se pouze poruchy a havárie způsobené jediným selháním/chybou. Operátoři se nikdy při výcviku nesetkali s havárií, při které se vyskytly dvě nebo více nezávislých selhání/chyb. Při havárii TMI-2 se vyskytla 3 nezávislá selhání.
Musíme poznamenat, že nedostatečný výcvik se netýkal pouze operátorů. Při havárii se

ukázalo, že inženýři a zaměstnanci havarijní jednotky měli též problémy s analýzou události s vodíkovou bublinou, které zmátly i externí experty. I po vstupu vrcholových vedoucích provozu do řízení havárie trvalo ještě dlouho, než byl zjištěn plný rozsah poškození aktivní zóny a bylo stabilizováno její chlazení. Mezi pracovníky, kteří byli na směně při vzniku havárie nebyl ani jeden jaderný inženýr, nikdo z nich neměl vysokoškolské vzdělání a nikdo neměl výcvik pro zvládnutí složitých poruch reaktoru. Nejzávažnějším konstatováním bylo, že většina operátorů a ostatních, kteří byli při havárii, nerozuměli principům provozu JE. Tento nedostatek i u starších operátorů byl příčinou, že zůstali celkem bezradní a nebyli schopni reagovat v situaci, ve které se ocitli.

Výcvikový program s takovými nedostatky přes to všechno tehdy odpovídal nárokům NRC. Kandidáti na operátory v TMI měli dokonce v národním měřítku USA nadprůměrné výsledky při zkouškách pro získání licence NRC a při provozních testech.

Závěrem Kemenyho komise konstatovala, že výcvikové standardy NRC dovolily stát se operátorem i se slabou úrovní výcviku a předepisovaly jen minimum nároků. Nebyly např. stanoveny žádné požadavky na ukončené vzdělání, psychické schopnosti a trestní minulost kandidátů na operátory. Při zkoušce na získání licence nemuseli jednotlivci dokonce uspět při některých částech zkoušky, mezi které patřily i havarijní předpisy a bezpečnostní zařízení a přes to všechno zkoušku složili dosažením stanoveného průměru bodového hodnocení.

NRC tehdy neměla kvalifikační kritéria pro lidi, kteří vedli přípravu operátorů a neměla ani regulérní postup pro hloubkovou kontrolu výcvikových programů.

Sběr a využívání informací

Poučení a poznatky získané z předcházejících havárií a poruch nebyly zpracovány do jednoznačných instrukcí pro operátory. NRC tehdy dostávala enormní množství informací z provozních zkušeností na JE (2 až 3 tisíc hlášení za rok). Před havárií v TMI však neexistovala na NRC žádná systematická metoda pro hodnocení těchto zkušeností a zjišťování varovných signálů možných generických bezpečnostních problémů. V
r. 1978 byla za tento nedostatek NRC kritizována na vysoké vládní úrovni. Náprava tohoto stavu však byla provedena až po havárii TMI-2.

Společnosti GPUCS, Met Ed a B&W nedokázaly u více významných případůnáležitě zanalyzovat, jaké informace z nich potřebují a ani nevěděly, jak je správněpoužít. Svědčí to o tom, že v uvedených společnostech, které budovaly a provozovaly TMI-2 jakož i mezi nimi navzájem, vážně absentovala komunikace o některých kritických bezpečnostních otázkách. Podobný problém existoval i na NRC.

Ukázalo se, že v celém manažérském a kontrolním systému chybělo dotažení věcí do konce. Důležité bezpečnostní problémy byly vyzdvihovány a studovány do jistého stupně, ale ne do konečného řešení. Podle zprávy Kemenyho komise se poznatky z těchto studií nikdy nedostaly k lidem a organizacím, které o nich potřebovali vědět nejvíc.

Proces udělování licence a dozor

Nedostatky v procesu udělování licencí pro JE zabírají velkou část zprávy Kemenyho komise. Většina z nich existovala už při havárii. Je důležité porozumět jim, protože většinu podobných nedostatků lze nalézt i v postupech udělování licencí v jiných průmyslových odvětvích. Některé stejné chyby se opakovaly hlavně při zavádění počítačů do řídících systémů JE a jiných nebezpečných výrobních procesů.

Kemenyho komise konstatovala, že před havárií TMI nevěnovala NRC při udělování licence dostatečnou pozornost prevenci LOCA havárií s malou a střední velikostí úniku chladící směsi. Namísto toho se soustřeďovala jen na velké LOCA havárie. Zvládnutí havárie

na TMI-2 nebylo proto připraveno zejména na možné důsledky značného množství vodíku generovaného při obnažení paliva v aktivní zóně.

Proces udělování licence se soustřeďoval jen na zařízení na základě předpokladu, že přítomnost operátorů na BD může situaci jen zlepšit. Vůbec se neuvažovalo, že operátoři samotní mohou být problémem. Kemenyho komise zdůraznila přetrvávající předpoklad, že JE mohou být dostatečně bezpečné jen při vyloučení zásahu lidského činitele. Proto nebyla v procesech udělování licencí věnována dostatečná pozornost výcviku operátorů a provozním předpisům/procedurám.

Od žadatele licence se vyžadovaly analýzy havárií způsobené jen jedním selháním/chybou. Při udělování licence se nevyžadovalo analyzovat co se stane, když dva anebo více systémy selžou nezávisle na sobě a také se nevyžadovaly havarijní postupy pro tyto situace.

Zařízení se striktně rozdělovala na taková, která jsou bezpečnostně významná a taková, která bezpečnostně významná nejsou. Přísné prověrce a vysokým nárokům při udělování licence podléhala jen bezpečnostně významná zařízení. Ostatní zařízení byla z takové prověrky vyjmuta, ačkoliv v některých situacích mohla mít vliv na jadernou bezpečnost. Toto striktní rozdělení zařízení se ukázalo být nesprávné. Namísto něho by byl vhodnější systém priorit odpovídající důležitosti zařízení a systémy pro bezpečnost JE.

Kemenyho komise zjistila, že neexistovala přesná kritéria pro zařazení zařízení a systémů mezi bezpečnostně významná. Dělalo se to tak, že provozovatel vytvořil svůj návrh zařízení a předložil ho NRC ke schválení. Tak se stalo, že např. na TMI-2 nebyly pojistné ventily zařazeny mezi bezpečnostně významná zařízení proto, že měly zajištěné armatury a zajištěné armatury zase nebyly bezpečnostně významnými zařízeními proto, neboť jim byly předřazeny pojišťovací ventily.

Zavedení umělé kategorie „bezpečnostně důležitých“ zařízení způsobilo, že NRC přehlédla mnohé bezpečnostně významné problémy provozu JE a umožnilo tak jadernému průmyslu splnit poměrně lehce stanovené požadavky dozoru na bezpečnost. Přecenění kategorie „bezpečnostně důležité“ v kontrolních postupech NRC postupněinterferovalo v jaderném průmyslu s povědomím bezpečnosti a potlačilo tak povinnou každodenní starost o bezpečnost celého provozu JE.

V té době mohly elektrárny získat licenci i s několika nevyřešenými bezpečnostními problémy. Dostávaly se tak do stavu určitého zanedbání dozoru, protože jeho pravomoc byla rozdělena do dvou útvarů NRC. TMI-2 měla tento statut v doběhavárie už 13 měsíců po získání provozní licence.

Kemenyho zpráva konstatuje, že na NRC nebylo možné identifikovat žádný útvar odpovědný za přezkoumání inženýringu celého projektu elektrárny, včetně interakcí mezi hlavními částmi a rovněž žádný útvar zodpovědný za odzkoušení interface člověk-stroj na JE.,Dalším problémem uváděným v Kemenyho zprávě bylo primární zaměření firmy NRC pouze na proces udělení licence a že nevěnovala dostatečnou pozornost procesům kontroly zajištění jaderné bezpečnosti v provozovaných JE. Označení problému přívlastkem generický, což znamená, že se týká i mnohých jiných provozovaných JE, se stalo běžnou cestou odložení rozhodnutí o závažných problémech. Generické problémy nemusela elektrárna, která chtěla získat provozní licenci, vyřešit před jejim udělením. JE, které už získaly provozní licence, se bránily prosazování nových bezpečnostních standardů.

Nakonec se ukázalo, že velká část NRC se zaměřovala pouze na to, aby pozornost jaderného průmyslu byla úzce zaměřena na splnění požadavku dozoru a ne na to, aby se rozvíjela systematická péče o bezpečnost. Příkladem toho je už výše uváděná chyba v přípravě operátorů, kteří nebyli připravováni na zvládnutí havárií s více vzájemněnezávislými iniciačními událostmi.

Havarijní plánování

V procesu schvalování výběru lokality pro stavbu TMI požadovala NRC v té doběod žadatele licenční plán pro vnější následky havárie pouze v okruhu o průměru necelých 2 mil od JE. Havarijní ani evakuační plán nebyl v té době požadován. Všeobecně mělo havarijní plánování před havárií TMI na NRC pouze velmi malou prioritu. Kemenyho zpráva tvrdí, že důvodem této nízké priority byla důvěra dozoru v bezpečnost reaktorůa snaha vyhnout se zvýšení obav veřejnosti o bezpečnost jaderné energie. Zpráva rovněž tvrdí, že postoj, který posilovala NRC i společnost Met Ed v lokalitě TMI byl ten, že radiační havárie, která by mohla mít dopad za dvoumílový okruh okolo JE, nemůže být považována za možnou. Havarijní plán TMI nepožadoval, aby společnost uvědomila orgány státní nebo místní správy o případné radiační havárii. Tím bylo způsobeno zpoždění při oznámení události na TMI-2. Společnost Met Ed neoznámila havárii ani svým smluvním lékařům a jejich příprava na poskytnutí zdravotní péče při haváriích nebyla dostatečná. Středisko zdravotní péče pro havarijní situace bylo umístěno v oblasti, která se v prvních hodinách havárie stala neobyvatelnou. Na TMI-2 bylo málo respirátorůa nedostatečné dodávky nekontaminovaného vzduchu. Reakce na havárii byla charakterizována převážně jako totální zmatek a nedostatek komunikace na všech úrovních. Většina z místních komunit okolo TMI neměla detailní havarijní plány. Mnohá klíčová doporučení udělovali lidé, kteří neměli přiměřené informace, a ti, kteří řídili zvládnutí havárie si neuvědomovali dostatečně rychle význam a dopady vzniklé havárie. Skutečnost, že tak velký počet lidí a organizací si vůbec neuvědomoval rozsah a vážnost havárie na TMI-2, svědčí o velkých mezerách a nízké kvalitě připravenosti na havárie v JE.

Kemenyho komise doporučila centralizovat havarijní plánování do jedné agentury na federální úrovni s úzkou koordinací s agenturami na úrovni států. Tato agentura by odpovídala jak za zabezpečení vypracování adekvátních havarijních plánů, tak i za řízení havarijní odezvy. Rovněž doporučila, aby byla změněna pravidla havarijního plánování v lokalitách JE.

Havárie v jaderné elektrárněČernobyl

Zprávu o tragédii v Černobylu přednesli zástupci tehdejší SSSR na konferenci expertů věnované havárii v Černobylu uspořádané Mezinárodní agenturou pro jadernou energii (IAAE) v srpnu v r.1988. Zpráva (382 stránková) podala přehled všech konstrukčních a provozních nedostatků, které vedly k havárii.

Charakteristika JE Černobyl a průběh havárie

Jaderný energetický reaktor RBMK-1000 (Reaktor Boĺšoj Moščnosti Kanálnyj) je heterogenní, grafitem moderovaný, varný, lehkovodní, kanálový reaktor na tepelné neutrony, v kterém se jako palivo používá slabě obohacený uran U235. Tepelný výkon reaktoru je 320 MW. Palivové články jsou vloženy do válcových palivových kazet umístěných v individuálních vertikálních kanálech. Aktivní zóna se skládá z grafitových bloků sestavených do tvaru válce s průměrem 12 m a výškou 7 m. Je umístěna v hermetických prostorech vytvořených válcovou šachtou se spodní nosnou konstrukcí a horním ocelovým pláštěm. Stínění reaktoru tvoří beton, ocelový plášť, písek a voda.

Předností tohoto typu reaktoru jsou následující konstrukční a provozní vlastnosti:

- Konstrukce reaktoru nevyžaduje výrobně náročná rozměrná tělesa (tlakovou nádobu reaktoru), která omezuje jeho jednotkový výkon a vyžaduje speciální výrobní základnu (která v bývalém SSSR neexistovala).
- Reaktor umožňuje kontinuální výměnu paliva během provozu a má příznivou neutronovou bilanci.

- Reaktor dovoluje realizovat pružný palivový cyklus, který lze dobře přizpůsobit změnám na trhu paliva.
- Poskytuje možnost jaderného přehřívání páry.
- Lze kontrolovat parametry chladící směsi v jednotlivých kanálech.
- Existují zkušenosti s výrobou zařízení a výstavbou JE s tímto reaktorem.

K nedostatkům patří:

- Možnost samovolného nárůstu rychlosti řetězové štěpné reakce vlivem odpařování chladící směsi v aktivní zóně (kladný zpětnovazebný koeficient reaktivity), který má za následek rychlé zvýšení výkonu.
- Složitý systém řízení pro stabilizaci rozložení výkonu v aktivní zóněa vysoká citlivost neutronového toku vůči poruchám.
- Složitost a velká rozčleněnost (1690 tlakových kanálů) chladícího systému.
- Velké množství tepelné energie akumulované v grafitu.
- Mírně radioaktivní pára v sekundárním okruhu.

Potrubí pod reaktorem je v hermetických boxech, které jsou propojené do velkého barbitážního vodního bazénu umístěného pod celou budovou. V případě prasknutí kterékoliv potrubí se unikající pára odvede do bazénu pod vodní hladinu, kde se zkondenzují a zachytí radioaktivní částice v ní obsažené. Parní potrubí nad aktivní zónou bylo uvnitř obyčejných výrobních prostorů elektrárny a proto, pokud by některá z nich praskla, došlo by k uvolnění radioaktivní páry do těchto prostor. Rusové se v té doběspoléhali na prevenci a zmírňování následků havárie a budovali jen částečné kontejnmenty (barbitážní systémy). Po havárii na TMI začali i oni budovat v reaktorech kontejnmenty. Reaktor RBMK je ovládán 211 radiačními tyčemi. Velký počet těchto tyčí kompenzuje malou rychlost jejich zasouvání do aktivní zóny (AZ). Účinnost tyčí je velmi závislá na hloubce jejich zasunutí. Obzvlášť nízká je na počátku zasunutí do AZ. Úplné zasunutí radiačních tyčí do AZ trvá 20 sekund. Kladný zpětnovazebný koeficient reaktivity znamená, že se výkon reaktoru zvyšuje, když přítok vody klesá, na rozdíl od většiny reaktorů. V reaktorech tlakovodního typu (PWR) se voda používá jako moderátor a bez ní se řetězové štěpení reakce zastaví. Produkce přebytečného tepla v palivu pokračuje i v těchto reaktorech a jak je výše popsané, způsobila havárii TMI-2 [4].

Voda v RBMK se používá jen na odvod tepla z AZ. Zachytává některé neutrony, čímž zabraňuje jejich účasti na další štěpení. Když začne vřít a zmenší svou specifickou hustotu, neutrony, které by se v ní zachytily, přejdou do grafitu a po zmoderování se podílí na dalším štěpení. Tímto způsobem absence vody zvyšuje reaktivitu a početnost štěpení – výkon. Ovládání tohoto pozitivního zpětnovazebného koeficientu reaktivity zabezpečuje komplexní počítačový řídící systém, který umožňuje provádět operativní výpočty pro zabezpečení teplotechnické spolehlivosti bloku v režimu kontinuální výměny paliva při libovolném otevření regulačních ventilů chladící vody na vstupu do každého kanálu. Zkušenosti z tohoto provozu reaktorů RBMK ukazují, že udržování teplotního režimu paliva, grafitu a rezervy do kritického varu jsou zvládnuty na dobré úrovni.

Reaktor RBMK má dvě hlavní cirkulační kličky se čtyřmi hlavními cirkulačními čerpadly na každé z nich (3 pracující, 1 rezervní). Havarijní chladící čerpadla nabíhají za 10 až 20 sekund po výpadu hlavních čerpadel. Systém havarijních čerpadel tvoří 3 okruhy s vysokotlakým a nízkotlakým čerpadlem. Chladící voda je čerpána z barbitážního bazénu. Pro zajištění rychlého doplnění chladící směsi do poškozeného okruhu jsou připojeny tlakové hydroakumulátory. Pára z reaktoru pohání dvě turbíny.

Vlastní spotřeba elektrické energie při provozu JE nemůže být zajištěna jen vyráběnou elektřinou. Je nevyhnutelné, aby každá elektrárna měla samostatné elektrické vedení

z elektrizační soustavy, které slouží jako rezervní napájení. Už kvůli kladnému zpětnovazebnému koeficientu reaktivity v reaktorech BMK musí být elektrické napájení havarijních čerpadel trvale zajištěno.

Rusové konstruovali své JE s vyloučením současného vzniku havárie a ztráty elektrického napájení vlastní spotřeby. Pokud je odstavení reaktoru téměř okamžité, nemůže být vlastní spotřeba zajišťována samotnou elektrárnou. Musí se použít buď už rezervní napájení z jiných zdrojů/elektráren anebo z jiných bloků v dané lokalitě, pokud existují a jsou v provozu. Kromě těchto možností se vyžaduje ještě další zvláštní úroveňzajištění vlastní spotřeby, kdyby předcházející zdroje selhaly. Tato úroveň je zabezpečena diesel-generátory instalovanými na JE. V USA se požaduje, aby tyto dieselgenerátory dosáhly svůj plný výkon do 10 sekund od startu. Rusové prohlašovali, že jejich diesel-generátory dosáhnout plný výkon za 15 sekund., avšak ve zprávě, kterou přednesli ve Vídni uvedli, že potřebovali další zdroje elektřiny pro přibližně 45 sekund od odstavení reaktoru. Pro zajištění dodávky této energie se rozhodli využít setrvačnost turbíny. Experiment, který vyústil do havárie, byl plánován pro ověření toho, jak dlouho může setrvačnost dobíhající turbíny zásobovat elektřinou hlavní čerpadla.

Osudný experiment byl naplánován na den 25. dubna r. 1986 před odstavením 4. bloku na plánovanou revizi. Cílem experimentu bylo ukázat, že nově navržený systém regulace napětí na generátoru je schopen spolehlivě zásobovat elektrickou energií rychločinné čerpadlo systému havarijního chlazení po dobu 40-50 sekund při doběhu turbogenerátoru (TG) po jeho odstavení rychločinnou uzavírací armaturou. Předcházející testy s původním regulátorem byly neúspěšné, protože pokles napětí byl při doběhu TG příliš rychlý.

Elektrická zátěž čerpadla havarijního chlazení měla být simulována napájením většího počtu hlavních cirkulačních čerpadel, než jsou normálně napájeny z TG. Experiment byl jednoznačně považován za elektrickou záležitost nevýznamnou z hlediska jaderné bezpečnosti. Z tohoto důvodu experiment řídili specialisté na část elektro. Na jadernou bezpečnost se kladl minimální důraz a vlastní program experimentu nebyl schválen dozorovými orgány. Havárie by však nenastala, kdyby nedošlo k nepředvídanému nahromadění dalších problémů a vážných chyb.

- Experiment se skládal z následujících základních kroků:
- Snížení výkonu reaktoru na úroveň 700-1000 MW.
- Odpojení systému havarijního chlazení k zabránění jeho falešného působení během testu.
- Přepojení napájení hlavních cirkulačních čerpadel tak, aby byla 4 čerpadla napájena z venkovní sítě a 4 z TG č. 8.
- Odstavení TG č. 8.

Příprava na experiment začala v 01.00 hod. 25. dubna pomalým snižováním výkonu reaktoru. Ve 13.05 hod. dosáhl výkon reaktoru hodnotu 50 % a TG č. 7 byl odstaven. Krátce potom byl odpojen systém havarijního chlazení. Na žádost blokové dozorny (BD) však bylo další snižování výkonu pozastaveno takřka na 9 hod. Během celých těchto 9 hod. zůstal systém havarijního chlazení odpojený.

I když průběh dalších událostí nebyl tímto odstavením havarijních čerpadel významně ovlivněn, skutečnost, že systém havarijního chlazení nebyl znovu připojen, odráží postoj provozního personálu k dodržování provozních předpisů. Další snižování výkonu začalo ve 23.10 hod., přičemž došlo k další neobvyklé události. Při přepnutí řízení reaktoru z lokálního systému na globální systém nebyl splněn požadavek nutného setrvání na výkonové hladině, následkem čehož výkon reaktoru prudce klesl pod minimální úroveň 700 MWt stanovenou pro experiment. V důsledku významné redukce objemu páry v chladící směsi byl zpětnovazebným účinkem na reaktivitu výkon snížen až na úroveň 30 MWt. V této situaci mohl být výkon reaktoru zvýšen na 200 MWt jen pomocí ručního vysunutí regulačních tyčí.

V režimu výkonu pod 700 MWt je vztah mezi základními veličinami reaktoru silněnelineární, tzn., že malé změny výkonu způsobují značné změny objemu páry v chladící směsi, čímž se řízení výkonu a průtoku napájecí vody v reaktoru stává mimořádnětěžkým. Vytažení velkého počtu řídících tyčí z AZ při malém výkonu reaktoru znamenalo porušení provozních předpisů (limitů a podmínek bezpečného provozu reaktoru). Vznikly tím podmínky, které urychlily odezvy reaktoru a snížily účinnost ochranného systému.
Poloha řídících tyčí je pro odezvu reaktoru podstatná. Čím větší počet je jich z AZ vytaženo, tím větší hodnoty nabývá kladný zpětnovazebný koeficient reaktivity a tím citlivější je reaktor na jakékoliv změny, které vedou ke změně objemu páry v chladící směsi AZ. Při změnách výkonu modifikují ohřev paliva a přestup tepla do chladící směsi rychlost růstu výkonu. Zpětnovazebný teplotní koeficient paliva je záporný a výsledný efekt růstu teploty paliva a dodatečné zvýšení objemu páry je závislé na velikosti výkonu. Při provozu na nominálním výkonu je výsledný zpětnovazebný efekt vlivu na reaktivitu negativní. Pozitivním se stává pod úrovní 20 % nominálního výkonu.

Reaktor byl na výkonu 200 MWt , což je úroveň, při které je jeho ustálený provoz zakázán. Operátoři se přesto rozhodli v experimentu pokračovat, ačkoliv to bylo nejvýznamnějším porušením provozních předpisů. Sama o sobě by tato skutečnost ještěnebyla postačující pro vznik havárie. Přispěly k tomu další okolnosti.

Podle programu experimentu připojili operátoři v 01.03 hod. a 01.07 hod. dne 26. dubna 1986 záložní hlavní cirkulační čerpadla, protože byl v chladící směsi reaktoru nízký obsah páry a tím i snížený hydraulický odpor systému. Připojení čerpadel zvýšilo celkový průtok chladící směsi reaktorem nad dovolené hodnoty.

Takový provozní režim je podle provozních předpisů také zakázán vzhledem k nebezpečí přerušení dodávky vody a možnosti vzniku vibrací potrubních tras a čerpadel v důsledku kavitace. Dodatečné připojení hlavních cirkulačních čerpadel a tím i následné zvýšení průtoku chladící směsi reaktorem způsobilo snížení tvorby páry, snížení tlaku v separátorech a změnu dalších parametrů. V 01.19 hod. byla hladina vody v separátorech páry blízko limitní přípustné hodnotě. Operátoři proto zvýšili průtok napájecí vody. Zvýšený přítok vody do separátorů způsobil další snížení obsahu páry v chladící směsi, což se projevilo zvýšením záporné reaktivity. Vyvolanou zápornou změnu reaktivity (snížení výkonu) se pokusil kompenzovat automatický systém řízení. Pro udržení výkonu však bylo potřebné další ruční vytažení regulačních tyčí ze zóny. Tlak chladící směsi v systému začal klesat a ve snaze ho stabilizovat, uzavřeli operátoři přepouštěcí stanici páry do kondenzátoru. Vzhledem k problémům, které vznikly při udržování hladiny a tlaku chladiva v separátorech, odpojili operátoři havarijní signály od těchto parametrů, což bylo dalším hrubým porušením provozních předpisů.

Popis dalšího průběhu událostí při havárii v Černobylu vychází ze závěrůsovětských specialistů odvozených z matematického modelování přechodových procesův reaktoru. Když operátoři usoudili, že hladina vody v parních separátorech je už dostatečně vysoká, rázně snížili průtok napájecí vody. To způsobilo zvětšení objemu páry a vneslo zpětnovazebnou kladnou reaktivitu (zvýšení výkonu reaktoru), kterou automatická regulace ve snaze udržení konstantního výkonu okamžitě začala kompenzovat zasouváním regulačních tyčí. Před začátkem experimentu si operátoři nechali vypsat z počítače rozložení neutronového toku v AZ. Na základě tohoto výpisu bylo jasné, že z AZ bylo vytaženo příliš mnoho regulačních tyčí a že zásoba reaktivity pro havarijní odstavení reaktoru byla nepostačující. V tomto momentu měli operátoři odstavit reaktor, rozhodli se však pokračovat v experimentu. Provozní zásoba reaktivity na odstavení reaktoru je 30 řídících tyčí ruční regulace. Při 15 se musí reaktor odstavit. V daném stádiu experimentu byla zásoba reaktivity jen asi 6-8 řídících tyčí.

Pro případ neúspěchu experimentu si operátoři chtěli ponechat možnost jeho zopakování a proto odpojili (deblokovali) i havarijní ochranu od výpadku 2. TG (č. 8), která by odstavila reaktor po zavření rychločinných armatur u přívodu páry do turbíny. To bylo rozhodující hrubé porušení programu experimentu, protože při těchto ochranách by se byl reaktor bezpečně odstavil hned na samém začátku experimentu i při dané konfiguraci řídících tyčí. V tomto okamžiku byly do havarijní ochrany reaktoru zavedeny jen signály na převýšení výkonu a povolené periody.

Práci operátorů během testu řídil na BD zkušený technolog, který později přiznal, že jeho konceptuální model provozní fyziky reaktoru, na základě kterého vydal příkazy porušující provozní předpisy, byl chybný. Osvojil si ho ze studia provozní dokumentace a s trpkostí konstatoval, že na některá fakta o fyzice reaktoru ho nikdo před havárií neupozornil.

Vlastní experiment začal v 01.23,04 hod.

Uzavřením rychločinné uzavírací armatury přívodu páry do TG č. 8 začal tlak páry v separátorech růst, průtok chladící směsi AZ začal klesat, protože 4 hlavní cirkulační čerpadla dobíhala společně k dobíhajícím TG, ze kterého byla napájena. Rostoucí tlak chladící směsi v reaktoru, snížený průtok napájecí vody a redukovaný průtok chladící směsi reaktorem jsou rozhodujícími faktory, které ovlivnily objemový obsah páry (parních bublin) v chladící směsi a tím přes kladný zpětnovazebný koeficient reaktivity i výkon reaktoru. Je důležité opět zdůraznit, že se reaktor nacházel v takovém stavu, kdy i malé změny výkonu způsobují značné změny objemového obsahu páry a následné zvýšení výkonu reaktoru. Kombinace těchto faktorů vedla k nárůstu výkonu, který začal v 01.23,30 hod.

Operátor proto v 01.23,40 hod. stiskl tlačítko havarijní ochrany reaktoru, ale to už bylo v tomto okamžiku příliš pozdě. Řídící tyče, které byly v AZ, neměly dostatečnou zásobu reaktivity a tyče, vytažené ze zóny do ní nemohly být zasunuty dostatečně rychle, aby zabránily vyvolanému růstu výkonu. Podle výpočtů dosáhl výkon reaktoru za 3 sekundy hodnotu 530 MW a perioda zvyšování výkonu reaktoru klesla hluboko pod hodnotu 20 sekund.

Automatické havarijní signály pro odstavení reaktoru od výkonu a periody přišly také příliš pozdě na to, aby mohly účinně zapracovat. Kladný parní zpětnovazebný koeficient reaktivity reaktoru RBMK způsobil trvalý růst reaktivity nad kritickou hodnotu reaktoru na okamžitých neutronech. Výpočtem bylo odhadnuto, že v průběhu 4 sekund po 01.23,40 hod. dosáhl výkon reaktoru hodnotu převyšující 100 násobek nominálního výkonu.Tento katastrofální exkurz výkonu reaktoru způsobil destrukci paliva, prudkou tvorbu páry a následnou destrukci AZ a celé konstrukce reaktoru.

Rychlý průběh destrukce v prvních sekundách havárie, vysoká úroveň radiace a vysoké teploty znemožnily přímé měření v dalších okamžicích havárie. Další popis událostí proto vychází z vizuálních pozorování, měření úrovně radiace a z poznatkůz předcházejících experimentů s diesel-generátory a z výpočtů provedených po havárii. Pro získání detailnějšího obrazu o průběhu havárie v Černobylu a z průvodních jevů jsou nutné další analytické a experimentální studie vypočítaných analýz poškozených materiálů.

Nyní jsou známa tato fakta:

- Nastala první exploze, při které byly do okolí budovy reaktoru vyvrženy materiály z AZ.
- Při druhé explozi došlo k vyvržení paliva a grafitu.
- V okolí budovy reaktoru se našly grafitové bloky a úlomky paliva.
- Došlo k značnému poškození budov elektrárny.
- Mostový jeřáb v budově reaktoru a zavážecí stroj se zřítily.

- Horní betonová deska reaktoru byla nazdvižena a přesunuta dovnitřreaktorové haly.
- Poškodily se všechny kanály AZ.
- Štěpná řetězová reakce se zastavila.

S těmito skutečnostmi se spojují následující úvahy. Velký vklad kladné reaktivity způsobil extrémní uvolnění energie v palivu. Rozpálené palivo a grafit reagovaly s okolní vodou a následný vznik páry způsobil nárůst tlaku. Přetlak a vývin tepla vedly k prasknutí většího počtu palivových kanálů. Při první explozi došlo k rozptýlení úlomků materiálu (asi 30 % paliva se roztříštilo) a k poškození střechy reaktorové haly. Hermetický prostor reaktoru, který je projektován na prasknutí jenom jednoho kanálu, byl tak natlakovaný, že se nazdvihla horní betonová deska reaktoru s hmotností asi 1000 tun. V tomto momentu došlo k prasknutí všech kanálů, k vystřelení regulačních tyčí a odtržení horizontálních potrubí. Druhá exploze nastala asi 2 až 3 sekundy po první. Doposud není jasné, zda její příčinou byla reakce vzniklého vodíku se vzduchem anebo to byl důsledek druhé výkonné exkurze. Při ní bylo rozptýleno asi 25 % grafitových bloků a materiálu palivových kanálůa praskly stínící vodní nádrže].

Operátorům se podařilo zajistit pomocí havarijních napáječek vstřik vody do separátorů páry a kolektorů mezi separátory a čerpadly. Asi půl dne tam byla dodávána voda průtokem 200 až 300 tun za hodinu. Zdrojem vody byla nádrž havarijní zásoby
3. bloku černobylské JE. Část vody se odpařila a zbytek vytékal směrem k 1. a 2. bloku.

První upozornění ze zahraničí, že něco není v pořádku, přišlo ze Švédska [48]. Když přicházeli pracovníci JE Forsmark nacházející se severně od Stockholmu na ranní směnu v pondělí 28.dubna, indikoval u nich detektor radiace zamoření. Z obavy, že došlo k úniku z jejich elektrárny byl odstaven reaktor a elektrárna uzavřena. Pozdější testy ukázaly, že radiace nepochází z JE Forsmark a ani z jiných reaktorů ve Švédsku.

Švédové okamžitě upozornili Američany, kteří si zpočátku mysleli, že radioaktivita náhodně unikla z ruského podzemního testu jaderné zbraně do atmosféry. Odpoledne švédští vědci identifikovali složky radioaktivity a zjistili, že musí pocházet z reaktoru a ne z testu jaderné zbraně. Byli schopni určit, že radioaktivita pochází přinejmenším z částečně roztavené aktivní zóny reaktoru. Podle času, když radioaktivní mrak dosáhl jejich pobřeží a podle rychlosti a směru větru dokázali zpětně vystopovat jeho trasu ve směru přes Lotyšsko a Minsk do Kyjeva.

Švédští diplomati požádali ruskou stranu o vysvětlení a bylo jim řečeno, že neexistují žádné informace. Večer ve 21.00 hod. odvysílala sovětská televize zprávu, že v Černobylu došlo k havárii a že jeden z reaktorů byl zničen. Byla přijata opatření pro odstranění následků havárie a postiženým byla poskytnuta pomoc. Na vyšetření havárie byla ustanovena vládní komise. K tomuto oznámení bylo připojeno jenom několik doplňujících informací, což bylo tehdy běžnou praxí při všech jaderných událostech ve světě.

30. dubna už věděly i jiné státy, že radioaktivní mrak z černobylské havárie zanesl radioaktivní materiály na jejich území. V některých zemích byl zakázán prodej mléka, byla vydána upozornění, aby obyvatelé nepili vodu a byly rozdávány jodové tabletky.

Při havárii bezprostředně zahynulo na nemoc z ozáření 31 zaměstnancůelektrárny a hasičů. Přibližně tisíc rodin, které žily v elektrárenském městečku v okruhu 1 míle od elektrárny bylo evakuováno 12 hod. po explozi. Evakuace blízké vesnice Pripjaťa 71 dalších osad v okruhu 18 mil od elektrárny začala následující den. Počet úmrtí následkem havárie v Černobylu vzrostl přibližně na 42 osob, celkový počet úmrtí anebo rakovinových onemocnění z této havárie je prakticky nezjistitelný.

Příčinné faktory havárie – druhá úroveň

Na konferenci ve Vídni zdůraznili sovětští specialisté především tyto podmínky zavinění havárie:

Provedení testu bylo stanoveno před plánovaným odstavením bloku do běžné údržby, čímž se operátoři dostali pod mimořádně velký tlak. Pokud by se nepodařilo provést test úspěšně tehdy, potom by se muselo čekat na jeho provedení až do dalšího odstavení reaktoru, ke kterému by došlo za rok o rok.

Čtvrtý blok JE Černobyl byl vzorovým blokem, který dosahoval nejlepší provozní výsledky ze všech provozních reaktorů typu RBMK.

Ttest byl pojímán jako zkouška zařízení elektro a ne jako jaderný test. Doposud byl vždy proveden bez jakékoliv události. Operátoři proto nevěnovali dostatečnou pozornost efektům, které měly na reaktor vliv.

Existuje vážné podezření, že na provedení testu dohlíželi namísto operátorů zástupci výrobce turbíny.

Na kladný zpětnovazebný koeficient reaktorů RBMK upozorňovali sovětskou stranu britští specialisté už dávno a tvrdili, že je to vážná konstrukční chyba, která dělá práci operátorůmimořádně těžkou.Operátoři reaktoru RBMK měli minuty a možná jen sekundy na zareagování v kritických situacích.

Pro postavení reaktorů typu RBMK namísto bezpečnějších tlakovodních (PWR) se v Sovětském svazu rozhodli s největší pravděpodobností z vícero důvodů. Jeden z nejdůležitějších důvodů byl, že chtěli získávat plutonium a zároveň i vyrábět elektrickou energii v jednom jaderně energetickém zařízení. Dalším faktem bylo, že v té době nebyli schopni vyrobit velké tlakové reaktorové nádoby a ani tlakové nádoby pro parní generátory, jaké jsou potřebné pro reaktory typu PWR. Reaktor RBMK takovéto nádoby nepotřebuje. Později začali i v SSSR stavět reaktory typu PWR.

Černobylský reaktor neměl kontejnment, ale jen hermetické boxy s ventilací a filtry. V případě uvolnění radioaktivních plynů měly filtry zachytit radioaktivní části před jejich vypuštěním. Stavebně nebyly hermetické boxy projektovány na tak velký přetlak, jaký vznikl při havárii.

Příčinné faktory havárie – třetí úroveň

Projektová ovladatelnost reaktorů RBMK

Oficiální závěr sovětské strany k černobylské tragédii byl, že ji zavinili operátoři.Vědečtí pracovníci a specialisté z jiných států, kteří se zúčastnili minulé konference o Černobylu ve Vídni se s tímto tvrzením neztotožňovali. Souhlasili, že bezprostřední příčinou havárie byly zásahy operátorů, ale tvrdě dokazovali, že prvním faktorem byl projekt reaktoru RBMK s možnou kladnou zpětnou vazbou, která ho dělala těžko ovladatelným. Lord Marschall, předseda představenstva anglické elektrárenské společnosti říkal, že jeho vláda varovala představitele SSSR před tímto efektem už před 9 roky. Bylo jim tehdy řečeno, že jakýkoliv reaktor je bezpečný, pokud má dostatečné množství rozumných operátorů. Projektanti reaktoru RBMK však dali operátorům příliš těžkou úlohu. Lord Marschall vyhlásil, že RBMK si Sověti vybrali jen z důvodů úspory nákladů. Určitě věděli, že tento reaktor má nedostatky, mysleli si však, že je možné je kompenzovat. Dodal, že teď už nemá smysl rozebírat pozadí, protože rozhodnutí o stavbě reaktorů typu RBMK bylo předtím přijato. Vedoucí sovětské delegace odpovídal, že nevěděl o britském varování z r. 1977. Odmítl porovnávat kvalitu černobylských reaktorů s reaktory západními a řekl, že havárii způsobila série nepochopitelných a nepřípustných chyb operátorů.

Když dojde k těžkým haváriím, stane se tak vždy do té doby nepředvídaným způsobem – to je právě dělá těžkými. Avšak skutečnost, že nejsou předvídány přesné jevy vedoucí k havárii neznamená, že neexistuje jejich prevence. Nebezpečí jsou běžněznáma a opatření pro jejich eliminování/redukování můžeme vždy přijmout. Události, které se staly v Černobylu, nemusely být nutně predikovány, aby se vědělo, že konstrukce reaktoru RBMK dělá práci operátorů mimořádně těžkou. Během provozu reaktoru se vždy může přihodit několik událostí, které vyžadují ruční manipulace operátorů pod stresem. Je to podobné tomu, když během životnosti nadzvukových letadel mohou nastat události, které zapříčiní kolaps podlahy kabiny. V obou případech bylo rozhodnuto eliminovat takové události, protože to vyžadovalo upřednostnění jiných cílů jako např. nižší náklady anebo požadovaná funkcionalita. Nevyhnutelnost provádět rozhodnutí při takových faktech vede k většině těžkostí při řešení bezpečnostních problémů.

Výcvik operátorů

Operátoři a ostatní provozní personál nebyli připraveni rozumět a zvládnout technologické procesy v jaderném reaktoru. Přestali také vnímat existující nebezpečí. Navíc, podobně jako na TMI, ani operátoři v Černobylu neměli výcvik na simulátoru pro typ havárie, ke které došlo.

Schválení procedury vykonání testu

Ve zprávě sovětských specialistů je napsáno, že ani s hlavním inženýrem elektrárny v Černobylu a ani s lokálním inspektorem jaderného dozoru nebyl postup provedení testu konzultován a procedura testu nebyla prověřena specialisty na bezpečnost a jadernými inženýry a fyziky.

Sebeuspokojení

Sověti přiznali, že operátoři v Černobylu propadli značnému sebeuspokojení. Elektrárna fungovala tak dobře, že začali být příliš uvolnění a zaspali v nejnebezpečnějším postoji, že k havárii nemůže dojít. [4]. Jeden z amerických pozorovatelů ve Vídni konstatoval, že Sověti tehdy skutečně nevěřili, že by reaktor mohl havarovat.

Taktéž přiznali, že se hodně poučili z toho, co bylo v USA po TMI učiněno: potřeba lepšího výcviku operátorů na simulátorech, včetně scénářů havárií s více nezávislými událostmi, nevyhnutelnost mít ověřené postupy testů příslušnými odborníky pro jejich vykonání a potlačení nebezpečí a sebeuspokojení. Mnohým škodám v Černobylu se dalo vyhnout, kdyby byli Sověti věnovali větší pozornost zjištěním z TMI. To bohužel platí pro většinu průmyslových odvětví a převážnou většinu havárií. Učení se z chyb druhých se zdá být těžké.

Černobyl z pohledu roku 2005

V září r. 2005 se v sídle Mezinárodní agentury pro atomovou energii ve Vídni konala třídenní mezinárodní konference Černobylského Fóra. Odborníci z OSN na ní prezentovali 600 stránkovou zprávu o vlivu černobylské katastrofy na životní prostředí a na zdraví obyvatelstva, pod kterou je podepsaných 100 vědců z celého světa.

Na této konferenci o Černobylu se zajímavě vyjádřil Ing. Václav Hanuš, předseda České nukleární společnosti: „Od černobylské události v r. 1986 už uplynulo více než 19 let a odborníci už mohli seriózně vyhodnotit její dlouhodobé dopady na životní prostředí a zdraví obyvatelstva. Prezentované výsledky výzkumu např. říkají, že zhoubných nemocí bylo a je v populaci zasaženo černobylskou havárií úplně stejně, jako kdekoliv jinde na světě. Výjimkou je rakovina štítné žlázy, na kterou v okolí Černobylu zemřelo 9 osob. Zdá se tedy,

že „memento Černobyl“, kterým odpůrci jaderné energie děsí laiky a straší politiky, je jen obrovskou bublinou“.

Podle Ing. Hanuše je možné hlavní závěry vědeckých výzkumů prezentované na konferenci shrnout do 4 základních bodů:

- Radiací s vážnými zdravotními následky byli postiženi jen záchranáři a dělníci, kteří se bezprostředně podíleli na hašení bloku. Počet úmrtí takto zasažených osob byl stanoven na 59.
- Pro obyvatele platí, že se nepotvrdilo žádné zvýšení počtu rakoviny, leukémie či nerakovinových onemocnění, které by způsobila radiační zátěž z Černobylu. Výjimkou je rakovina štítné žlázy, kde počet úmrtí dosáhl doposud 9 případů.
  Zdravotní rizika z kouření a nadměrného požívání alkoholu jsou mnohonásobněvyšší než rizika plynoucí z černobylské radiační zátěže. Na druhé straně nikdo bohužel nekvantifikoval počet zachráněných životů při nadstandardní zdravotní péči, která byla zkoumáním populace věnována.
- Dopady na životní prostředí mimo 30 km zakázaného pásma v okolí elektrárny jsou prakticky neměřitelné. Situace se nyní natolik zlepšila, že je možné přistoupit k výraznému zmenšení zakázaného pásma.
- Černobyl byl více sociální katastrofou než radiační. Sociální problémy spojené s evakuací, přesídlením a ztrátou zaměstnání v podmínkách rozpadlého SSSR jsou těmi nejtěžšími.

Na konferenci ve Vídni byly rozebírány dva dopady Černobylu na jadernou energetiku. Bylo konstatováno, že černobylská tragédie měla negativní i pozitivní dopad na rozvoj světové jaderné energetiky. V některých státech zapůsobil Černobyl extrémněnegativně. Především v Itálii a Německu se stal doslova obuškem, kterým zelení dotlačili vládu k odklonu od jaderné energetiky a k okamžitému resp. postupnému zavření JE. Bude zajímavé, jak se na základě výsledků vídeňské konference vypořádají zelení s „černobylskou bublinou“.

Na druhé straně měl Černobyl pro jadernou energetiku i pozitivní dopad. Za největší přínos této havárie se považuje založení organizace WANO – Světová organizace provozovatelů JE. Posilnila se pozice státních dozorů nad jadernou bezpečností a bezpečnost JE se od té doby mnohonásobně zvýšila po stránce technické a hlavně po stránce organizační a personální, tvrdí Ing. Václav Hanuš.

Z výsledků vědeckých studií dvacetiletého vývoje po události v Černobylu je zřejmé, že se jaderná katastrofa apokalyptických rozměrů, jak ji popisovali příslušníci Greenpeace, ve skutečnosti, nestala.

Spolehlivost lidského činitele
Vydal: Výzkumný ústav bezpečnosti práce, v.v.i., Jeruzalémská 9, Praha 1
Rok: 2008
Náklad: 200 výtisků
Vydání: první
Zpracovali: Ing. Miloš Paleček, CSc. RNDr. Sranislav Malý, Ph.D., Ing. Adam Gieci
Tisk: Repronis s. r. o., Teslova 873/2, Moravská Ostrava

ISBN 978-80-86973-28-9

Výzkumný ústav bezpečnosti práce, v.v.i.
Praha 2008