



# VALIDITA TECHNIK POUŽÍVANÝCH V PRAXI PŘI PRÁCI S RIZIKY

Dana PROCHÁZKOVÁ

## VALIDITY OF TECHNIQUES USED IN PRACTICE AT WORK WITH RISKS



ENVIRONMENTAL POLICY TOOLS '2019

### ABSTRAKT

*PUBLIKACE SE ZABÝVÁ RIZIKY, KTERÁ NARUŠUJÍ BEZPEČNOST TECHNICKÝCH DĚL A JEJICH OKOLÍ. UKAZUJE, ŽE KVŮLI SLOŽITOSTI SOUČASNÝCH TECHNICKÝCH DĚL, JE NUTNO U DŮLEŽITÝCH TECHNICKÝCH DĚL ZVAŽOVAT I RIZIKA, KTERÁ JSOU SPOJENÁ S VNITŘNÍMI PROPOJENÍMI. PROTO V PŘÍPADĚ STRATEGICKÝCH ŘEŠENÍ PROBLÉMŮ TECHNICKÝCH DĚL JE NUTNÉ POUŽÍVAT SYSTÉMOVÉ POJETÍ ZALOŽENÉ NA INTEGRÁLNÍM RIZIKU. POSTUPY ZALOŽENÉ NA VYPOŘÁDÁNÍ DÍLČÍCH RIZIK ČI INTEGROVANÉHO RIZIKA NEZAJIŠTÍ DOSTATEČNĚ BEZPEČNÉ TECHNICKÉ DÍLO. VZHLEDEM K DYNAMICKÉMU VÝVOJI SVĚTA, JE TŘEBA PRIORITY RIZIKA MONITOROVAT A VYPOŘÁDÁVAT V ČASE. POSOUZENÍ VALIDITY METOD A PROCEDUR PRÁCE S RIZIKY, KTERÉ JSOU POUŽÍVANÉ V PRAXI, UKAZUJE, ŽE DOSUD PŘEVládAJÍ TECHNIKY, KTERÉ NERESPEKTUJÍ SYSTÉMOVOU POVAHU TECHNICKÝCH DĚL A DYNAMIKU VÝVOJE.*

**KLÍČOVÁ SLOVA:** *technické dílo; systémové pojetí; systém systémů; pohromy; vnitřní propojení; riziko; identifikace rizik; analýza rizik; hodnocení rizik; řízení rizik; vypořádání rizik; řízení rizik v čase zacílené na bezpečné technické dílo.*

**ABSTRACT:** *THE PAPER DEALS WITH RISKS THAT DISTURB THE SAFETY OF TECHNICAL FACILITIES AND THEIR VICINITY. IT SHOWS THAT DUE TO TECHNICAL FACILITIES COMPLEXITY, IT IS NECESSARY AT IMPORTANT TECHNICAL FACILITIES TO CONSIDER ALSO RISKS THAT ARE CONNECTED WITH INTERNAL LINKS (INTERDEPENDENCES). THEREFORE, ON STRATEGIC LEVEL OF PROBLEM SOLUTIONS IT IS NECESSARY TO USE THE SYSTEM CONCEPT BASED ON INTEGRAL RISK. THE PROCEDURES BASED ON COPPING WITH PARTIAL RISKS OR INTEGRATED RISKS DO NOT ENSURE SUFFICIENTLY SAFE TECHNICAL FACILITY. WITH REGARD TO WORLD DYNAMIC DEVELOPMENT IT IS NECESSARY THE PRIORITY RISKS TO MONITOR AND TO COPE WITH THEM DURING THE TIME. JUDGEMENT OF VALIDITY OF METHODS AND PROCEDURES OF WORK WITH RISKS THAT ARE USED IN PRACTICE, SHOWS THAT THERE ARE PREDOMINATED THE TECHNIQUES, WHICH DO NOT RESPECT SYSTEM NATURE OF TECHNICAL FACILITIES.*

**KEY WORDS:** *technical entity; system concept; system of systems; disasters; interdependences; risk; risk identification; risk analysis; risk assessment; risk management; trade-off with risks; management of risks in time targeted to safe technical entity.*

### 1. Úvod

Na základě současné úrovně znalostí chápeme každé technické dílo jako otevřený složitý systém systémů, tj. jako několik otevřených systémů, které se vzájemně prolínají, a jsou propojené s okolím



[1-3]. Propojení způsobují závislosti, které jsou příčinami specifických zranitelností [3]. Kromě žádoucích propojení vznikají za jistých podmínek i propojení nežádoucí, která vedou k selhání technických děl, která za jistých okolností výrazně poškozují i okolí. Proto je třeba technická díla chápat jako otevřené systémy systémů, které mají rozmanitá aktiva a která se v dynamicky proměnném světě mění [1-3]. Rozmanitost aktiv způsobuje, že za jistých podmínek jsou požadavky na opatření, která zajišťují bezpečnost jednotlivých aktiv, konfliktní, což znamená, že metody používané k řízení rizik zacílené na bezpečnost technických děl musí být multikriteriální [1-5].

V současné době je v pokrokových inženýrských disciplínách **bezpečnost chápána jako vlastnost, která vystupuje na úrovni systému** [2]. Představuje soubor opatření a činností, které zajistí, že systém je bezpečný, přičemž platí dále uvedené souvislosti:

**Spolehlivý systém** je systém, který vykonává požadované funkce v daném místě, daném čase a v požadované kvalitě po celou dobu životnosti.

**Zabezpečený systém** je spolehlivý systém, který je ochráněn proti vnitřním i vnějším pohromám (škodlivým jevům všeho druhu).

**Bezpečný systém** je zabezpečený systém, který ani při svých kritických podmínkách neohrožuje sebe a své okolí.

## 2. Základní pojmy inženýrství pracujícího s riziky

Z logického důvodu je třeba v úvahu vzít posloupnost pojmů, které hrají roli při zajišťování bezpečného technického díla. Je třeba začít od příčin narušení bezpečnosti a pokračovat až k míře narušení bezpečnosti, kterou je kritičnost:

**Pohroma** označuje každý jev, který poškozuje aktiva sledovaného systému, tj. patří do nich i škodlivá propojení a zdroje organizačních havárií. Jejich přehled a charakteristiky jsou v pracích [4-6].

**Ohrožení** je normativně určená velikost pohromy, která se zvažuje při zajišťování bezpečnosti systému. Pohroma s takto definovanou velikostí se nazývá projektová. Při řízení bezpečnosti se vůči větším, tj. nadprojektovým pohromám dělají nouzové, krizové a další plány.

**Nebezpečí** označuje stav systému, při kterém vznik újmy, škody či ztráty na chráněných aktivech má vysokou pravděpodobnost (tj. je téměř jisté, že újma, škoda nebo ztráta vznikne). To znamená, že jde o **označení možnosti** vzniku újmy, ztráty či škody na jednom aktivu či více aktivech. Nebezpečí je určeno vlastnostmi látek, které se nachází v zařízení, objektu či území, anebo vlastnostmi procesů, které probíhají v zařízení, objektu či území. Je bezprostřední, když vývoj nezadržitelně směřuje k pohromě, a tím k vyvolání nouzové situace; a je plíživé, když vývoj směřuje k pohromě nenápadně a bez zřejmých příznaků.

**Riziko** je chápáno jako pravděpodobná velikost ztrát, škod a újmy na chráněných aktivech v konkrétní entitě rozpočtená na jednotku plochy a času. Je závislé na velikosti konkrétní pohromy a místní zranitelnosti.

**Kritičnost** označuje mez, od které dopady rizika jsou závažné až likvidační pro sledovanou entitu, což znamená, že příslušné riziko se musí vždy vypořádat.

Bezpečnost a riziko spolu jistým způsobem souvisí, ale nejsou komplementární veličiny. Snížení rizika znamená zvýšení bezpečnosti, ale obráceně to neplatí [1,2].

Další základní a odvozené pojmy a jejich souvislosti používané v inženýrských disciplínách spojených s rizikem jsou uvedeny v pracích [4,5], další specifické pak v pracích [1-3].

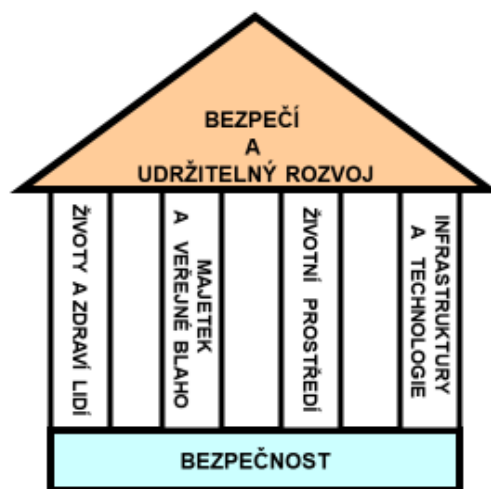
## 3. Postup zvládání rizik technických děl

Uvedeme postupně dílčí úlohy, které musíme vyřešit, jestliže chceme zvládnout jisté riziko a přitom znát zanedbání, kterých jsme se dopustili při výběru modelu řešení. Je třeba začít určením kontextu, ve kterém chápeme rizika a pak pokračovat přes postupy jejich identifikace, analýzy, hodnocení, řízení až k postupům jejich vypořádání.



### 3.1. Kontext chápaní rizik spojených s technickými díly

Nejobecnější kontext je založen na zvažování technického díla jako součásti lidského systému, který má aktiva a procesní model, jež jsou znázorněny na obrázku 1 [1,4,5]. Na základě šetření, která byla provedena při shromažďování podkladů pro práce [1-3], údajů z odborných prací, které jsou citované v pracích [1-5] a zkušeností získaných přímo z šetření v praxi [7] se v technickém sektoru často zvažuje jen kontext technického díla nebo kontext podniku, který technické dílo spravuje a v řadě případů jen kontext výrobního zařízení. Je pochopitelné, že čím užší je kontext, tím větší jsou zanedbání, což v praxi znamená, že jsou z řešení vyloučeny některé zdroje rizik; velmi často se jedná o vyloučení jevů z okolí sledované entity a o vyloučení jevů, které jsou vyvolány špatnými rozhodnutími managementu podniku či správních orgánů [2,7].



Obr. 1. Aktiva lidského systému a procesní model pro zajištění jeho bezpečí[4].

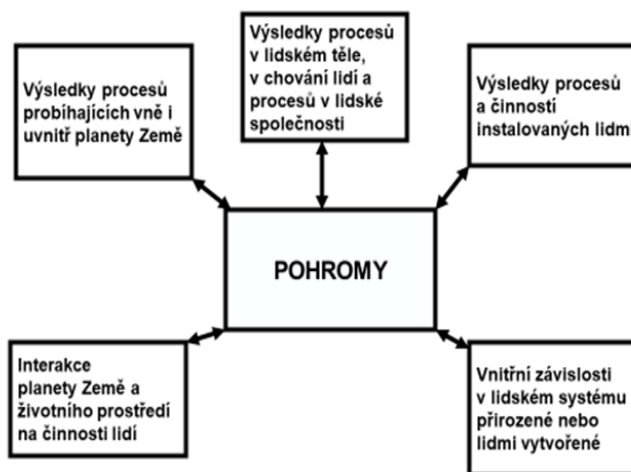
### 3.2. Výběr zdrojů rizik

Na základě šetření, která byla provedena při shromažďování podkladů pro práce [1-3], údajů z odborných prací, které jsou citované v pracích [1-5] a zkušeností získaných přímo z šetření v praxi [7] se v technické praxi používají dále uvedené výběry zdrojů rizik:

- Zdroje rizik určené buď legislativou, anebo zkušeností pracovníka, který předmětný úkol řeší.
- Jen technické zdroje rizik v daném technickém díle. Většinou jde o:
- rizika spojená s materiálem (splnění potřebných parametrů, dodavatelské vztahy – náhradní materiál....),
- rizika spojená s konstrukcí a propojováním komponent a zařízení (nestanovené postupy, přítomné labilní nebezpečné látky....),
- rizika spojená s výrobními postupy, např. při svařování, specifickém obrábění atd.,
- rizika spojená s podmínkami, které jsou nutné pro kvalitní výrobek, např. jistý tlak, jistá teplota či jistá vlhkost okolního prostředí atd.
- Technické zdroje rizik a lidský faktor. Úlohy jsou zaměřené na prevenci špatných technických úkonů v technickém díle. K položkám uvedeným v bodě 2 tak přibývají ochrany proti výskytu špatných úkonů pracovníků.
- Technické zdroje rizik a lidský faktor. Úlohy jsou zaměřené na prevenci technických rizik, špatných technických úkonů a prevenci organizačních havárií v technickém díle (tj. prevenci špatných rozhodnutí, prevenci použití nesprávných postupů atd.).



- Technické zdroje rizik a zdroje rizik spojené s BOZP a s pracovním prostředím. Úlohy řeší jen problémy technického díla a neřeší dopady na okolní prostředí a na konkurenceschopnost a požadavky na zajištění obslužnosti území v delším časovém intervalu.
- Technické zdroje rizik, zdroje rizik spojené s BOZP, pracovním a okolním životním prostředím. Úlohy neřeší dopady technického díla na konkurenceschopnost a požadavky na zajištění obslužnosti území v delším časovém intervalu.
- Zdroje rizik z oblastí technické, propojení zařízení, komponent a systémů – technická integrita, automatizace, vzdělávání a dobré dovednosti, BOZP, ochrany majetku, ochrany dat a informací, ochrany specifických znalostí, know-how apod. Úlohy neřeší dopady vnějšího prostředí na technické dílo, které následně ovlivní konkurenceschopnost technického díla a zajištění obslužnosti území v delším časovém intervalu (např. špatné postupy veřejné správy).
- All Hazard Approach[4-6]. Předmětný výběr zvažuje rizika z pěti základních oblastí uvedených na obrázku 2. Je velmi náročný na data, metody, znalosti, zkušenosti a dobu provedení; vyžaduje systémový přístup, a proto podle hodnocení provedených pro EU v rámci projektu FOCUS má stále při aplikacích v praxi řadu nedostatků [1,6].



Obr. 2. Procesy, jejichž výsledkem jsou pohromy v lidském systému[4,5].

### 3.3. Typ rizika

Na základě šetření, která byla provedená při shromažďování podkladů pro práce [1-3], údajů z odborných prací, které jsou citované v pracích [1-5] a zkušeností získaných přímo z šetření v praxi [7] se v technické praxi používají rizika dílčí, integrovaná a integrální.

**Dílčí riziko** je riziko spojené s jedním aktivem. Dílčí rizika jsou rozmanitá, např. zdravotní rizika, technologická rizika, riziko požáru atd. Pro výpočet dílčích rizik již existuje řada právních předpisů, norem a standardů a s nimi souvisejících podpurných software [5]. **Základní skupiny dílčích rizik zvažovaných v technických projektech a při zajištění bezpečnosti technických děl jsou:**

- Stavebně-technologická a projekční rizika.
- Kreditní rizika.
- Tržní rizika.
- Vnější rizika.
- Provozní rizika.
- Rizika spojená s řízením a rozhodováním.

*Stavebně-technologická a projekční rizika* zahrnují: stavební a projekční rizika; rizika lokality; a rizika chybných technologií, sítí a souvisejících služeb. Stavební a projekční rizika obsahují riziko spojené s



projektovou dokumentáci (správna / špatná, chyby); rizikospojené skontrukci / stavbou; rizikospojené sprekročením stavebních nákladů; rizikospojené se znečištěním lokality / okolí během realizace projektu, které způsobí veřejná správa; rizikospojené se znečištěním lokality/okolí během realizace projektu, které způsobí dodavatel; riziko spojené s vlivem projektu na životní prostředí během životnosti projektu, které způsobí veřejná správa špatným rozhodnutím; a rizikospojené s vlivem projektu na životní prostředí během životnosti projektu, které způsobí dodavatel a provozovatel).

Riziko lokality zahrnuje riziko spojené se stávajícím objektem; rizikospojené s dostupností lokality; rizikospojené s vlastnictvím lokality; rizikospojené se stavem lokality; rizikospojené se sítěmi (utilitami) nacházejícími se na lokalitě (v místě stavby); rizikospojené s územním plánem; rizikospojené se stavebním povolením; rizikospojené s kulturním /archeologickým dědictvím; a riziko spojené s chráněnou krajinnou oblastí.

Rizika spojená s chybnými technologiemi, sítěmi a souvisejícími službami obsahují: riziko spojené s vadou v průběhu realizace projektu; riziko spojené s vadou v průběhu životnosti projektu; riziko spojené s použitím chybné technologie; riziko spojené technologickou nedostatečností; riziko spojené s neočekávaným přerušením dodávky energie, výpadku služeb a podpůrných systémů zajišťovaných soukromým sektorem; a rizikospojené s neočekávaným přerušením dodávky energie, výpadkem služeb a podpůrných systémů zajišťovaných veřejnou správou.

*Kreditní rizika* zahrnují: riziko likvidity; riziko nesplnění závazků / tj. tzv. riziko dostupnosti, které se dále dělí na: riziko spojené s dostupností (nedodržení závazků soukromým sektorem); riziko spojené se selháním protistrany a ztrátou pro veřejnou správu; rizikospojené se selháním protistrany a ztrátou pro dodavatele; riziko spojené s koncentrací (na všechny dodávky je jen jeden dodavatel); a riziko spojené se zamítnutím partnerství (veřejná správa projekt nepodporuje).

*Tržní rizika* zahrnují: riziko poptávky v případě, že dodavatelem je veřejná správa; riziko poptávky v případě, že dodavatelem je soukromý subjekt; riziko zvýhodnění konkurence; a ostatní tržní rizika jako jsou: riziko měnové; riziko inflační; a riziko úrokové.

*Vnější rizika* zahrnují: politická rizika; vyšší moc; a ostatní vnější rizika. Politické riziko zahrnuje: rizikopolitické spojené s národní či mezinárodní situací; riziko defaultu spojené se selháním vlády; a rizikonadnárodní politické spojené s povinnostmi ČR v EU, NATO.

Riziko spojené s vyšší mocí zahrnuje: rizikospojené s přírodní pohromou rozměru katastrofy; rizikospojené s terorismem; a riziko spojené s válkou.

Položka ostatní vnější rizika zahrnuje: riziko legislativní / daňové obecného charakteru spojené se změnou legislativy / daní; riziko legislativní / daňové specifického charakteru; riziko spojené s potřebou dodatečných povolení; a riziko spojené se situací v odvětví / stávky.

*Provozní rizika* zahrnují: rizika související se zařízením; rizika související s lidmi; a rizika spojená s jednáním lidí. Rizika související se zařízením zahrnují: riziko související se zařízením, vstupy (materiálem); riziko spojené s údržbou, opravami, modifikacemi a adaptacemi; a riziko spojené s nízkou zůstatkovou hodnotou. Rizika související s lidmi jsou: riziko spojené s neodpovídajícími pracovními silami; rizikospojené s nezastupitelností; riziko spojené s nedostatkem lidských zdrojů; riziko spojené s pracovními právními spory; a riziko spojené se selháním lidského faktoru.

Rizika spojená s jednáním lidí zahrnují: riziko spojené s podvodným jednáním; riziko spojené s nelegálním jednáním; riziko spojené s bezpečností technologických systémů; a riziko spojené s poškozením, krádeží.

*Rizika spojená s řízením a rozhodováním* zahrnují: smluvní rizika; a ostatní rizika spojená s řízením a rozhodováním. Smluvní rizika zahrnují: riziko spojené s odpovědností třetím stranám; riziko spojené se změnou smlouvy; a riziko spojené s porušením obecně závazných předpisů. Ostatní rizika spojená s řízením a rozhodováním zahrnují: riziko spojené s strategickým rozhodnutím; a riziko spojené s reputací.

V oblasti finanční se používají dále uvedená dílčí rizika:

- Finanční riziko představuje míru snížení hodnoty sledovaného objektu, tj. podniku / majetku / kritické infrastruktury / technologie, které je způsobené živelní či jinou pohromou nebo interakcí možnou v lidském systému. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.





- Kreditní riziko představuje míru snížení hodnoty sledovaného objektu, tj. podniku / majetku / kritické infrastruktury / technologie, které je způsobené tím, že protistrana nesplní existující závazek (nezaplatí úvěr, fakturu, nedodá výrobek apod.). Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
- Tržní riziko představuje míru snížení hodnoty obchodovatelných finančních nároků, tj. zboží / objektů / majetku / kritické infrastruktury / technologie, které je způsobené změnami na trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
- Měnové riziko představuje míru snížení hodnoty deviz, které je způsobené změnami na bankovním trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
- Kurzovní riziko je druh rizika vznikajícího změnou kurzu jedné měny vůči jiné měně. Když investoři a firmy drží statky či provádějí obchodní operace napříč hranicí měnových oblastí, vystavují se měnovému riziku, proti kterému se však mohou zajistit.
- Úrokové riziko představuje míru snížení hodnoty majetku, tj. zboží / objektů / budov / kritické infrastruktury / technologie, které je způsobené změnami na finančním trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
- Akciové riziko představuje míru snížení hodnoty akcií, které je způsobené změnami na burze. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
- Komoditní riziko představuje míru snížení ceny obchodovatelných komodit, které je způsobené změnami na trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
- Likviditní riziko představuje míru ztráty schopnosti realizovat určitý obchod v dané chvíli, což je způsobené: platební neschopností či insolvencí podnikatele (vlastní nelikvidita); neexistencí protistrany pro obchod (nelikvidita trhu); a změnami na trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.

**Integrované riziko** – představuje součet nebo jinou agregaci dílčích rizik. Používá se např. v BOZP [5].

**Integrované riziko** je založeno na systémovém pojetí entity a zahrnuje propojení mezi aktivy a komponentami technického díla [1,2]. Je dané vztahem

$$R(H) = \left[ \sum_{i=1}^n A_i(H) Z_i(H) + \sum_{i=1}^n \int_0^T \int_S F(H, A_i, P_i, O, t) dS dt \right] \cdot \tau^{-1}$$

ve kterém je ohrožení spojené s danou pohromou v místě objektu;  $A_i$  jsou hodnoty sledovaných aktiv pro  $i = 1, 2, \dots, n$ ;  $Z_i$  jsou zranitelnosti aktiv pro  $i = 1, 2, \dots, n$ ;  $F$  je ztrátová funkce;  $P_i$  jsou pravděpodobnosti výskytu poškození aktiv pro  $i = 1, 2, \dots, n$  – jde o podmíněné pravděpodobnosti;  $O$  zranitelnost ochranných opatření;  $S$  velikost sledovaného objektu;  $t$  je čas měřený od vzniku škodlivého jevu;  $T$  je čas, po který vznikají ztráty; a  $\tau$  je perioda opakování pohromy.

Je zřejmé, že pro dlouhodobé zajištění bezpečného technického díla je třeba zvažovat integrované riziko. Jelikož ve výše uvedeném vzorci je neznámá ztrátová funkce, tak v pracích [1,2] jsou uvedené postupy používané v praxi.

Je také třeba poznamenat, že určení jednotlivých typů rizik se také liší náročností na data a metody jejich zpracování [4,5].

### 3.4. Způsoby vypořádání rizik

Na základě šetření, která byla provedená při shromažďování podkladů pro práce [1-3], údajů z odborných prací, které jsou citované v pracích [1-5] a zkušeností získaných přímo z šetření v praxi [7] se v technické praxi používají způsoby:



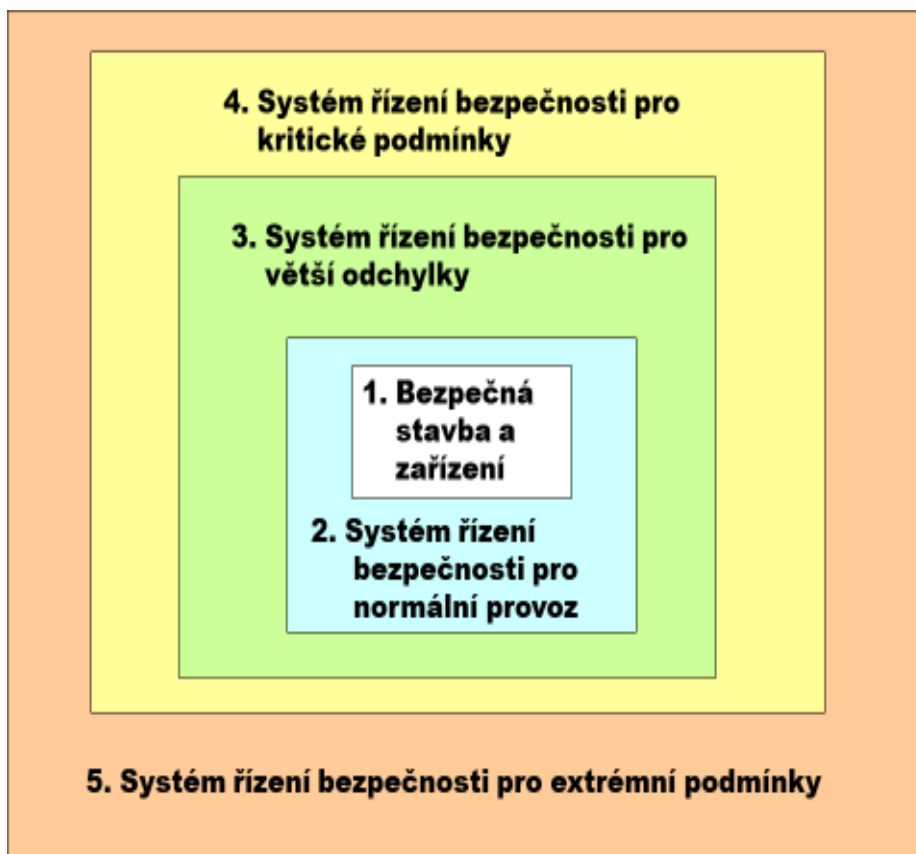
- rizika se určují a vypořádávají až po vytvoření produktu[1]. Předmětný způsob má nebezpečí, že některá závažná rizika, která lze snížit jen specifickými technickými opatřeními v zadání projektu technického díla, již lze snížit jen organizačními opatřeními, která jsou však méně účinná než opatření technická [1-3,7] (např. problémy dálnice D8),
- vyjmenovaná rizika se zvažují od začátku projektu technického díla až do jeho odstavení z provozu. Předmětný způsob závisí na požadavcích legislativy, znalostech projektantů, konstruktérů a provozovatele,
- rizika se zvažují od začátku projektu technického díla a používá se v praxi ověřená strategie založená na přístupu Defence-In-Depth, který je znázorněn na obrázku 3. Předmětný způsob vyžaduje systémové myšlení, mnohaoborové a mezioborové znalosti a zkušenosti[1,2,7].

### 3.5. Práce s riziky, aplikace TQM a Coaseho teorému

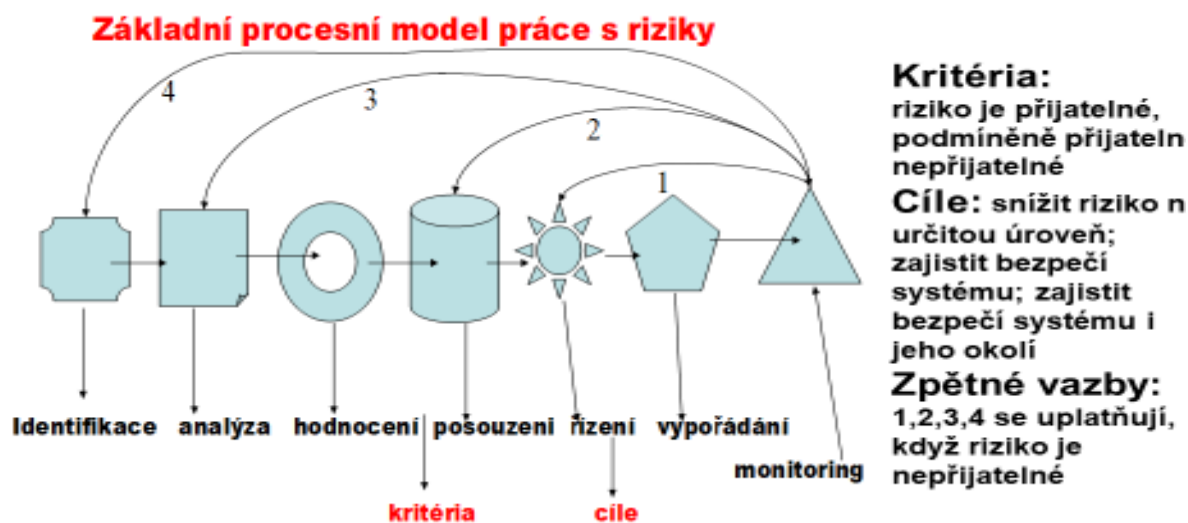
Zajištění bezpečnosti technických děl a všech dalších entit závisí na kvalitě práce s riziky a na disponibilních možnostech jak managementu a personálu technických děl, tak veřejné správy [2,4]. Zvládání rizik v čase a místě vyžaduje znalosti, schopnosti, finanční, materiální, technické a lidské zdroje. Proto se dále zabýváme nejenom samotnou prací s riziky, ale i praktickými postupy, které se používají při rozhodování o vypořádání rizik.

#### 3.5.1. Práce s riziky

Na základě údajů z odborných prací, které jsou citované v pracích [1-5] a zkušeností získaných přímo z šetření v praxi [7] práci s riziky zacílenou na bezpečná technická díla lze popsat procesním modelem, který je na obrázku 4 [1-3,5]. Další modely jsou uvedeny v práci [5], popř. v pracích, které jsou v předmětné práci citovány.



Obr. 3. Pětistupňový systém řízení bezpečnosti složitého objektu [1].



Obr. 4. Procesní model práce s riziky. Kritéria = podmínky, které stanovují, kdy je riziko přijatelné, podmíněně přijatelné nebo nepřijatelné. Cíle označují žádoucí stavy. Čísla 1,2,3,4 označují zpětné vazby, které se používají, když monitoring ukáže, že nejsou splněny stanovené požadavky na bezpečnost [3].

Je zřejmé, že nejsme-li schopni riziko identifikovat a analyzovat, tak nejsme schopni se proti němu účinně bránit. Chyba, které se dopustíme při analýze rizika, se přenáší do nouzových a krizových plánů, do plánů kontinuity a snižuje jejich hodnotu ve vztahu k plánovaným opatřením směřujícím především k ochraně lidských životů a zdraví, ale i v oblasti akceschopnosti záchranných složek podílejících se na realizaci záchranných operací.

Úkolem řízení rizika je najít optimální způsob, jak zjištěná rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Úkolem inženýrství rizika je pak navržená opatření a činnosti pro vypořádání rizik způsobem stanoveným řízením rizik, dle disponibilních možností a dle podmínek v místě řešení realizovat a zajistit jejich spolehlivost a funkčnost. Snižování rizika je prakticky vždy spojeno se zvyšováním nákladů a s nároky na znalosti. Řízení rizika je tedy vedeno snahou najít hranici, na kterou je únosné riziko ještě snížit, aby vynaložené náklady byly společensky přijatelné.

Důležitou roli v práci s riziky hraje jak hodnocení rizika, tak posouzení rizika. Dle požadavků uvedených v pracích [5,8,9] u hodnocení jde o splnění požadavků: provedení hodnocení v požadované šíři a kvalitě v souladu s přijatou metodikou hodnocení; úplnost hodnocení; zahrnutí nejnovějších poznatků vědy; odhad nejistot v případě použití extrapolací; jednotné vyjádření charakteristik rizika; a průhlednost provedení procesu hodnocení rizik.

U posouzení rizika jde o správné ocenění přijatelnosti rizika a o volbu správné reakce na riziko. Přijatelnost rizika je ve skutečnosti výsledkem porovnávání několika typů přijatelnosti – technická přijatelnost (spolehlivost a složitost technologií, strojů a zařízení), ekonomická přijatelnost (náklady) a socio-politická přijatelnost (vnímání rizik) [1-3,5]. K posouzení rizika se v praxi používá nejčastěji matice rizika ve tvaru na obrázku 5 [5].





|                                             |   | Kategorie závažnosti dopadů nehod |   |   |   |   |
|---------------------------------------------|---|-----------------------------------|---|---|---|---|
|                                             |   | 5                                 | 4 | 3 | 2 | 1 |
| Kategorie závažnosti četností výskytu nehod | A |                                   |   |   |   |   |
|                                             | B |                                   |   |   |   |   |
|                                             | C |                                   |   |   |   |   |
|                                             | D |                                   |   |   |   |   |
|                                             | E |                                   |   |   |   |   |

Obr. 5. Matice rizika[5].

V souladu s veřejným zájmem je třeba, aby přijatelnost rizika měla sociální rozměr. Proto je třeba zvažovat:

- Pro koho má být riziko přijatelné?; pro původce rizika, pro politiky nebo pro veřejnou správu?
- Kdo stanoví přijatelnost?; politici rozhodují o tom, co je zákonné, a tudíž by neměli rozhodovat o tom, co je přijatelné,
- Zda při stanovení přijatelnosti rizik byla diskutována aktuálně tolerovatelná rizika, netolerovatelné prahové hodnoty a postoje veřejnosti k rizikům.

Rizika byla, jsou a budou a neustále se budou objevovat nová. Řízení rizik proto vyžaduje rozměr a měření rizika, které berou v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Proto se také používá definice rizika uvedená v odstavci 2.

Řada současných technik na určování rizika nereprezentuje holistický přístup a většina z nich nezvažuje vazby a toky mezi prvky systému za zranitelné položky, které zvyšují škody, ztráty a újmy. Často se při alokaci úkolů spojených s vypořádáním rizika zapomíná na skutečnost, že zvládání rizik spojených s technickým dílem je rozdělené na všechny úrovně řízení technického díla a také na lokální, regionální i státní úroveň veřejné správy [2,5].

Pro správce a provozovatele technických děl se jeví vhodná kategorizace přijatelnosti rizik, kterou používá OSN; její popis je v práci [4]. Na závěr je třeba připomenout, že ignorování či podceňování řízení rizik je důvodem většiny problémů lidské společnosti.

### 3.5.2. Řízení rizik stanovené TQM a Coaseho teorém

V našich podmínkách se používá typ řízení Total Quality Management (TQM)[10]. Pro jeho úspěšnost byly vytvořeny ISO normy třídy 9000, 14000 apod. Přístup TQM spočívá na požadavku, že na procesu zlepšování kvality entity se podílí všichni zaměstnanci, od řadových zaměstnanců až po nejvyšší řídicí pracovníky entity. Proces zlepšování jakosti (tj. v jeho nejvyšší úrovni jde de facto o zvyšování integrální bezpečnosti) vychází z impulsů, které vychází z potřeb zákazníka / občana.

TQM vychází z předpokladu, že trvalá kvalita (jakost) výrobků a služeb se nedá zajistit příkazy, kontrolou, dílčími programy, organizačními nebo ekonomickými opatřeními, ale cíleným hledáním, měřením a hodnocením příčin toho, proč se produktivita a kvalita nezvyšuje; de facto jde o jistou kulturu bezpečnosti (jinými slovy způsob aplikace opatření a činností lidí). Pozornost se zaměřuje na procesy probíhající v entitě. Při implementaci TQM se přihlíží na specifika entity, protože z důvodu účinnosti všechna opatření musí odpovídat struktuře entity, tj. musí být místně specifická.

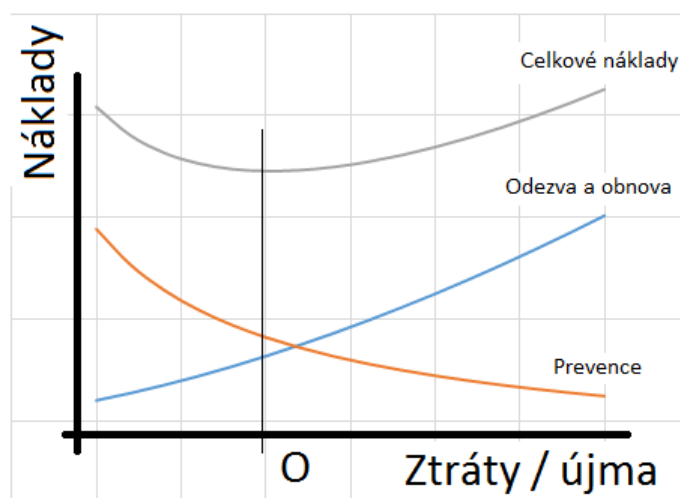
Výstupy z procesu řízení rizik pro potřeby správného řízení podle TQM jsou:

1. *Seznam vyhodnocených rizik* (risk assessment document) - zde se zaznamenávají veškeré informace o příslušném riziku.
2. *Seznam rizik vyžadujících nejvyšší pozornost* (top risks list) - obsahuje seznam vybraných rizik, jejichž řešení má nejvyšší nároky na zdroje a čas.



### 3. Seznam neaktuálních / vyřešených rizik (retired risk list) - slouží jako historický odkaz pro budoucí rozhodování.

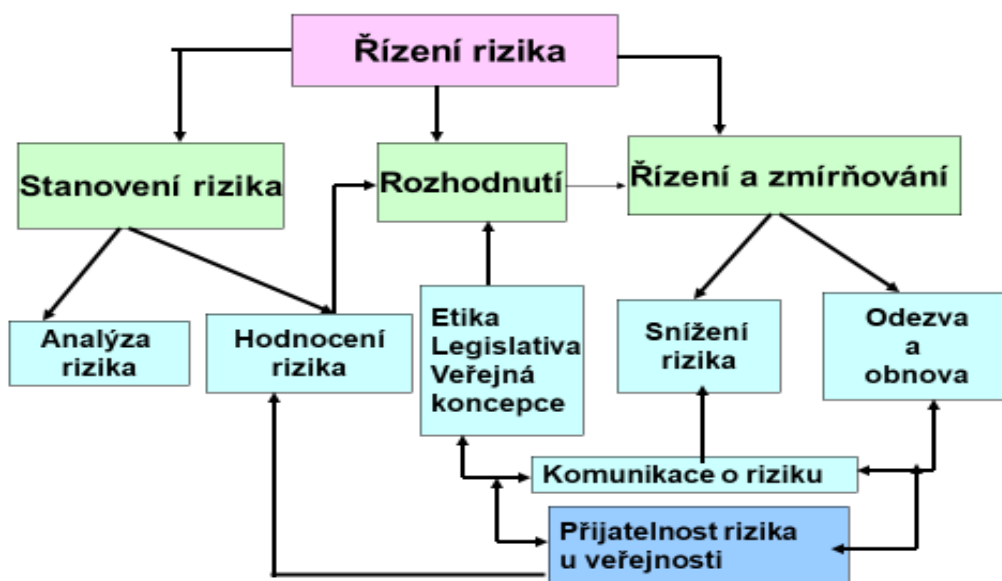
Technika samotného řízení rizik z důvodu hospodárneho nakládání se silami, zdroji a prostředky před každou fází práce s riziky formálně přezkoumává řízení a vypořádání rizik v kontextu přínosů a nákladů na výstupy. Coaseho teorém [11] se používá pro stanovení ekonomického optima v nákladech na vypořádání rizik.



Obr. 6. Coaseho teorém- Ekonomické optimum nákladů na prevenci, odezvu a obnovu [11].

### 3.6. Řízení a vypořádání rizik technického díla

Nejprve si je třeba uvědomit, že řízení a vypořádání rizik technického díla není úkolem jednotlivce, ani úkolem jedné organizace či jednoho sektoru. Jde o kolektivní zacílené úsilí všech zúčastněných. V uvedeném smyslu obrázek 7 ukazuje model řízení a vypořádání rizik [5]. Ze základní struktury modelu je zřejmé, že:



Obr. 7. Základní rámec pro řízení a vypořádání rizik [5].



- stanovit riziko mohou odborníci, kteří mají znalosti, data a schopnost aplikovat vhodné metody,
- rozhodnout o riziku mohou jen ti, co mají příslušné oprávnění (tj. právně určený subjekt veřejné správy nebo v případě objektu (tj. technického díla) právně určený subjekt podniku, jemuž entita patří,
- řízení a zmírňování, tj. vlastní aplikace opatření a činností vedoucí ke zvládnutí rizika mohou jen odborníci, kteří mají příslušné znalosti, schopnosti, vybavení, zdroje a prostředky.

Veřejnost je platným účastníkem při vypořádání rizik, protože jde o její bezpečí a kvalitu života. Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá v rozdělení opatření a činností na vypořádání rizik do kategorií, ve kterých se příslušná část rizika zajistí tak, že:

- preventivními opatřeními se sníží nebo odvrátí realizace rizika,
- účelovými preventivními (zmírňujícími) opatřeními odezvy a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se zmírní dopady, tj. sníží se nebo se odvrátí nepřijatelné dopady při realizaci rizika,
- pojištěním se pokryje část možných ztrát a škod při realizaci rizika,
- vytvořením rezervy na odezvu a obnovu a záloh se zajistí přežití lidí, kontinuitu provozu technického díla, objektu a území,
- přípravou plánu pro odezvu na nepředvídané situace (Contingency Plan) se zajistí provedení reakce na realizaci rizik neřiditelných nebo příliš nákladných, anebo málo častých.

K tomu se rovněž připojuje rozdělení zvládání rizik mezi všechny zúčastněné [1,2,5]. Rozdělení provedení konkrétních opatření a činností ve správném řízení se provádí tak, že se vychází z toho, že za zvládání rizik odpovídají všichni zúčastnění a že zvládání konkrétního rizika je nejlépe přidělit tomu subjektu, který je na to nejlépe připraven [5]. Je zřejmé, že toto je však možné jen v organizaci, ve které je kvalifikované projektové a procesní řízení, tj. činnosti a opatření se aplikují na základě znalostí, a to věcných i z oblasti řízení (tj. činnosti jsou vzájemně provázané, nejsou chyby v komunikaci, každý zúčastněný ví, co má dělat a jak to má dělat) [5].

Pro stanovení rizik technického díla je důležité:

- jaká chráněná aktiva jsou sledována,
- jaké pohromy mohou vzniknout v daném místě / území / objektu a způsobit dopady na chráněná aktiva,
- jak je chápán proces, jehož výsledkem je realizace rizika (výskyt nepřijatelných dopadů jisté pohromy, výskyt kombinace malé pohromy a selhání bezpečnostních systémů nebo náhodná kombinace malých jevů,
- od jaké úrovně škod jsou dopady nepřijatelné.

V praxi používáme několik úrovní analýzy rizik:

- A – předběžná analýza rizika,
- B – standardní, rychlá a méně přesná analýza rizika,
- C – detailní analýza rizika v souhrnném kontextu,
- D – individuální a specifická analýza rizika.

Jednotlivé úrovně se liší požadavky na kvalifikovaná data, jejich kvalifikované zpracování a vyhodnocení; největší nároky jsou vyžadovány při strategickém plánování zacíleném na bezpečný systém v dlouhodobém časovém měřítku.

Podle cíle vyjednávání s riziky je nutno, jak již bylo výše uvedeno, odlišovat metody, které jsou vhodné pro: identifikaci rizika; stanovení hodnoty rizika, ve kterém jde o přesný údaj pro potřeby



strategického rozhodování; a stanovení hodnoty rizika pro potřeby kontroly rizika konkrétního procesu v čase a prostoru, při kterém lze použít míru (a to i verbální) a o taktické a operativní rozhodování. Aby hodnoty rizika měly jasnou vypovídací hodnotu, tak je důležité mít nejenom nástroj, ale jasně definovanou hodnotovou stupnici jak pro klasifikaci dílčích položek, dle kterých stanovujeme úroveň rizika, tak pro souhrn těchto položek.

Aby řízení / správa organizace mohla pracovat účinně s riziky, je třeba stanovit postup pro stanovení rizik právním předpisem a zároveň je třeba stanovit hodnotové stupnice, dle kterých se interpretují výstupy z nástrojů na stanovení rizik v organizaci, tj. je třeba určit, co je přijatelné, co je podmíněně přijatelné a co je nepřijatelné. Mezi nástroji pro stanovení rizik je třeba odlišit sofistikované nástroje pro odbornou sféru a nástroje pro řízení / správu organizace, pro kterou jsou nejvhodnější kontrolní seznamy.

Při práci s riziky je důležité aplikovat výsledky poznání, tj. aby řízení dosáhlo cílů, je nutné:

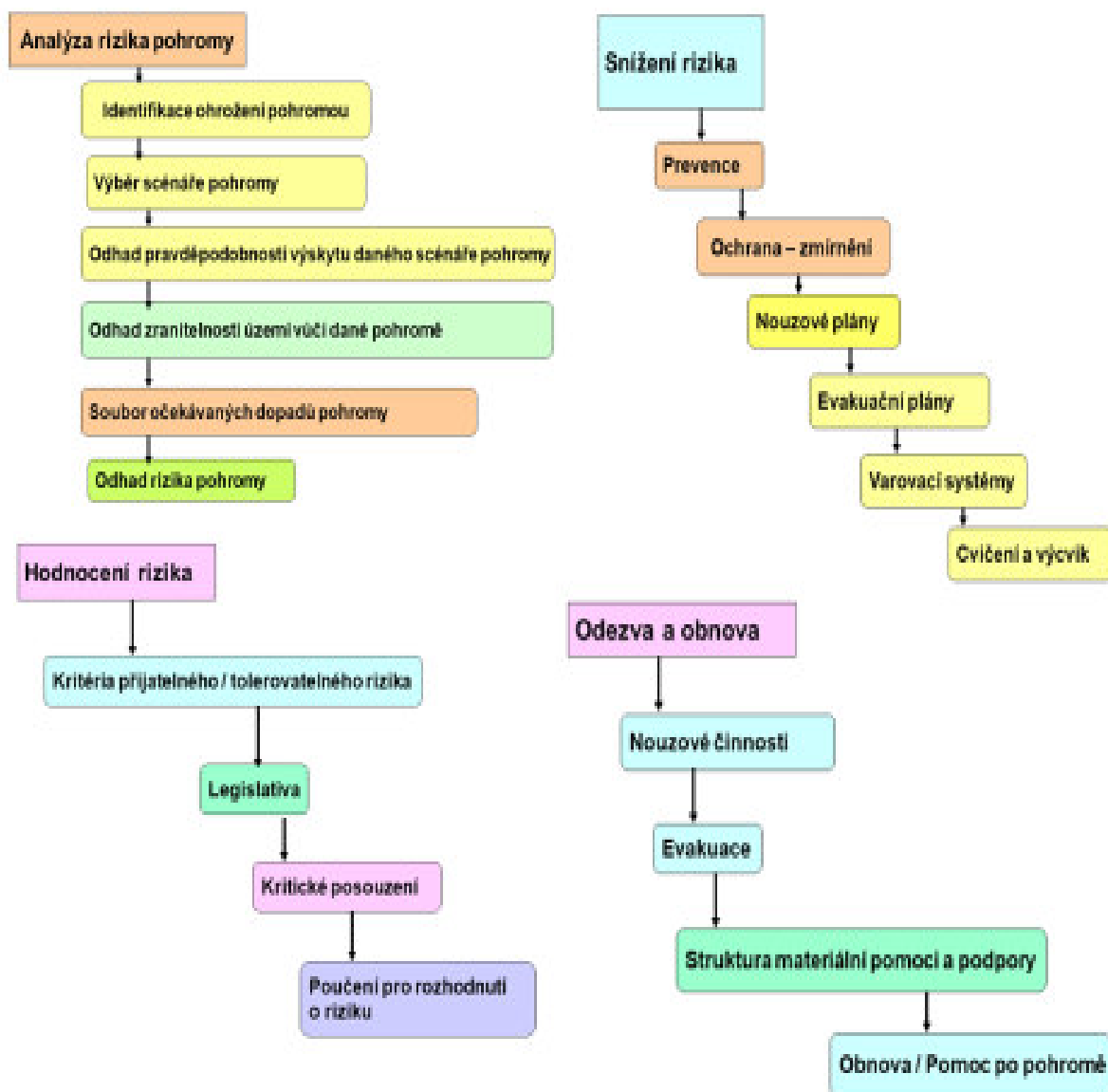
- používat jen podklady získané na základě kvalifikovaných dat, která splňují požadavky na reprezentativní datové soubory (úplnost, ocenění nejistot, vypořádání s neurčitostmi v datech pomocí specifických matematických přístupů),
- aplikovat správné metody rozhodování, které jsou adekvátní problému, o kterém se rozhoduje.

Dle zásad uvedených v pracích [5,8,9] platí, že pro:

- strategické řízení entity je třeba používat integrální riziko, a pro jeho zjištění ověřené reprezentativní datové soubory, ověřené metody pro zpracování dat a ověřené metody pro rozhodování, protože na tomto úseku je důležitá dlouhodobá udržitelnost,
- střednědobé (taktické) řízení možno používat integrované riziko, a pro jeho zjištění méně přesná data, metody zpracování dat i metody rozhodování (je možné použít software) s tím, že při rozhodování se budou respektovat záměry dané strategickým řízením,
- operativní řízení je možno používat dílčí rizika a na základě cíleně získaných znalostí a zkušeností použít naučené a procvičené postupy a nouzové situace zvládnout s tím, že se především soustředíme na životy a zdraví lidí a na další chráněná aktiva v technické entitě a jejím okolí.

V práci [5] jsou podrobně popsány všechny položky zobrazené na obrázku 7.

Obrázek 8 uvádí modely základních činností, které jsou podrobně popsány v [5].



Obr. 8. Modely základních činností pro řízení a vypořádání rizik[5].

Hodnocení dopadů pohrom v konkrétním místě je základní součástí jakéhokoliv pokusu o kvantifikaci a hodnocení rizika. Hodnocení rizika je strukturovaná procedura, která se pokouší odpovédět na dále uvedené otázky:

- jaké ztráty, škody a újmy budou na chráněných aktivech?
- jak často se to stane?
- jak zareagují bezpečnostní systémy ve sledovaném objektu, tj. v technickém díle či území?
- jaké ztráty, škody a újmy budou na chráněných aktivech, když selžou bezpečnostní systémy v technickém díle či území?

Na základě šetření, která byla provedená při shromažďování podkladů pro práce [1-3], údajů z odborných prací, které jsou citované v pracích [1-5] a zkušeností získaných přímo z šetření v praxi [7] v technické praxi platí:

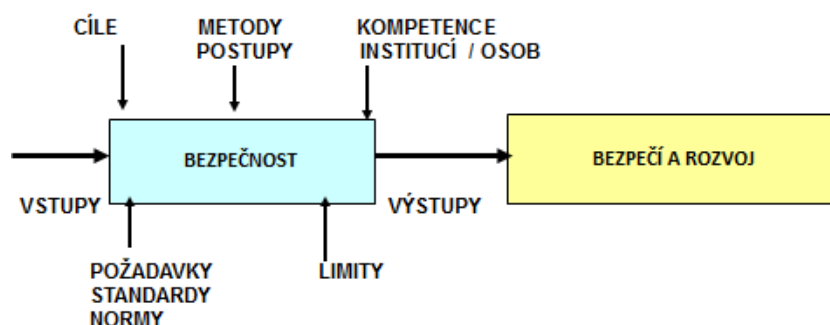




- Hodnocení rizik, která jsou spojená se strategickými cíli a operacemi musí zahrnovat faktory: externí a interní; sociálně – politické; technické a ekonomické. Musí brát v úvahu, že z hlediska zajištění rozvoje je třeba: prosazovat prevenci, tj. snížení zranitelnosti objektu, a tím i snížení rizik; pravidelné hodnocení rizik a sledování jejich aktuálnosti; prosadit změny specifických úprav určité činnosti; a revidovat adekvátnost hodnocení rizik.
- Sociálně – politická rizika jsou obtížně kvantifikovatelná, např. politická stabilita, dopad teroristického útoku apod. Často se interní sociálně – politické faktory odlišují od externích (viz názor české a rakouské veřejnosti na jadernou elektrárnu Temelín). V dosavadní praxi se při jejich sledování používá:
  - sociologický přístup, který spočívá v tom, že se vytváří popis povahy rizika z pohledu sociálních skupin a vztahů se zaměřením na ekologická a sociální rizika a na aktivizaci veřejného mínění,
  - politická analýza, která tato rizika hodnotí pragmaticky a hledá jejich ekonomické dopady,
  - analýza rozložení rizik ve společnosti, která spočívá v identifikaci původce (zdroje) rizika, způsobu „šíření“ (realizace) rizika a „spotřebitele“ (skupiny lidí, která je postižena dopady realizace) rizika.
- Technická rizika lze kvantitativně vyjádřit např. odchýlením od standardů určitého technického parametru, předpisů, norem apod. Není přesné, protože normy odpovídají mediánu  $\pm \sigma$ , 68.5% případů. Tam, kde jde o vysokou bezpečnost, tam se nemohou použít běžné metody, pro které jsou software [1,3].
- Ekonomická rizika lze rovněž kvantitativně postihnout, je však zapotřebí zvažovat nejen vzniklé situace, ale i předpokládaný hospodářský vývoj a politiku vlády. V makroekonomice se jedná o ekonomickou stabilitu země, směnné kurzy, dovozní a vývozní politiku, daňovou politiku apod. V mikroekonomice se může při jejich zanedbání zhoršovat ekonomická situace a platební schopnost podniků, a tím schopnost plnit závazky vůči zahraničním a domácím partnerům. Např. dochází k různému plnění vládních trendů v různých zemích a k různým změnám portfolia produktů v závislosti na uplatněných tendencích.
- Kategorii zvládání rizika lze definovat jako výběr a implementaci nejvhodnějších regulačních činností, na podkladě předcházejících výsledků a různých vstupů v podobě: rizikové analýzy; dostupné řídicí (kontrolní) technologie; analýzy metodou nákladů a užitků CBA (Cost-Benefit Analysis); rizika, přijatelnosti počtu případů; politické analýzy; a sociálních a politických faktorů [8].

#### 4. Řízení rizik v čase

Ze systémového hlediska je zajištění bezpečnosti základním požadavkem na systém jako celek, nikoli jen požadavkem na jeho komponenty, a poměrně snadno se dá odvodit systémové schéma řízení bezpečnosti v určité situaci uvedené na obrázku 9. Z obrázku je zřejmé, že čím jaká opatření používáme k zajištění bezpečnosti, tím určujeme výsledek, tj. bezpečí jako stav systému.



Obr. 9. Procesní model vytváření aktuální bezpečnosti, jeho vstupy a výstupy[3].



Rizika jsou inherentní vlastností lidského systému i každého technického díla, a proto je třeba, je řídit během celé doby životnosti technického díla. Cílem řízení rizik je zajistit konkurenceschopnost technického díla dnes i v budoucnosti, tj. jde o určení prioritních rizik (viz TQM – požadavek norem) a jejich správné řízení. Řízení rizik musí zajistit konkurenceschopnost produktu při podmínkách: normálních; abnormálních i kritických.

Na základě současného poznání, shrnutého v pracích [1-5], systém řízení bezpečnosti (tzv. SMS – Safety Management System) komplexního objektu je postaven na zásadách procesního řízení a zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepříjemných dopadů v území. Zpravidla se týká řady otázek, kromě jiného i organizace, pracovníků, identifikace a hodnocení ohrožení a z nich plynoucích rizik, řízení chodu organizace, řízení změn v organizaci, nouzového a krizového plánování, monitorování bezpečnosti, auditů a přezkoumávání. Jeho model je na obrázku 10.



Obr. 10. Model řízení bezpečnosti komplexního kritického objektu v čase. Procesy: 1- koncepce a řízení; 2 - administrativní postupy; 3 - technické záležitosti; 4 - vnější spolupráce; 5 - nouzová připravenost; a 6 - dokumentace a šetření havárií[1].

Proces řízení se soustřeďuje na šest procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií. Uvedené procesy se dále dělí na podprocesy:

- První proces se skládá z podprocesů pro: celkovou koncepci; dosahování dílčích cílů bezpečnosti; vedení / správu bezpečnosti; systém řízení bezpečnosti; personál a zahrnuje úseky pro: řízení lidských zdrojů, výcvik a vzdělání, vnitřní komunikaci / informovanost a pracovní prostředí; revize a hodnocení plnění cílů v bezpečnosti.
- Druhý proces se skládá z podprocesů pro: identifikaci ohrožení od možných pohrom a hodnocení rizika; dokumentaci postupů (včetně systémů pracovních povolení); řízení změn; bezpečnosti ve spojení s kontraktory; a dozor nad bezpečností výrobků.
- Třetí proces zahrnuje podprocesy pro: výzkum a vývoj; projektování a montáže; inherentně bezpečnější procesy; technické standardy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů.
- Čtvrtý proces obsahuje podprocesy pro: spolupráci se správními úřady; spolupráci s veřejností a dalšími zúčastněnými (včetně akademických pracovišť); a spolupráci s dalšími podniky.



- Pátý proces obsahuje podprocesy pro: plánování vnitřní (on-site) připravenosti; usnadnění plánování vnější (off-site) připravenosti (za kterou odpovídá veřejná správa); a koordinaci činností resortních organizací při zajišťování nouzové připravenosti a při odezvě.
- Šestý proces má podprocesy pro: zpracování zpráv o pohromách, haváriích, skoro nehodách a dalších poučných zkušenostech; vyšetřování škod, ztrát a újm a jejich příčin; a odezvu a následné činnosti po pohromách (včetně aplikace poučení a sdílení informací).

Koordinace procesů je zacílena na zajištění bezpečného objektu za podmínek normálních, abnormálních a kritických. Koordinace je v daných souvislostech chápána jako řízený proces, jehož cílem je vytvořit a provozovat technické dílo v potřebné kvalitě; sleduje procesy v prostoru, čase, personálu, materiálu, financích i dokumentech [1,2].

Pro podporu systému řízení bezpečnosti je třeba dle údajů jak v pracích [1-5], tak v pracích v nich citovaných, zpracovat řadu podpůrných nástrojů jako jsou: bezpečnostní plány, vnitřní a vnější nouzové plány, plány kontinuity a krizové plány. V praxi se velmi osvědčily plány řízení prioritních rizik [2]. Předmětné plány mají tabelární formu, která obsahuje: oblast rizika; popis rizika; ocenění rizika; a opatření pro zvládnutí rizika. Oblast rizika se zpravidla dělí na podoblasti: organizační; technickou; personální; vnějších faktorů; a kybernetickou. Popis rizika obsahuje zásadní dopady a jejich důsledky na sledovaná aktiva. Oblast ocenění rizika obsahuje výsledek hodnocení pravděpodobnosti výskytu a výsledek ocenění dopadů na aktiva dle stanovených stupnic (právě zde je v praxi nejvíce chyb – stupnice jsou jen verbální a není vyznačen vztah ke škodám na aktivech [2]). Oblast opatření na zmírnění rizika obsahuje taxativně: opatření, které se udělá při realizaci rizika; stanovení jak a podle čeho se opatření udělá; a kdo opatření udělá (tj. odpovědnost za provedení). Příklady jsou v práci [2].

## **5. Norma ČSN ISO 31000**

Základní systém pro řízení rizika stanovuje norma ČSN ISO 31000. Předmětná norma je mezinárodní a stanovuje řadu principů, které je třeba naplnit, aby bylo řízení rizik efektivní. Doporučuje, aby organizace rozvíjely, implementovaly a kontinuálně zlepšovaly rámec, jehož účelem je integrovat proces pro řízení rizik do svého celkového vedení, strategie a plánování, managementu, procesů podávání hlášení, politik, hodnot a kultury. Norma se opírá o projektové a procesní řízení v entitě. Její model je na obrázku 11.

Podle citované normy kvalifikované řízení rizik:

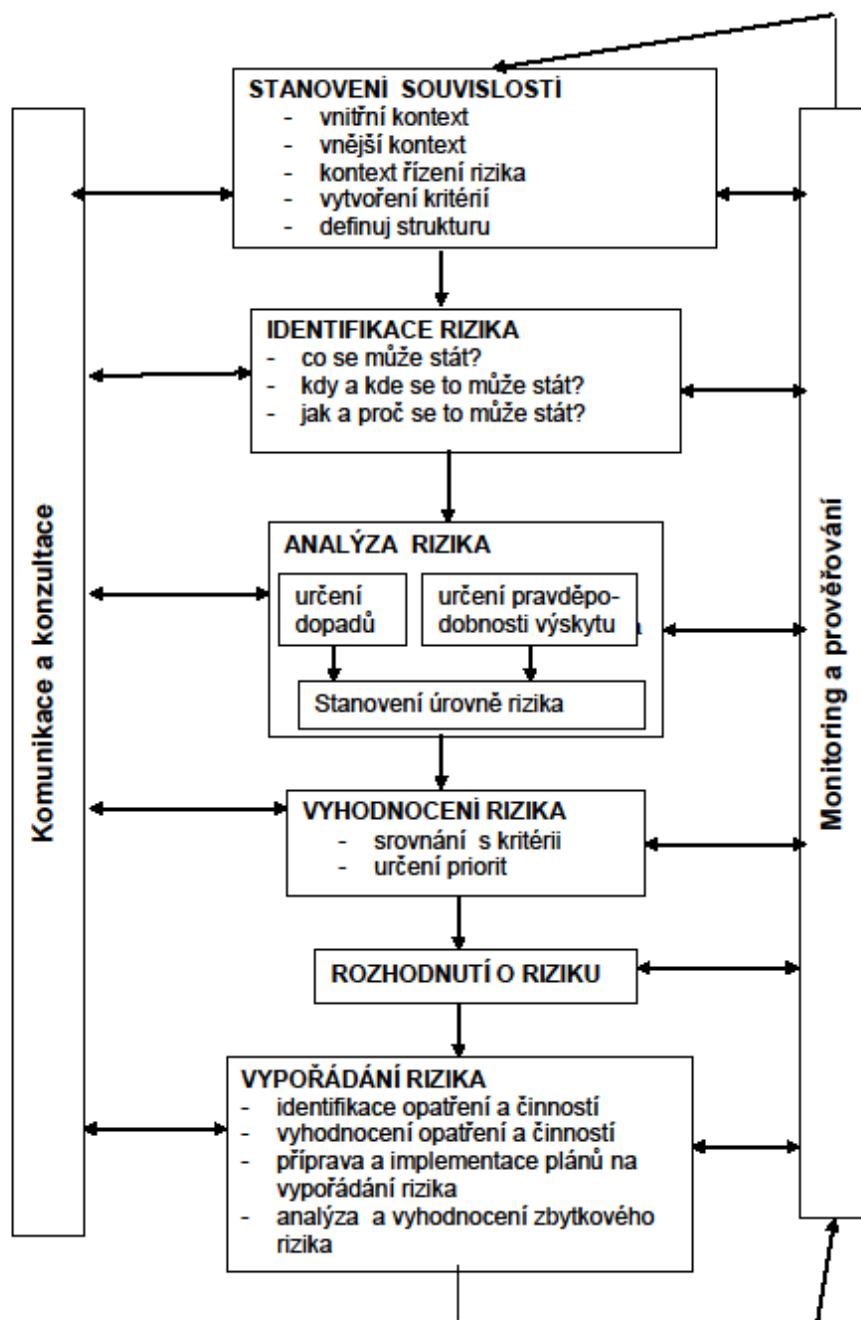
- vytváří hodnoty, protože přispívá k prokazatelnému dosahování cílů jako zlepšení zdraví, bezpečí, kvality životního prostředí, účinnosti procesů a činností atd.,
- je nedílnou součástí procesů, které probíhají v systému, protože za ní odpovídá řídicí struktura systému a je nedílnou součástí všech procesů, z nich složených projektů v objektu i řízení změn,
- je součástí rozhodovacích procesů v systému, čímž pomáhá rozhodovat podle důležitosti a rozpoznávat alternativní způsoby řešení problémů,
- je realistické, protože se explicitně zabývá nejistotou i neurčitostí jak v podmínkách, v nichž se systém nachází, tak v procesech, které v objektu i vně probíhají,
- je systematické, uspořádané a včasné, čímž zajišťuje účinnost opatření a činností,
- je založeno na nejlepších dostupných informacích, což zajišťuje aktuální řešení založené na znalostech,
- je přizpůsobené systému, tj. je místně specifické, což zaručuje jak hospodárnost, tak účinnost,
- bere v úvahu lidské a kulturní faktory v systému, což ovlivňuje jeho přijatelnost u zúčastněných,
- je transparentní a komplexní, což zvyšuje jeho spolehlivost,



- je dynamické, opakovateľné a reaguje na zmeny v systéme, čo zaručuje jeho aktuálnosť a napomáha neustálemu zlepšovaniu a rozvoju systému.

Rámec řízení rizik zahrnuje:

- Pochopení systému a jeho souvislostí. V oblasti vně systému je třeba sledovat především kulturní, politické, právní, finanční, technologické, ekonomické, přírodní a konkurenční aspekty prostředí. V oblasti vnitřní se jedná především o kvalitu zdrojů a znalostí (např. kapitál, čas, lidé, procesy, systémy a technologie), informační systémy, informační toky a rozhodovací procesy (jak oficiální, tak neoficiální), vnitřní zainteresované strany, hodnoty, kultura a řídicí struktura systému.
- Politiku řízení rizik. Politika řízení rizik určuje vazby mezi řízením rizik, cíli systému a dalšími politikami (je upřednostněna nebo je na posledním místě při rozhodování; jak se řeší konflikty; jaké metody řízení se používají; jaké nástroje podporují řízení rizik atd.
- Integraci výsledků řízení rizik do řídicích procesů. Aby řízení rizik bylo efektivní a účinné, musí být obsaženo ve všech směrnících a realizačních procesech, které v systému probíhají. Patří do strategického plánování a do politiky rozvoje.
- Stanovení odpovědnosti za opatření a činnosti spojené s řízením rizik.
- Zdroje nutné pro řízení rizik včetně znalostí, dovedností, zkušeností a kompetencí.
- Stanovení mechanismů pro interní komunikaci a podávání zpráv o rizicích a jejich zvládnutí.
- Stanovení mechanismů pro externí komunikaci a podávání zpráv o rizicích a jejich zvládnutí.



Obr. 11. Schéma pro řízení rizika [5].

Pro implementaci řízení rizik je nutné:

- Stanovit vhodnou strategii a politiku zařadit je do všech procesů v systému.
- Proces řízení rizik začlenit do všech významných úrovní a funkcí systému, tj. musí být součástí všech předpisů a směrnic pro procesy v systému.

Kritéria pro posuzování rizik vychází z:

- charakteru a druhu následků, které se mohou vyskytnout včetně jejich měření,
- způsobu stanovení pravděpodobnosti výskytu rizika,
- časového rámce následků a pravděpodobnosti výskytu rizika,
- způsobu určení úrovně rizika,



- úroveň, pod níž je riziko přijatelné nebo tolerovatelné,
- úroveň rizika, od níž je třeba zajistit cílenou odezvu,
- možnosti kombinace více rizik.

Analýza rizika znamená kritické studium kauzálního vztahu příčiny – dopady. Hodnocení rizik znamená porovnání úrovní rizik získaných analýzou rizik s kritérii pro posuzování rizik. Hodnocení rizika z pohledu prevence, připravenosti, odezvy a obnovy musí obsahovat:

- identifikaci ohrožení; specifikaci jevů (nebo scénářů), které ohrožují; specifikaci četnosti výskytu jevů (nebo scénářů), které ohrožují; odhad důsledků jevů (nebo scénářů), které ohrožují (ve kterých je zahrnuto i působení místní zranitelnosti); odhad rizika z kombinace důsledků jevů (nebo scénářů), které ohrožují a četností výskytu; ocenění kroků pro odhad rizika a provedení odhadu rizika; ocenění výsledků odhadu rizika pro potřeby rozhodnutí,
- standardy a normy pro regulaci projektování a provozování lidských činností; postupy a systémy řízení bezpečnosti; a popř. další,
- jakým způsobem jsou cíle řízení rizika nastaveny, zda: cíle o úrovni rizika jsou kvalitativní nebo kvantitativní; splňují technické standardy; standardy řízení jsou systémové; a další.

Zvládání rizik dle podkladů uvedených v [5] znamená v případě, že riziko není přijatelné, provést:

- vyhnutí se riziku (tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika), když to jde – u přírodních pohrom to nejde,
- odstranění zdrojů rizik, tj. zabránění vzniku pohrom, když to jde – u přírodních pohrom to nejde,
- snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom (např. snížením množství nebezpečných chemických látek v podnicích), když to jde – u přírodních pohrom to nejde,
- snížení závažnosti dopadů rizika, tj. příprava zmírňujících opatření jako jsou varovací systémy, systémy odezvy a obnovy,
- sdílení rizika, tj. rozdělení rizika mezi zúčastněné a pojišťovny,
- retenci rizika.

Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika.

Pro posuzování účinnosti řízení rizika se používá index, který hodnotí výkonnost řízení rizika – RMI (Risk Management Index). Jedná se o kvalitativní míru, která je založená na cílech, které si řízení rizik vytyčilo. Někdy se též používají indikátory, u kterých se požaduje, aby byly transparentní, robustní, reprezentativní a snadno pochopitelné pro uživatele (veřejnost, politici, veřejná správa apod.).

Řízení rizik je třeba aplikovat na celé technické dílo, celou organizaci, která technické dílo spravuje, a to v mnoha oblastech a na mnohých úrovních, v kteroukoli dobu a také při řízení projektů a činností.

## **6. Validita zvládnutí rizika při použití norem a standardů**

Další používané normy spojené s rizikem v technické praxi jsou: ČSN IEC 300-3-9; ČSN OHSAS 18001; ČSN EN ISO 12100; ČSN EN ISO 12100-1; ČSN EN ISO 14121-1; ČSN EN 1050:2001; ČSN EN ISO 12100-1; ČSN EN ISO 12100-2; ČSN EN ISO 9000 atd.

Normy a standardy ukládají požadavky, které jsou oprávněné. Nestanovují však často způsob, jak požadavky splnit, tj. jaká data a jaké metody použít.

Při aplikaci norem a standardů si musíme uvědomit, co standardy pokrývají. V daném směru jsou obvykle založené na zásadách teorie pravděpodobnosti. Proto si musíme uvědomovat, že v žádném případě nepokrývají všechny možné varianty. Při použití normálního rozdělení platí, že interval (medián- $\sigma$ , medián+ $\sigma$ ) pokrývá 68.5 % případů; interval (medián- $2\sigma$ , medián+ $2\sigma$ ) pokrývá 95.4 % případů; interval (medián- $3\sigma$ , medián+ $3\sigma$ ) pokrývá 99.8 % případů. To znamená, že neplatí





pro celý rozsah možných podmínek. Proto u důležitých technických děl je nutno provádět všechna hodnocení spojená s riziky a bezpečností jako místně specifická, tj. vycházet z logických základů metod a systémového pojetí entity; aplikace různých kódů a software, které nejsou místně specifické, mohou za kritických podmínek vést k selhání technických děl [2,7].

V praxi při práci s riziky spojenými s technickými díly se stále používají jen tradiční metody, jako jsou Kontrolní seznam, HAZOP, FMEA, FMECA, QRA apod. [8], protože pro ně existují software. Předmětné metody při práci s riziky nerespektují systémový charakter technického díla při dopadech vnějších pohrom, úmyslných vnějších aktů (např. korupce na správních úřadech s cílem oslabit konkurenceschopnost technického díla), teroristických činů apod. Podle šetření, které provedla US EPA [12], předmětné metody lze použít s ohledem na bezpečnost technických děl jen při řešení některých úloh, ve kterých nejde o integritu bezpečnosti technického díla, což odpovídá i údajům shromážděným v [7], které byly zmíněny v [2]. Všeobecně použitelné metody dle [7,12] jsou správně aplikované metody What, If [8] a místně specifické kontrolní seznamy, které jsou sestavené experty. Podle diskusí na odborných setkáních [1] a nakonec i ve sdělovacích prostředcích v poslední době je otázka, kdo je expert. Podle nároků na experty, jež jsou shrnuté v práci [1] se expertem míní osoba, která je uznávána odbornou komunitou, má experimentální zkušenosti v dané oblasti, určitý počet kvalitních odborných publikací, zná podstatu nejistot různých konceptů, rozmanitost podmínek, způsoby kompenzace škod a má zájem o řešení předmětného problému. Mnoho příkladů z praxe však ukazuje, že řada expertů je postižena provozní slepotou, je uchlácholena splněním požadavků norem a standardů a nevidí rizika spojená s různými vazbami a spřaženími s okolím [1,7].

Praxe také ukázala, že u složitých technických děl nestačí jeden expert, ale je třeba kombinovat znalosti několika expertů. Velký důraz je kladen na kvalifikovanost expertů (průkaz znalostí, zkušeností, objektivitu a schopnosti hledat konsensus). Kombinaci návrhů lze dle povahy rozhodovaného problému zajistit pomocí analytických metod nebo heuristik, např. metody DELPHI, panelová diskuse [8]. Systematické zapojení expertů snižuje potřebu improvizace při zvládání kritických situací.

Rozvoj technologií směřuje stále více ke kombinaci jednotlivých zařízení a aplikací do komplexních (složitých) systémů s cílem dosáhnout zvýšení výroby a vysoké ziskovosti. Vytvářené systémy nejsou výsledkem expertů z jedné disciplíny (oboru), nýbrž jsou výsledkem interdisciplinárního týmu. Zvláště pro síťové technologie platí, že jednotlivý expert není schopen kompletně posoudit a ovládat velké technické systémy, a proto je nutná spolupráce expertů z řady disciplín, která vyžaduje vzájemné pochopení cílů a schopnost hledání konsensu. Dodnes je skutečností, že při sestavování technických děl a při vytváření jejich bezpečnosti experti z různých oborů pracují odděleně, což nezaručuje ani optimální bezpečnost, ani optimální náklady. Často se stává, že jednotlivé dílčí systémy jsou bezpečné, protože pro ně existují standardy a normy (např. jednotlivé technické části určitého provozu), ale bezpečnost celku, který vznikl jejich propojením s kybernetickými a jinými infrastrukturami již sledovaná není, protože se hodnocení a prokázání bezpečnosti nepožaduje relevantní legislativou a navíc k danému účelu není dosud k dispozici relevantní odborný postup. Právě uvedená skutečnost znamená slabinu pro bezpečnost technických děl. Dosavadní řešení jsou prováděna na základě dobré inženýrské praxe a jejich dlouhodobá bezpečnost a spolehlivost se těžko prokazuje.

## **7. Závěr**

Přehled oblastí, které ovlivňují výběr jednotlivých technik práce s riziky, ukazuje, že tam, kde jde o zajištění bezpečných technických děl, tam je třeba používat techniky pro práci s riziky, které jsou založené na systémovém pojetí a kritickém hodnocení všech vlivů, které jsou možné dnes i v budoucnosti. Posouzení validity metod a procedur práce s riziky, které jsou používány v praxi, ukazuje, že dosud v české praxi převládají techniky, které nerespektují systémovou povahu technických děl a dynamiku vývoje.



## ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů*. ISBN: 978-80-01-05771-1. Praha: ČVUT 2015, 208p.
- [2] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. e-ISBN: 78-80-01-06182-4. Praha: ČVUT 2017, 364p. <http://hdl.handle.net/10467/72582>
- [3] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN: 978-80-01-05245-7. Praha: ČVUT 2013, 223p.
- [4] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN: 978-80-01-04844-3. Praha: ČVUT 2011, 483p.
- [5] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. ISBN: 978-80-01-04841-2. Praha: ČVUT, Praha, 2011, 405p.
- [6] PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládní*. ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234p.
- [7] PROCHÁZKOVÁ, D. *Archiv řešených úloh z oblasti řízení bezpečnosti a krizového řízení*. Praha: ČVUT, fakulta dopravní, ústav bezpečnostní technologií a inženýrství.
- [8] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369p.
- [9] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Data a metodika jejich zpracování pro potřeby inženýrských disciplín*. ISBN: 978-80-01-05792-6. Praha: ČVUT 2015, 186p.
- [10] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991.
- [11] COASE, R. H. The Problem of Social Costs. *Journal of Law and Economics*, Vol. 3, The University of Chicago Press 1960, pp. 1-44.
- [12] US EPA. PHA Techniques in Chemical Emergency Prevention & Planning. *Newsletter* 2008, No. 8, pp. 3-6.

## ADRESA AUTORA

**Doc. RNDr. Dana Procházková, PhD., DrSc.**

ČVUT v Praze, Fakulta strojní, katedra energetiky, Praha, Česká republika

e-mail: prochdana7@seznam.cz



### **RECENZIA TEXTOV V ZBORNÍKU**

Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

### **REVIEW TEXT IN THE CONFERENCE PROCEEDINGS**

Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.