Jak a kdy používat jednotlivé koncepty řízení a vypořádání rizik
How and when individual concepts of management and trade-off with risks may be used

Dana Procházková

Abstrakt
Článek předkládá posouzení konceptů práce s riziky, které jsou používány v manažerských a inženýrských disciplínách s cílem zajistit bezpečí pro lidi prostřednictvím zajištění bezpečných budov, bezpečných území a bezpečných lidských komunit, zvažovaných jako systémy. Jednotlivé koncepty předmětných disciplín plní různé cíle, jsou založeny na různých předpokladech, mají různé nároky na znalosti, data, síly, zdroje a prostředky, a proto zahrnují různá opatření a činnosti při realizaci v praxi. Šetření, jehož výsledky jsou dále uvedeny, umožňuje rozdělit úkoly v praxi do skupin tak, že je zřejmé, kdy je nutné použít velmi pokročilé postupy a kdy jsou jednoduché postupy dostatečné. Zvláštní pozornost je věnována inženýrské oblasti a případům, v nichž je nutno uplatnit pokročilé postupy pro zajištění bezpečnosti jak systému systémů, tak i okolí systému systémů.

Abstract
The paper passes judgement of concepts of work with risks that are used in managerial engineering disciplines directed to ensure the security for humans through ensuring the safe of buildings, safe territories and safe human communities considered as systems. Individual concepts of these disciplines fulfil different goals, are based on various assumptions, have different demands on knowledge, data, forces, sources and means, and therefore, they involve different measures and activities for implementation in practice. The investigation, the results of which are furthermore presented, enables to split up tasks in practice into groups by the way that it is evident when it is necessary to use very advanced procedures and when simple ones are sufficient. The special attention is paid to engineering domain and to cases in which advanced procedures may be used for ensuring the safety of both, the system of systems and the system of systems´ vicinity.

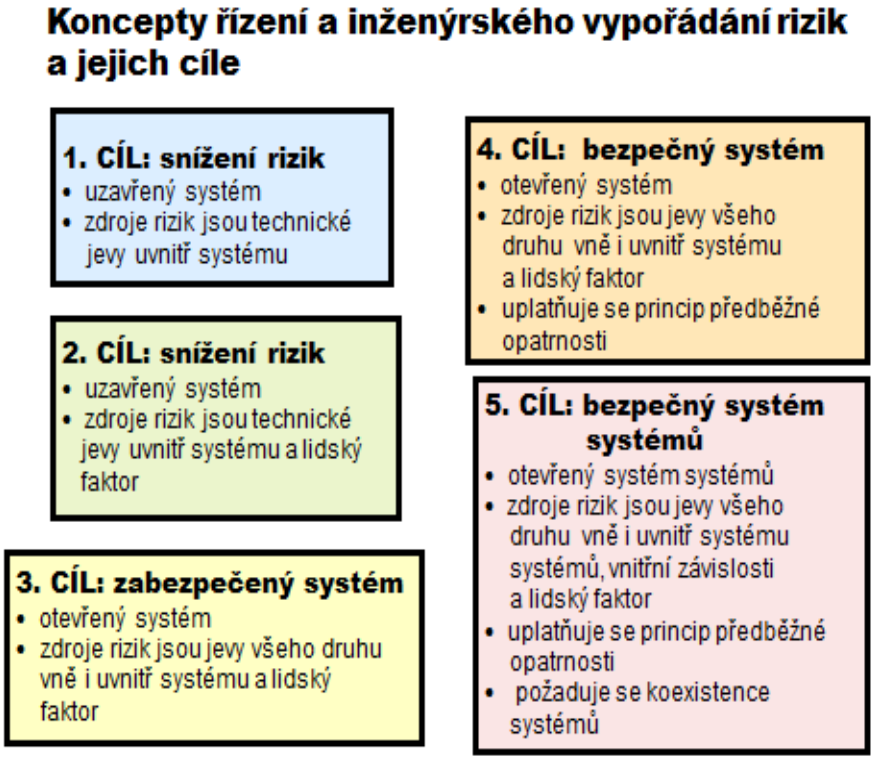
Klíčová slova
řízení rizik; rizikové inženýrství; bezpečnostní inženýrství; inženýrství bezpečnosti; bezpečnost procesu; bezpečnost systému

Keywords
risk management; risk engineering; security engineering; safety engineering; process safety; system safety

Úvod

Současným cílem lidí je žít v bezpečném prostoru. OSN [1] formulovala cíl lidské společnosti jako bezpečný lidský systému a EU [2] ho formulovala jako bezpečnou komunitu. Cílem obou konceptů je zajistit pro lidi existenci, bezpečí a potenciál pro rozvoj. Základní nástroje lidské společnosti pro dosažení uvedených cílů jsou řízení lidské společnosti a správné uplatňování znalostí a zkušeností při vyjednávání s riziky tak, že se respektuje veřejný zájem. V předmětném ohledu hrají velkou roli manažerské a inženýrské disciplíny, jejímž cílem je

zajistit lidskou existenci, bezpečí a potenciál pro rozvoj. Současné poznání ukazuje, že to znamená postarat se o veřejná aktiva (statky, zájmy): lidské životy, zdraví a bezpečí; majetek a veřejné blaho; životní prostředí; kritické technologie a infrastruktury [3]. Nástroj, který je zaměřen na předmětné cíle, je integrální (komplexní) bezpečnost [3] aplikovaná správným způsobem na lidský systém. Na základě poznání k dosažení uvedených cílů je třeba řešit problémy na několika úrovních: technické, funkční (organizační, operativní), taktické, strategické a politické [4], a to tak, aby řešení na všech úrovních byla propojená. Robustnost a kapacita řešení na technické úrovni jsou aspekty, které v kritických podmínkách zaručí bezpečné objekty, které jsou důležité pro zajištění ochrany a přežití obyvatel [5].
Základem lidského úsilí při vytváření bezpečného prostoru je zvládnout (zkrotit) rizika. Pojem "*riziko*" má původ v středověku a naše dnešní znalosti o vyjednávání s riziky jsou systematicky shromažďovány od třicátých let minulého století. Získané znalosti a zkušenosti byly postupně aplikovány v řízení rizik a jím určená opatření a činnosti byly zaváděny postupně do praxe inženýrskými obory [5]. V současné práci s rizikem, je riziko chápáno jako potenciál, že při dané akci nebo činnosti (včetně volby nedělat nic) dojde ke ztrátě (nežádoucímu výsledku). V dnešní praxi se používá pět konceptů řízení rizik a inženýrského vypořádání rizik, tj.: klasické řízení a inženýrství rizika; klasické řízení a inženýrství rizika zahrnující lidský faktor; řízení a inženýrství zaměřené na bezpečí (zabezpečovací řízení a inženýrství); řízení a inženýrství zaměřené na bezpečnost, tj. takové ovládání a vypořádání rizika, které zajistí jak zabezpečený systém, tak jeho bezpečné okolí; a řízení a inženýrství zaměřené na bezpečnost systému systémů (SoS) [4, 5], obrázek 1. Je zřejmé, že čím pokročilejší koncept používáme, tím vyšší jsou nároky na znalosti, nástroje, čas, finance, kvalifikaci personálu atd. Pro každý koncept řízení a inženýrství byla vyvinuta určitá sada standardů a norem pro jeho využívání v praxi [5]. Kvůli různým předpokladům konceptů nejsou výsledky jejich aplikace v praxi stejné. Proto v následujících odstavcích porovnáváme zmíněné koncepty a posuzujeme oprávněnost jejich použití v praxi z hlediska jejich schopnosti zajistit bezpečný lidský systém, tj. lidskou existenci, bezpečí a potenciál rozvoje.

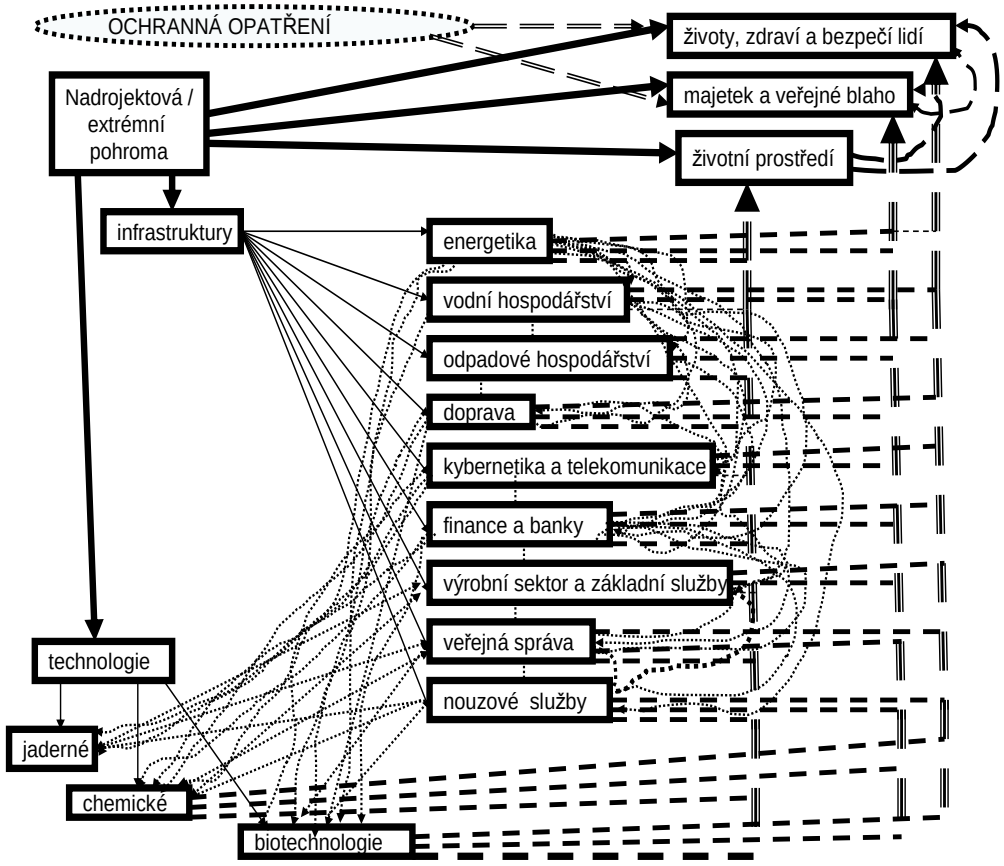


Obrázek č. 1: Koncepty řízení a inženýrského vypořádání rizik a jejich cíle, uspořádané chronologicky dle zavedení do inženýrské praxe

Zdroj: vlastní zpracování

1. Současný stav poznání

Současný stav poznání v oblasti řešení problémů je podle poznatků shrnutých v pracích [4, 5], následující: každý zvažovaný objekt je systém, tj. vyznačuje se prvky, vazbami a toky; zranitelnosti systému jsou rovněž způsobeny vazbami a hlavně toky energií, informací, materiálů, financí atd. mezi prvky systému, které způsobují spřažení; zmíněná spřažení vytváří obvykle vnitřní závislosti, které jsou často příčinou selhání při výskytu extrémních (nadprojektových) pohrom, obrázek 2 [3-6]. Povaha vnitřních závislostí je fyzická, kybernetická, organizační a územní [5]. Recentní poznání ukazuje, že dnešní svět a jeho části jsou reprezentovány modelem označovaným jako systém systémů, který znázorňuje několik překrývajících se systémů, které jsou otevřené a plní určité funkce [3-5]. Jsou provázané vazbami i toky, což vytváří vzájemné závislosti a je příčinou specifických zranitelností [5].



Obrázek č. 2: Dopady extrémní pohromy na lidský systém

Zdroj: [3]

Pozn. Antropogenní opatření a činnosti zajišťují ochranu aktiv jen pro pohromy s nižší velikosti než je projektová pohroma; pouze u určených jaderných zařízení se dělají opatření a činnosti proti vybraným nadprojektovým pohromám.

Systém ve své podstatě znamená více než jen součet částí [4], a proto při poznávání jeho podstaty je důraz kladen na faktory: studium interakcí a propojení; nelineární myšlení; interakce; indukce; zpětné vazby; a experimenty nebo realistické simulace. Například zpětné vazby působí nelinearity v chování systému a způsobují, že chování systému je nepředvídatelné, a proto není možné používat běžné prognostické metody pro identifikaci možných budoucích stavů systému.

Složitost systémů, se kterými pracujeme v praxi, je rozdílná. Podle práce [6] se používají dále uvedené čtyři typy konfigurací celků v systémovém pojetí:

- jednoduše organizované celky,
- složené (kompozitní, integrované, sjednocené) celky,
- složité (komplexní) celky,
- a soubor překrývajících se celků.

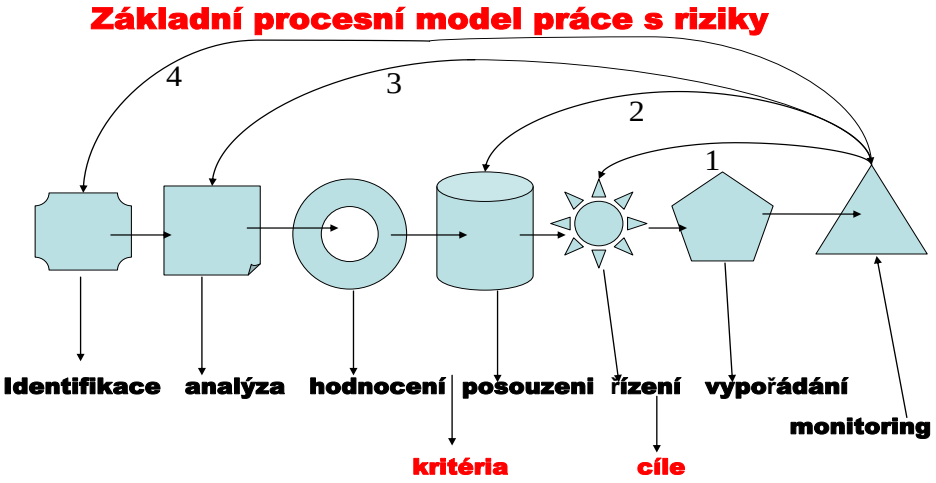
Chování jednoduše organizovaných celků je jasně dáno strukturou a vlastnostmi dílčích částí a je popsáno analytickými funkcemi. Složené celky jsou chápány jako soubor dílčích částí, které jsou uspořádány a propojeny určitým způsobem do jisté struktury tak, aby plnily určité funkce. Jejich chování je popsáno výsledky statistických funkcí, které se opírají o analytické funkce, jejichž parametry jsou proměnné v určitém intervalu, což odráží různé možné stavy / varianty chování celku. Složené (komplexní) celky mají mnoho komponent (často tvořených systémy), které na sebe vzájemně působí a jsou organizačně uspořádány do několika úrovní [6], což způsobuje, že pozorujeme: náhle vynořené rysy chování, které není možné získat na základě znalosti chování jednotlivých komponent (dílčích částí), tj. mluvíme o emergenčním / náhle vynořeném rysu systému; hierarchie; samo organizovanost; a různé struktury spřažených operací, a to všechno dohromady se jeví jako chaos, a proto při popisu jejich chování je nutno zvažovat náhodné a znalostní nejistoty (znalostní nejistota = neurčitost), tj. jejich chování lze popsal výsledky simulací, při kterých jsme vzali v úvahu existenci neurčitostí. Soubor několika překrývajících systémů (často komplexních systémů) je velmi složitý, je znázorněn modelem systém systémů (zkráceně SoS). Jeho chování lze popsat pouze tak, že aplikujeme multidimenzionální a inter-dimenzionální přístup, který je založen na simulaci variant pomocí multikriteriálních postupů.

Jelikož ***řešení mnoha problémů v praxi znamená zvažovat složité systémy a SoS***, je systémové myšlení základní princip výzkumu, jestliže se zabýváme bezpečností objektů. Systémové myšlení znamená: vidět celek i detaily současně; ***zaměřit se na dynamiku procesů;*** pozornost soustředit na vztahy, propojení a interakce; ***brát v úvahu role zpětných vazeb;*** zvažovat relativitu možných situací; a přemýšlet daleko dopředu [4, 5].

Při řízení a inženýrském řešení problémů komplexních systémů a systémů, systémů je pak nutné použít multikriteriální přístupy a v případě systémů systémů je také nutné zvážit průřezová rizika, která jsou příčinami emergenčních vnitřních závislostí, které vzniknou za určitých podmínek, a proto na jejich odhalení je soustředěna pozornost inženýrských disciplín již v oblasti navrhování systémů. Při řešení jejich problémů se používají nástroje, které jsou založené na teorii: chaosu; fuzzy množin; složitosti; a možností – odkazy jsou v [5, 6]. V případě řízení SoS musíme také respektovat základní požadavky, tj. koexistenci překrývajících se systémů [7]. Je si třeba uvědomit, že pro splnění lidských cílů je třeba zajistit koexistenci důležitých systémů, a to minimálně systémů sociálního, ekologického a technologického, které vytvářejí lidský systém.

Podle současných standardů a norem riziko vyjadřuje pravděpodobnou velikost nežádoucích a nepřijatelných dopadů (ztrát, škod a újmy) pohrom o velikosti rovné normativnímu ohrožení na aktiva systému nebo podsystémů v daném časovém intervalu (obvykle 1 rok) a v daném místě, což znamená, že riziko je vždy místně specifické [4]. Typické vlastnosti rizika jsou náhodnost a neurčitost (znalostní nejistota). Pokud chceme řídit riziko, musíme ho identifikovat, analyzovat, vyhodnotit, a poté rozhodnout, co můžeme udělat, abychom riziko snížili, což závisí na našich možnostech, tj. na našich znalostech, disponibilním personálu, disponibilních technických prostředcích a disponibilních finančních zdrojích. K danému účelu požíváme mnoho různých metod, nástrojů a technik, i principy správné praxe (dobré inženýrské praxe). Základní aspekty jsou zahrnuty v následujících definicích základních pojmů.

Práce s rizikem je vyjádřena modelem uvedeným na obrázku 3 [6]. Zpětné vazby uvedené v předmětném obrázku jsou používány tehdy, když úroveň rizika nemá požadovanou úroveň [6]. Pro zajištění bezpečí lidí a bezpečnosti lidského systému (tj. území, organizace, podnik) musíme řídit integrální riziko, které zahrnuje lidský faktor, tj. je třeba najít způsob řízení průřezových rizik a soustředit pozornost na vyšetřování vnitřních závislostí a kritických míst s potenciálem spustit kaskádovité selhání systému, domino efekt, podivné chování atd., a na základě příslušných místních znalostí připravit opatření a činnosti, která zajišťují kontinuitu omezeného provozu infrastruktury a přežití lidí.
Vyhodnocení současných znalostí ukazuje, že jednou z mnoha příčin vnitřních závislostí vyvolávajících kaskádovitá selhání v lidském systému nebo v jeho částech, je lidská chyba (úmyslná nebo neúmyslná) v řízení. Proto v řídících činnostech i inženýrských činnostech musíme udělat všechna opatření k tomu, abychom odvrátili lidská selhání, a to zejména při rozhodování. Protože důsledky chyb vzniklých při rozhodování jsou často obrovské, obrázek 4, je příčinám selhání lidského faktoru na řídící úrovni nyní věnována velká pozornost při práci s rizikem [6, 8].



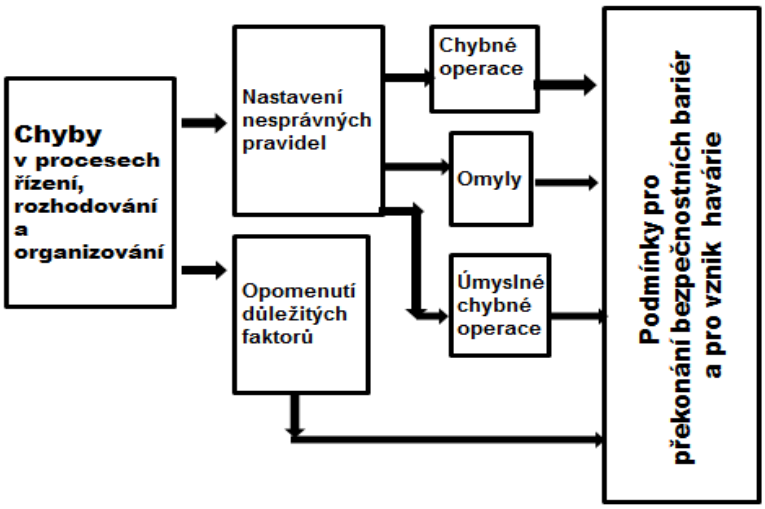
Kritéria: riziko je přijatelné, podmíněně přijatelné, nepřijatelné

Cíle: snížit riziko na určitou úroveň, zajistit bezpečí systému, zajistit bezpečí systému i bezpečí okolí

Zpětné vazby: 1, 2, 3 a 4 se uplatňují, když riziko je nepřijatelné

Obrázek č. 3: Procesní model práce s riziky, čísla 1, 2, 3 a 4 označují zpětné vazby

Zdroj: vlastní zpracování



Obrázek č. 4: Důsledky chyb v rozhodování

Zdroj: vlastní zpracování

Z dnešního pohledu OSN, EU a veřejného zájmu [1-3] je základem pro lidské bytí zachování existence, bezpečí a potenciálu pro rozvoj lidi. V předmětné souvislosti se v praxi používají dále uvedené definice:

1. *Bezpečí (security)* je stav lidského systému, při kterém výskyt škody nebo ztráty na aktivech lidského systému (chráněných veřejných zájmech) má přijatelnou pravděpodobnost (tj. je téměř jisté, že škody a ztráty nevzniknou). To znamená, že je zajištěna určitá stabilita lidského systému v čase a prostoru, tj. udržitelný rozvoj, což znamená, že systém je zabezpečen, tj. je dobře chráněn proti vnitřním a vnějším pohromám všeho druhu.
2. *Bezpečnost (safety)*je soubor antropogenních opatření a činnosti k zajištění zachování existence, bezpečí a rozvoje lidského systému a jeho aktiv. Jeho měřítkem je účinnost vhodných opatření a činností pro zajištění existence, bezpečí a rozvoje aktiv lidského systému.
3. *Zabezpečený systém (secured system)* je systém, který je ochráněn vůči všem pohromám, jejichž zdroje jsou uvnitř i vně systému, a to včetně lidského faktoru.
4. *Bezpečný systém (safe system)* je systém, který je ochráněn vůči všem pohromám, jejichž zdroje jsou uvnitř i vně systému a neohrožuje své okolí při svých normálních, abnormálních a kritických podmínkách.
5. *Zabezpečení systému (system security)* znamená, že žádná pohroma se zdrojem uvnitř a vně systému neohrožuje systém a jeho aktiva. Od 80. let minulého století se v české praxi v daném případě mluví o tzv. systémové bezpečnosti.
6. *Bezpečnost systému (system safety)* znamená, že systém, jeho aktiva a okolí systému nejsou ohroženy žádnou pohromou, tj. ani problémy uvnitř samotného systému při normálních, abnormálních a kritických podmínkách; je zajištěno bezpečí systému i bezpečí okolí systému.
7. *Zabezpečený lidský systém (secured / secure human system)* představuje území s lidskou společností, které je dobře chráněno proti vnitřním a vnějším pohromám.
8. *Bezpečný lidský systém (safe human system)* je reprezentován územím s lidskou společností, jehož aktiva (veřejné statky jsou: lidské životy, zdraví a bezpečí, majetek, veřejné blaho, životní prostředí, infrastruktury a technologie) mají zajištěnu existenci, jsou v bezpečí a mohou se rozvíjet. To znamená, že předmětný systém je chráněn proti vnitřním a vnějším pohromám všeho druhu, a samotný systém neohrožuje okolí při svých normálních, abnormálních a kritických podmínkách, protože dobrá symbióza každého systému s jeho okolím je nezbytná pro existenci systému. Podobně: *bezpečná organizace* je organizace, jejíž chráněná aktiva jsou v bezpečí a mohou se rozvíjet, a organizace neohrožuje své okolí při svých normálních, abnormálních a kritických podmínkách; *bezpečný podnik* je podnik, jehož chráněná aktiva jsou v bezpečí a mohou se rozvíjet, a podnik neohrožuje své okolí při svých normálních, abnormálních a kritických podmínkách; a *bezpečné zařízeni* je zařízení, jehož chráněná aktiva jsou v bezpečí a mohou se rozvíjet, a zařízení neohrožuje své okolí při svých normálních, abnormálních a kritických podmínkách.
9. *Řízení bezpečnosti lidského systému (human system safety management)* je antropogenní řízení lidského systému v dynamicky proměnném světě, které je zaměřeno na bezpečnost lidského systému, jejímž výsledkem je zachování existence, bezpečí a rozvoje všech veřejných aktiv.
10. *Inženýrství (engineering)* je soubor disciplín, které realizují úkoly, jež jsou stanovené v procesu řízení, do praxe. Jak bylo uvedeno výše, riziko je v inženýrské praxi vyjádřeno jako pravděpodobná výše ztrát, škod a újmy na chráněných aktivech, které jsou způsobeny pohromou s určitou velikostí (normativní ohrožení) a které jsou rozpočteny na určitou časovou jednotku (obvykle 1 rok) a na určitý objekt nebo určité místo. *Rizikové*

inženýrství (správně inženýrství rizika; risk engineering) se stalo fenoménem dvacátého století a na jeho základě byla v rozvinutých zemích vytvořena základna pro ochranu lidí a jejich rozvoj, která je docela odolná proti tradičním pohromám, zejména přírodním; chorobám lidí, zvířat a rostlin; technologickým selháním; a sociálním pohromám. Podle definice používané OSN, zajišťovnou Swiss Re, Světovou bankou a dalšími významnými institucemi je rizikové inženýrství chápáno jako systematické využívání inženýrských znalostí a zkušeností pro optimalizaci ochrany lidských životů, životního prostředí, majetku a hospodářských aktiv, tj. pro dosažení optimálního bezpečí a udržitelného rozvoje lidského systému, a jeho hlavním cílem je snížit všechny typy škod a ztrát prostřednictvím kvalifikovaného vyjednávání s rizikem. Je nezbytné si uvědomit, že rizikové inženýrství není statická disciplína, vyvíjí se v čase (obrázek 1) a je problémem u řady dnešních specialistů, hlavně výpočtářů, že neodlišují různé koncepty a v některých případech je tato jejich neznalost příčinou nesprávných řešení (např. tehdy, když použijí standardy a normy pro zabezpečený systém a správné řešení problému vyžaduje standardy a normy pro bezpečný systém, protože selhání systému má velký potenciál poškodit aktiva v okolí systému).

Často používaná charakteristika inženýrských disciplín, které pracují s riziky je následující:

- jedná se mnoha oborové a průřezové obory, které používají jak obecné, tak specifické metody, nástroje a techniky. Specifické metody, nástroje a techniky jsou buď jednoduché, nebo komplexní. Komplexní pak představují uspořádané použití několika obecných či jednoduchých metod, nástrojů a technik,
- používají se metody, nástroje a techniky logické, výpočetní, experimentální, technické, finanční, manažerské a rozhodovací, protože nedílnou součástí disciplín je rozhodování o technických problémech, nákladech a časovém plánování,
- současné úlohy, které souvisí s řízením a vypořádáním rizik pro potřeby zajištění bezpečného lidského systému, vyžadují pro netriviální řešení problémů používat vícekriteriální metody, nástroje a techniky, ve kterých musíme respektovat, že aktiva i zdroje rizik mají rozdílnou podstatu, která je zdrojem nesouměřitelnosti kritérií a je důvodem pro aplikaci jen vícekriteriálních metod, nástrojů a technik, které jsou vhodné. To znamená, že při výběru metod, nástrojů a technik je třeba respektovat: kvalitu dat, strukturu problému, který řešíme i požadavky na kvalitu výsledku; a speciálně prověřovat jak kvalitu dat (správnost, úplnost, vypovídací schopnost k danému problému), tak při použití expertů jejich kvalifikovanost (IAEA, OECD, USA, WB aj. mají přísná kritéria na posuzování kvalifikace experta) [6].

Speciální nároky na metody, nástroje a techniky inženýrských disciplín jsou dané dále uvedenými skutečnostmi:

- při řešení problémů je třeba zvažovat, že: všechny procesy probíhají dynamicky, a proto se musí používat speciální aparát, kterým je soubor procedur tvořený výzkumnými postupy pro optimální řízení rizik; a pohrom je mnoho, působí na různorodá aktiva rozmanitě, a proto důležitou roli hraje zranitelnost jak aktiv, tak i jejich vzájemných propojení,
- na základě ocenění kvality disponibilních datových souborů, především jejich nejistot a neurčitostí, je třeba při řešení úkolů praxe:

* použít přístup deterministický, stochastický nebo heuristický v závislosti na cíli řešení,

* integrovaným způsobem aplikovat kvalitativní a kvantitativní přístupy k riziku a bezpečnosti systémů, které se v obecné rovině sestávají z dále uvedených kroků: definice systému a prostředí; identifikace možných nebezpečí; stanovení ohrožení při

extrémních jevech; vyhodnocení rizik; návrh korekčních a nápravných akcí podle kritérií bezpečnosti s cílem zajistit přijatelné bezpečí; a verifikace přijatelnosti rizika.

Dále je třeba strukturalizovat metody podle kvality dat a podle cíle řízení rizik, protože z hlediska praxe je třeba oddělit úlohy pro:

- identifikaci rizika,
- analýzu rizika,
- stanovení hodnoty rizika, ve kterém jde o:
  * „přesný“ údaj pro potřeby strategického rozhodování,
  * hodnotu rizika pro potřeby kontroly stavu systému,
  * okamžité zvládnutí rizika konkrétního procesu v čase a prostoru (operativní rozhodování), při kterém lze použít míru (někdy postačí i verbální).

Poté je třeba metody, nástroje a techniky rozdělit s ohledem na počet chráněných aktiv a v případě dvou a více aktiv odlišit, zda budeme sledovat riziko integrované nebo integrální a které jevy v daném místě budeme považovat za zdroje rizik. Správně je třeba aplikovat přístup „All Hazard Approach“ [9]. Je skutečností, že u všech metod, které používáme v praxi, musíme rozlišovat dva faktory: určitá integrace metody do matematického aparátu; a realitu, jak určitou metodu lze použít při řízení a vypořádání rizik na základě práce s rizikem ve zvolené koncepci řešení problému.

Klíčové koncepty současného inženýrství zaměřeného na bezpečnost jsou:

- přístupy jsou založené na riziku, tj. intenzita práce a dokumentace je přiměřená úrovni rizika,
- odborný přístup je založen na realitě, že se zvažují pouze kritické atributy kvality a kritické parametry procesu,
- řešení problému se orientuje na kritické položky, tj. sledují a řídí se kritické aspekty technických systémů zajišťujících konzistenci operací systému,
- prověřené parametry kvality se objevují již v návrhu projektu,
- důraz je kladen na kvalitní inženýrské postupy, tj. je nutno prokazovat správnost vybraných postupů v daných podmínkách,
- zacílení na zvyšování bezpečnosti, tj. trvalé zlepšování procesů s využitím analýzy kořenových příčin poruch a selhání.

Pro respektování uvedených položek musí být použity reprezentativní datové soubory a pouze ověřené metody, které poskytují výstupy s určitou vypovídací schopností.

Vzhledem k existenci mnoha faktorů, zejména lidského faktoru, které ovlivňují řešení problémů v reálných podmínkách a skutečnosti, že uvedené faktory nejsou pouze náhodné, ale také znalostní (neurčitosti), jsou opatření, činnosti a postupy označené jako dobrá inženýrská praxe typické pro inženýrské obory. Modus operandi (osvědčené) postupy v jednotlivých oblastech na základě zkušeností zajišťují dobrý výsledek ve velké většině případů. Uvedený postup se používá v případech, ve kterých nebyl schválen jednotný postup (tj. nejsou normy nebo standardy); často se používá při měření v laboratořích, jednání s lidmi atd. ***Dobrá inženýrská praxe (dobrý inženýrský postup)*** se pak definuje jako soubor inženýrských metod a standardů, které se používají během životního cyklu technického systému s cílem dosáhnout vhodné a nákladově efektivní řešení. Je podporována vhodnou dokumentací (konceptuální dokumentace, diagramy, manuály, zprávy z testování apod.).

V daném kontextu je inženýrská odbornost chápaná jako výraz schopnosti při řešení problému: aplikovat znalosti matematiky, vědy a inženýrství; navrhnout a realizovat experimenty; analyzovat a interpretovat data; navrhnout komponenty nebo celý systém podle požadavků a v rámci realistických omezení identifikovat, formulovat a řešit inženýrské problémy; efektivně komunikovat; chápat dopady inženýrských řešení v širším kontextu;

využívat nejmodernější nástroje a metody v inženýrské praxi; dodržovat profesionální a profesní odpovědnosti a etiky; a vést interdisciplinární tým. Většina z uvedených požadavků je zacílena na korekci negativního projevu lidského faktoru.

2. Materiály a metody pro posuzování kritičnosti sledovaných konceptů

Používané koncepty řízení rizik i inženýrských způsobů vypořádání rizik, používané v praxi jsou zmíněny výše (obrázek 1). Jelikož našim cílem je hodnocení a každé hodnocení závisí významně na cílech a kritériích hodnocení [4], zdůrazňujeme, že dále provedené hodnocení je zaměřené na posouzení schopnosti sledovaných konceptů řízení rizik a inženýrských postupů vypořádání rizik naplnit cíle lidí, kterými je existence, bezpečí a rozvoj lidí, tj. jde o ochranu lidí v nejširším kontextu. Autorka si dovoluje poznamenat, že při jiných cílech hodnocení se z metodického hlediska musí použít jiná kritéria a jiné prahové hodnoty, což pochopitelně zpravidla ovlivňuje výsledky.
Předložené hodnocení se provádí v lidském systému, který se skládá z nesouměřitelných aktiv a je systémem systémů. Proto účinnost a kritičnost sledovaných konceptů je možno posoudit pouze pomocí multikriteriálního přístupu [4, 6]. ***Kritičnost lidského systému a jeho aktiv*** závisí na zranitelnosti, pružné odolnosti a na důležitosti pro existenci, bezpečí a rozvoj lidského systému a jeho aktiv. Je daná úrovní integrálního rizika, přičemž velkou roli hrají průřezová rizika [5].
V analogii s postupy používanými při posuzování bezpečnosti a ochrany kritické infrastruktury [10], ve kterých hodnocení je zacílené na bezpečnost a ochranu lidského systému, ***použijeme míru kritičnosti jednotlivých koncepcí jak řízení rizik, tak inženýrských způsobů vypořádání rizika,*** a pro její určení použijeme následující faktory:

1 - míra schopnosti ochrany lidských životů, zdraví a bezpečí uvnitř systému,
2 - míra schopnosti ochrany lidských životů, zdraví a bezpečí vně systému,
3 - míra schopnosti ochrany majetku uvnitř systému,
4 - míra schopnosti ochrany majetku vně systému,
5 - míra schopnosti ochrany veřejného blaha uvnitř systému,
6 - míra schopnosti ochrany veřejného blaha vně systému,
7 - míra schopnosti ochrany životního prostředí uvnitř systému,
8 - míra schopnosti ochrany životního prostředí vně systému,
9 - míra schopnosti ochrany životně důležitých infrastruktur a technologií uvnitř systému,
10 - míra schopnosti ochrany životně důležitých infrastruktur a technologií vně systému,
11 - míra schopnosti ochrany lidských životů a zdraví před dopady pohrom způsobených vnitřními závislostmi,
12 - míra schopnosti ochrany životního prostředí před dopady pohrom způsobených vnitřními závislostmi,
13 - míra schopnosti ochrany lidské společnosti před dopady pohrom způsobených vnitřními závislostmi,
14 - míra schopnosti ochrany životně důležitých infrastruktur a technologií před dopady pohrom způsobených vnitřními závislostmi.

Údaje pro hodnocení byly získány od šesti expertů, vybraných podle kritérií používaných v EU [6] z oblastí:

- ochrana obyvatelstva,
- ochrana území,
- ochrana životního prostředí,
- veřejná správa zaměřená na ochranu obyvatelstva,

- ochrana technologických systémů,
- Integrovaného záchranného systému.

Odborníci hodnotili 14 faktorů, uvedených výše, podle svých znalostí a zkušeností, dle následující stupnice, která je analogická ke stupnici, kterou pro hodnocení rizik používají ČSN normy [6]:

0 bodu - faktor zajišťuje extrémně vysokou schopnost ochrany (očekávané škody jsou nižší než 5 %, aplikace konceptu znamená nevýznamné riziko pro aktiva, tj. zanedbatelnou kritičnost konceptu),

1 bod - faktor zajišťuje velmi vysokou schopnost ochrany (očekávané škody jsou v intervalu 5-25 %, aplikace konceptu znamená nízké riziko pro aktiva, tj. nízkou kritičnost konceptu),

2 body - faktor zajišťuje vysokou schopnost ochrany (očekávané škody jsou v intervalu 25-45 %, aplikace konceptu znamená střední riziko pro aktiva, tj. střední kritičnost konceptu),

3 body - faktor zajišťuje střední schopnost ochrany (očekávané škody jsou v intervalu 45-70 %, aplikace konceptu znamená vysoké riziko pro aktiva, tj. vysokou kritičnost konceptu),

4 body - faktor zajišťuje nízkou schopnost ochrany (očekávané škody jsou v intervalu 70-95 %, aplikace konceptu znamená velmi vysoké riziko pro aktiva, tj. velmi vysokou kritičnost konceptu),

5 bodů - faktor zajišťuje zanedbatelnou schopnost ochrany (očekávané škody jsou vyšší než 95 %, aplikace konceptu znamená extrémně vysoké riziko pro aktiva, tj. extrémně vysokou kritičnost konceptu).

Výsledná hodnota pro každý faktor je určena jako medián z údajů získaných od expertů. Výsledná míra kritičnosti, tj. schopnosti ochrany pro všechny faktory s předpokladem, že všechny faktory mají stejnou váhu, může nabýt hodnot 0 až 70. Jestliže opět použijeme přístup používaný v ČSN normách, tak získáme hodnoty, které jsou uvedené v tabulce 1.

Tabulka č. 1: Rozsah hodnot pro určení míry kritičnosti konceptů používaných pro řízení rizik a pro inženýrské způsoby vypořádání rizik

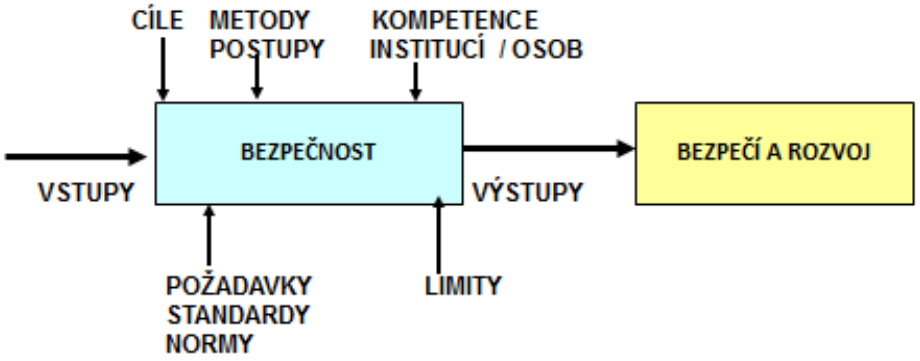
Míra kritičnosti koncepce	Hodnoty v %	Počet bodů pro faktor
Extrémně vysoká	Více než 95 %	Více než 66.5
Velmi vysoká	70 - 95 %	49 – 66.5
Vysoká	45 - 70 %	31.5 – 49
Střední	25 – 45 %	17.5-31.5
Nízká	5 – 25 %	3.5 – 17.5
Zanedbatelná	Méně než 5 %	Méně než 3.5

Zdroj: vlastní zpracování

3. Výsledky

Strategie řízení lidského systému pro zajištění existence, bezpečí a udržitelného rozvoje lidí je určena způsobem vyjednávání s riziky. Obvykle se v praxi [4] používá dále uvedený přístup: část rizika se sníží preventivními opatřeními, tj. odvrátí se realizace jistých dopadů předem; část rizika se zmírní tím, že se připraví jistá opatření a činnosti (výstražné systémy a další opatření nouzového a krizového řízení), tj. sníží se nebo se odvrátí nepřijatelné dopady při realizaci rizika na chráněná aktiva; část rizika se pojistí, aby byly peníze na obnovu; část rizika se při realizaci zajistí opatřeními a činnostmi odezvy a obnovy, tj. jsou připraveny

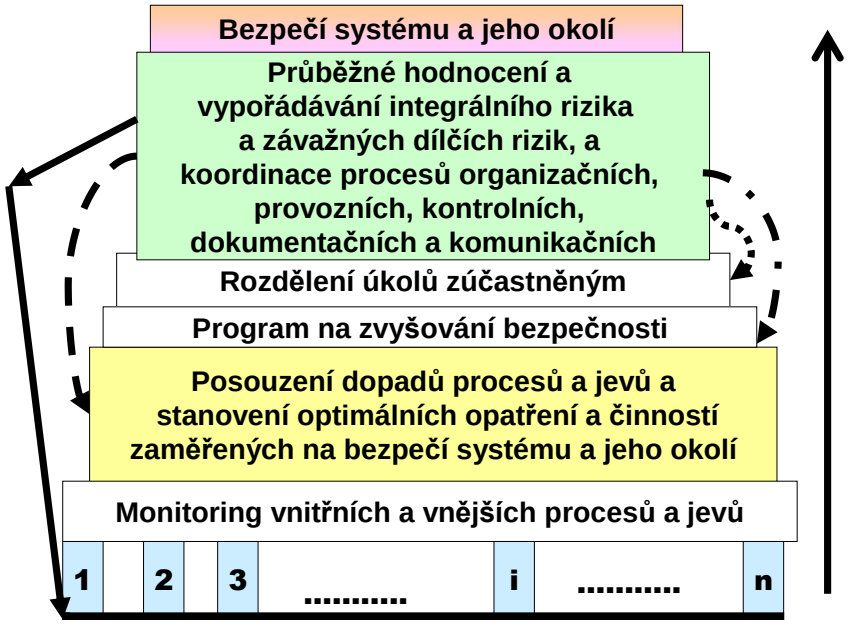
prostředky, síly a prostředky pro reakci a obnovu; a zbytková část rizika, která je buď neřiditelná, nebo příliš nákladná na zvládnutí anebo málo častá se u starších konceptů ponechává bez lidské pozornosti, a u pokročilejších konceptů se připravuje pohotovostní (contingency) plán a plán kontinuity. Vyjednávání s rizikem je doplněno rozložením úkolů mezi všechny zúčastněné strany.
Proces řízení bezpečnosti systému je znázorněn na obrázku 5. Systém řízení bezpečnosti je uveden na obrázku 6; zpětné vazby, které jsou označeny na obrázku, jsou používány tehdy, když úroveň bezpečnosti není na požadované úrovni [6].



Obrázek č. 5: Proces řízení bezpečnosti systému.

Zdroj: vlastní zpracování

Je nezbytné uvést, že řízení rizik není dosud jednotně chápáno [4]. V našem výzkumu považujeme jeho interpretaci uvedenou na obrázku 4, která je v souladu s definicí, kterou používá FERMA (Federation of European Risk Management Associations), EMA (Emergency Management Office of Australia), vláda UK, vláda a kongres USA (Congressional Commission on Risk Assessment and Risk Management), OECD, MAAE atd. Koncepty řízení a inženýrského vypořádání rizik, jejich charakteristiky a popisy jejich výstupů jsou uvedeny v tabulce 2, která je zhotovena podle výsledků kritické analýzy publikací [7, 11-30] a dalších, které jsou v [4-6].



Obrázek č. 6: Systém řízení bezpečnosti; čísla označují vnitřní a vnější procesy, které mají vliv bezpečnost systému a čáry (tečkovaná, čerchovaná, čárkovaná a plná) označují zpětné vazby.

Zdroj: vlastní zpracování

Tabulka č. 2: Koncepty řízení a inženýrského vypořádání rizik, jejich charakteristiky a popisy jejich výstupů

Koncept řízení a inženýrského vypořádání rizik	Charakteristika konceptu	Popis výstupů aplikace konceptu
Klasický koncept	Objekt chápaný jako systém (podnik, území, organizační jednotka) je uzavřený systém. Zdroje rizik jsou technologické jevy (pohromy, nehody, havárie) uvnitř objektu. Vznik v 30. letech minulého století.	Cílem je snížení technologických rizik v systému na určitou úroveň. Inženýrská praxe má postupy dané standardy a normami. Riziko se stanovuje až po návrhu systému, a proto není možné snížit rizika spojená s nevhodným řešením pro dané místo a systém. Snížení rizik spojených s nevhodným řešením pro dané místo a systém lze provést pouze organizačními opatřeními, jejichž účinnost je nižší než účinnost technických opatření [3].
Klasický koncept zvažující lidský faktor	Objekt chápaný jako systém (podnik, území, organizační jednotka) je uzavřený systém. Zdroje rizik jsou technologické jevy (pohromy, nehody, havárie) uvnitř objektu a lidský faktor. Vznik na konci 70. let minulého století.	Cílem je snížení technologických rizik a rizik spojených s lidským faktorem v systému na určitou úroveň. Inženýrská praxe má postupy dané standardy a normami, které zvažují i lidský faktor. Riziko se stanovuje až po návrhu systému, a proto není možné snížit rizika spojená s nevhodným řešením pro dané místo a systém. Snížení rizik spojených s nevhodným řešením pro dané místo a systém lze provést pouze organizačními opatřeními, jejichž účinnost je nižší než účinnost technických opatření [3].
Koncept zajišťující zabezpečený systém	Objekt chápaný jako systém (podnik, území, organizační jednotka) je otevřený systém. Zdroje rizik jsou pohromy, tj. jevy uvnitř i vně objektu a lidský faktor. Do zdrojů rizik patří i špatná rozhodnutí při řízení nebo vypořádání rizik; tj. příčiny tzv. organizačních havárií [4]. Vznik v první polovině 80. let minulého století.	Cílem je snížení rizik, která představují pohromy všeho druhu, tj. jevy uvnitř i vně objektu a lidský faktor, který se projevuje při konkrétních činnostech i rozhodování, na určitou úroveň. Inženýrská praxe má postupy dané standardy a normami, které zvažují i lidský faktor. Dopady objektu na okolí nejsou zvažovány, tj. nejsou prováděna specifická technická opatření v projektu a provozu. Nepřijatelné dopady na okolí lze pouze zmírnit zvláštními nouzovými plány (např. havarijními a povodňovými plány) [3], tj. organizačními opatřeními a činnostmi, když je stát vynutí legislativou a kontrolní činností.
Koncept zajišťující bezpečný systém	Objekt chápaný jako systém (podnik, území, organizační jednotka) je otevřený systém. Zdroje rizik jsou pohromy, tj. jevy uvnitř i vně objektu, vnitřní závislosti a lidský faktor. Do zdrojů rizik patří i špatná rozhodnutí při řízení nebo vypořádání rizik; tj. příčiny tzv. organizačních havárií a u objektů zvláštní důležitosti (např. jaderné elektrárny, jaderný průmysl) se vyžaduje aplikace principu předběžné	Cílem je zajistit bezpečí systému i bezpečí okolí systému při normálních, abnormálních a kritických podmínkách systému. Uplatněním principu předběžné opatrnosti se vyjednává i s málo častými riziky, která mohou mít vysoce nepřijatelné dopady na sledovaná aktiva. Právně je uplatnění předmětného principu vyžadované u specifických jaderných a chemických objektů. U složitých (komplexních) je výsledkem je

	opatrnosti [4]. Vznik v druhé polovině 80. let minulého století. Pokročilé inženýrství zaměřené na bezpečnost používá při stanovení rizika následující principy: - riziko se v daném objektu stanovuje během celého životního cyklu, tj. při umísťování, navrhování, projektování, výstavbě, provozu, odstavení a vyřazení z provozu a nakonec též při uvedení území do původního stavu, - stanovení rizika se zaměřuje též na požadavky uživatelů a na úroveň poskytovaných služeb, - riziko se stanovuje podle kritičnosti dopadů na procesy, poskytované služby a na aktiva, která jsou určena veřejným zájmem, - nepřijatelná rizika se zmírňují nástroji pro řízení rizik a pro inženýrské vypořádání rizik, tj. technickými a organizačními návrhy, standardizací pracovních postupů nebo automatizovanou kontrolou [5]. Pro přípravu správných podkladů je nutné propojit analytické metody s expertními hodnoceními, kterými odstraníme neurčitosti (znalostní nejistoty) v datech.	optimální řešení pro vyjednávání s riziky od pohrom všeho druhu, tj. jevů uvnitř i vně objektu, vnitřních závislostí a od lidského faktoru, který se projevuje při konkrétních činnostech i rozhodování. Inženýrská praxe má postupy dané standardy a normami, které zvažují vnitřní závislosti i lidský faktor (např. PSA). Kromě technických opatření spojených s respektováním principu předběžné opatrnosti jsou: sestavovány plány kontinuity obsahují specifická řešení technických problémů pro překonání kritických podmínek v systému; a krizové plány pro ochranu okolí systému, když systém nezvládne své kritické podmínky a vyvolá nepřijatelné dopady na veřejná aktiva v okolí. Řízení a inženýrské vypořádání rizik má znaky: - při umísťování, navrhování, projektování a výstavbě objektů se aplikují opatření a činnosti vedoucí k minimalizaci rizik, - do provozu objektu je začleněn systém včasného varování a postupy pro zajištění přijatelné úrovně rizika, - provoz objektu má postupy pro zvládnutí abnormálních, nouzových a kritických podmínek a pro vyřazení z provozu [3].
Koncept zajišťující bezpečný systém systémů	Objekt chápaný jako systém systémů (podnik, území, organizační jednotka) je otevřený systém systémů. Zdroje rizik jsou pohromy, tj. jevy uvnitř i vně objektu, vnitřní závislosti v systému i napříč systémů a lidský faktor, který se projevuje při konkrétních činnostech i rozhodování (tj. příčiny tzv. organizačních havárií. U objektů zvláštní důležitosti (např. jaderné elektrárny, jaderný průmysl) se vyžaduje aplikace principu předběžné opatrnosti [4]. Pro bezpečnost systému systémů je nutné zajistit koexistenci jednotlivých systémů. Vznik na počátku třetího tisíciletí.	Cílem je zajistit: bezpečí obou, tj. systému systémů včetně jeho aktiv a okolí systému systémů; a koexistenci jednotlivých systémů tvořících systém systémů. Soubor standardů a norem je stále diskutován a připravován.

Zdroj: vlastní zpracování

Jak bylo uvedeno výše, v praxi se používá pět různých konceptů pro řízení rizik a pro inženýrské vypořádání rizik. Výsledky jejich hodnocení z pohledu zajištění bezpečnosti lidského systému pomocí 14 faktorů, získané na základě dat získaných od 6 expertů jako medián, jsou uvedeny v tabulce 3.

Tabulka č. 3: Míra kritičnosti sledovaných konceptů řízení rizik a inženýrského vypořádání rizik

Faktor	Klasický koncept řízení a inženýrského vypořádání rizik	Klasický koncept řízení a inženýrského vypořádání rizik zvažující lidský faktor	Koncept řízení a inženýrského vypořádání rizik zajišťující zabezpečený systém	Koncept řízení a inženýrského vypořádání rizik zajišťující bezpečný systém	Koncept řízení a inženýrského vypořádání rizik zajišťující bezpečný systém systémů
1	4	3	1	1	1
2	5	5	5	1	1
3	4	3	1	1	1
4	5	5	5	1	1
5	5	3	1	1	1
6	5	5	5	2	1
7	4	3	1	1	1
8	5	5	5	1	1
9	4	3	1	1	1
10	5	5	5	1	1
11	5	5	4	5	1
12	5	5	4	5	1
13	5	5	4	5	1
14	5	5	4	5	1
Všechny faktory	66	60	41	31	14

Zdroj: vlastní zpracování

Srovnání údajů v tabulkách 3 a 2 ukazuje, že míra kritičnosti u:

- obou, tj. u klasického konceptu řízení a inženýrského vypořádání rizik a u konceptu řízení a inženýrského vypořádání rizik zvažujícího lidský faktor, je velmi vysoká,
- konceptu řízení a inženýrského vypořádání rizik zaměřeného na zabezpečený systém je vysoká,
- konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém je střední,
- konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém systémů je nízká.

To znamená, že na základě našich současných znalostí a zkušeností je koncept řízení a inženýrského vypořádání rizik zaměřený na bezpečný systém systémů nejefektivnější koncept práce s riziky s ohledem na cíle lidí, uvedené výše.

Když vezmeme v úvahu skutečnost, že využívání různých konceptů se liší požadavky na znalosti, údaje, kvalifikace personálu, materiál, finance a na technická řešení, je zřejmé, že nejúčinnější koncept je na zdroje nejnáročnější. Protože zdrojů, sil a prostředků na bezpečnost není nikdy dostatek, je třeba z důvodů hospodárnosti postupovat následovně:

- pro řešení problémů na strategické úrovni používat koncept řízení a inženýrského vypořádání rizik zaměřený na bezpečný systém systémů,
- pro řešení problémů na taktické a funkční úrovni používat koncept řízení a inženýrského vypořádání rizik zaměřený na bezpečný systém,

- pro řešení problémů na technické funkční úrovni používat koncept řízení a inženýrského vypořádání rizik zaměřený na zabezpečený systém, a to jen tehdy, když výskyt možných škod v okolí systému je málo pravděpodobný anebo škody jsou přijatelné (např. manipulace s nádrží s vysoce nebezpečnou látkou již do předmětné kategorie nepatří).

Závěr

Tabulka 3 popisuje koncepty řízení rizik a inženýrského vypořádání rizik používané v současné praxi. Pro každý koncept existují nebo se připravují standardy a normy. Protože požadavky jednotlivých konceptů jsou odlišné, tak příslušné standardy a normy se též liší. Proto výsledky jejich aplikací jsou obvykle různé a pro jejich získání jsou různé požadavky na data, znalosti, materiál, technologie, finance atd. Kvůli hospodárnému nakládání se zdroji, silami a prostředky je nezbytné vždy správně rozhodnout o tom, který koncept je dostačující pro řešení daného problému. Při rozhodování hraje roli velikost rizika a úroveň, na níž se řeší problém.
Výsledky uvedené výše ukazují, že na strategické úrovni řešení problému je nutné používat koncept řízení a inženýrského vypořádání rizik zaměřený na bezpečný systém systémů. Na taktické a funkční úrovni je nutné respektovat doporučení strategického konceptu a pro místně specifická řešení problémů použít koncept řízení a inženýrského vypořádání rizik zaměřený na bezpečný systém, protože charakter řešených problémů není tak zásadní z dlouhodobého hlediska. Na technické úrovni je nutné respektovat doporučení všech vyšších konceptů, tj. strategické, taktické a funkční a pro místně specifická řešení problémů použít koncept řízení a inženýrského vypořádání rizik zaměřený na zabezpečený systém, jestliže charakter řešených problémů není tak zásadní z hlediska času. Řešení problémů na politické úrovni by měla respektovat strategická řešení, protože je tak zajistí respektování veřejného zájmu. Poslední požadavek je často problém, protože politici mají zpravidla nízké odborné znalosti a zkušenosti, a velmi často mají dojem, že získali božskou moudrost, když se dostali do politických orgánů.
Je také zřejmé, že v nouzovém řízení nebo v řízení krizových situací není čas a dostatek dat na určení nejvhodnějšího strategického řešení, tj. v nouzovém řízení se používá pro řízení a inženýrské vypořádání rizik obvykle klasický koncept práce s riziky zvažující lidský faktor. V mnoha případech u důležitých objektů jako jsou provozy a sklady s nebezpečnými látkami, se používá koncept práce s riziky orientovaný na zabezpečený objekt (vnitřní havarijní plán). U vysoce kritických objektů jako jsou jaderné elektrárny a přehrady se i zde používá koncept práce s riziky zaměřený na bezpečný systém (vnitřní a vnější havarijní plány, krizový plán, plán kontinuity). Pro bezpečnost, a tím i ochranu kritické infrastruktury se vytváří postupy práce s riziky zaměřené na bezpečný systém systémů.

Literatura

[1] UN: *Human Development Report*. New York: UN, 1994, www.un.org.
[2] EU: *The Safe Community Concept*. Brussels: EU, 2004, PASR project.
[3] D. Procházková: *Strategické řízení bezpečnosti území a organizace*. Praha: ČVUT, 2011, 483p.
[4] D. Procházková: *Analýza a řízení rizik*. ISBN 978-80-01-04841-2. Praha: CVUT, 2011, 405p.
[5] D. Procházková: *Bezpečnost kritické infrastruktury*. ISBN: 978-80-01-05103-0, Praha: ČVUT, 2012, 318p.
[6] D. Procházková: *Základy řízení bezpečnosti kritické infrastruktury*. ISBN: 978-80-01-05245-7. Praha: ČVUT, 2013, 225p.
[7] H. Bossel: *Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme*. Books on Demand, Norderstedt/Germany, ISBN 3-8334-0984-3, 2004. www.libri.de.
[8] AIChE: *Guidelines for Preventing Human Error in Process Safety*. American lnstitute of Chemical Engineers, New York, NY, 1994.
[9] FEMA: *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. FEMA, Washington 1996.

[10] D. Procházková, J. Procházka: *Model for Critical Infrastructure Safety Management*. Brno: UNOB 2013, in print.
[11] AFMC/ENPI: *Risk Management*. AFMC Pamphlet 63-101, Headquarters Air Force Materiel Command, Wright-Patterson Air Force Base 1997.
[12] AS/NZS: *Australia and New Zealand Standard: Risk Management, issued by Standards Australia, Guideline 4360*. http://www.riskmanagement. com.au/Default.aspx?tabid=148 –116 pp.; b) Risk Management Guidelines - Companion to AS/NZS 4360:2004 available for purchase at http://www.riskmanagement.com.au/Default.aspx?tabid=157 – 28 pp.
[13] Canadian Standards Association: *CAN/CSA-Q850-97 Risk Management: Guideline for Decision-Makers – A National Standard of Canada*. http://www.csa- intl.org/onlinestore/ GetCatalogItemDetails.asp?mat= 000000000002005912
[14] EPA: *Guidance for Risk Assessment and Management: Off-site Individual Risk from Hazardous Industrial Plant. Environmental Protection Authority. State of Western Austria*.2000, pp. 21. www.environ.wa.gov.au/ downloads/Guidance_Statements/8.pdf
[15] NRC: *Science and Judgement in Risk Management*. U.S. National Research Council 1994 ("Blue Book"). http://www.nap.edu/books/030904894X/html/
[16] WB: *Natural Disaster Risk Management*. The World Bank. Urban and City Management 2004. http://www.worldbank.org/wbi/urban/ paper disaster.htm
[17] R. Bris, C. G. Soares, S. Martorell (eds): *Reliability, risk and safety: Theory and Application*. ISBN: 978-0-415-55509-8, 2367p., CD ROM - ISBN: 978-0-203-85975-9, CRC Press / Balkema, Leiden 2009.
[18] B. Ale, I. Papazoglou, E. Zio (eds): *Reliability, Risk and Safety*. Taylor & Francis Group, London 2010, ISBN 978-0-415-60427-7, 2448p.
[19] Ch. Bérenguer, A. Grall, and C. G. Soares (eds): *Advances in Safety, Reliability and Risk Management*. Taylor & Francis Group, London 2012, ISBN 978-0-415-68379-1, 3068p.
[20] CISP: *Workshop on Critical Infrastructure Protection and Civil Emergency Planning-Dependable Structures, Cybersecurity*. Commnon Standard. Zurich 2005, Centre for International Security Policy, www.eda.admin.ch
[21] A. Kuhlmann: *Does Safety Science Fulfill the Requirements of Modern Technical Systems? In: Safety of Modern Systems*. Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 9-17.
[22] H. J. Pasman and J. K. Vrijling: *Social Risk Assessment of Large Technical Systems*. In Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, pp. 151-162.
[23] IAEA: *Safety Guides and Technical Documents*. Vienna: IAEA 1954 – 2013.
[24] COMAH: *Safety Report Assessment Manual: COMAH*. London: UK- HID CD2 London 2002, 570 p.
[25] ASCE: *Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters", Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards", Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters*. ASCE, Washington 2001.
[26] H. E. Roland, B. Moriarity: *System Safety Engineering and Management*. ISBN 0-471-6186-0. J. Willey 1990, 321p.
[27] R. Anderson: *Security Engineering – a Guide to Building Dependable Distributed Systems*. ISBN 978-0-470-068552-6, J. Willey 2008, 1001p.
[28] F. P. Lees: *Loss Prevention in the Process Industries*. Butterworths, London 1980.
[29] A. Kossiakoff , W. N. Sweet: *Systems Engineering. Principles and Practices*. ISBN 0-471-23443-5. J.Wiley, New Jersey 2003, 459p.
[30] DoD US: *DoD Security Engineering Facilities Planning Manual*. Department of Defense US. DRAFT UFC 4-020-01, 3 March 2006. http://www.wbdg.org/ndbm /DesignGuid/ pdf/FINAL%20DRAFT UFC 4-020-01.pdf

Kontakt:
doc. RNDr. Dana Procházková, DrSc.
České vysoké učení technické v Praze,
Fakulta dopravní
Konviktská 20
110 00 Praha
email: prochazkova@fd.cvut.cz