Motivation - Education - Trust - Environment - Safety 2020
METES
Recenzovaný zborník z V. medzinárodnej vedeckej konferencie, 21.II.2020, Ružomberok
Proceedings of the 5th International Conference, Ružomberok, February 21,2020
Bratislava: SSŽP et Strix. Edition ESE-54, ISBN 978-80-973460-7-2

# PŘIŘAZENÍ OPTIMÁLNÍCH NÁSTROJŮ INŽENÝRSKÝCH DISCIPLÍN PRACUJÍCÍCH S RIZIKEM K DOSAŽENÍ HLAVNÍCH CÍLŮ ŘÍZENÍ TECHNICKÝCH DĚL

**Dana PROCHÁZKOVÁ**

# AFFILIATION OF OPTIMUM RISK ENGINEERING TOOLS TO TECHNICAL FACILITY MANAGEMENT MAIN TARGETS ACHIEVEMENT

METES
Motivation - Education - Trust - Environment - Safety 2020

***ABSTRAKT***
*STUDIE HAVÁRIÍ A SELHÁNÍ SLOŽITÝCH TECHNICKÝCH DĚL UKÁZALA, ŽE V MNOHA PŘÍPADECH SE PŘEDMĚTNÉ JEVY VYSKYTUJÍ, KDYŽ INTEGRÁLNÍ RIZIKO TECHNICKÉHO DÍLA PŘEKROČÍ JISTOU MÍRU KRITIČNOSTI, TJ. TAKÉ TEHDY, KDYŽ V TECHNICKÉM DÍLE DOJDE V KRÁTKÉM OBDOBÍ K REALIZACI VĚTŠÍHO POČTU ZDROJŮ MALÝCH RIZIK A JEJICH DOPADY JSOU VZÁJEMNĚ PROPOJENY. SOUČASNÉ NÁSTROJE INŽENÝRSKÝCH DISCIPLÍN PRACUJÍCÍCH S RIZIKY JSOU ROZMANITÉ A MAJÍ RŮZNÉ POŽADAVKY NA DATA, ZNALOSTI, DOBU ZPRACOVÁNÍ, TJ. I NA FINANCE, A PRAXE SE SAMOZŘEJMĚ ZAJÍMÁ O NEJMÉNĚ NÁROČNÉ NÁSTROJE. ČLÁNEK UKAZUJE OPTIMÁLNÍ NÁSTROJE INŽENÝRSKÝCH DISCIPLÍN PRACUJÍCÍCH S RIZIKY PRO DOSAŽENÍ HLAVNÍCH TŘÍ CÍLŮ TECHNICKÉHO DÍLA (SPOLEHLIVOST, ZABEZPEČENÍ, BEZPEČNOST), KTERÉ ZÁVISÍ NA MÍŘE SLOŽITOSTI TECHNICKÝCH DĚL.*

***KLÍČOVÁ SLOVA:*** *technické dílo; složitost; riziko; nástroje inženýrských disciplín pracujících s riziky; bezpečnost; zabezpečení; spolehlivost; řízení rizik.*

***ABSTRAKT***
*THE STUDY OF ACCIDENTS AND FAILURES OF COMPLEX TECHNICAL FACILITIES HAS SHOWN THAT IN MANY CASES, THESE PHENOMENA OCCUR WHEN THE TECHNICAL FACILITY INTEGRAL RISK EXCEEDS THE CERTAIN CRITICALITY RATE, I.E. ALSO IF LARGER NUMBER OF SMALL RISK SOURCES EXECUTES IN TECHNICAL FACILITY IN A SHORT PERIOD OF TIME AND THEIR IMPACTS ARE SPECIALLY INTERCONNECTED. THE PRESENT RISK ENGINEERING TOOLS ARE DIVERSE AND HAVE DIFFERENT REQUIREMENTS FOR DATA, KNOWLEDGE, PROCESSING TIME, I.E. FINANCE, AND PRACTICE IS OF COURSE INTERESTED IN THE LEAST DEMANDING TOOLS. THE ARTICLE SHOWS OPTIMUM RISK ENGINEERING TOOLS WORKING WITH RISKS FOR ACHIEVEMENT OF MAIN THREE TARGETS OF TECHNICAL FACILITY (RELIABILITY; SECURITY; SAFETY), WHICH DEPEND ON THE TECHNICAL FACILITIES´ COMPLEXITY RATE.*

***KEY WORDS:*** *Technical facility; complexity; risk; risk engineering tools; safety; security; reliability; risk management.*

## 1. Úvod

Každý technický produkt nebo každé technické dílo (dále jen technické dílo) je výsledkem lidské činnosti s cílem zajistit produkty a služby podporující lidské životy a vývoj. Pro zajištění bezpečnosti technického díla je nutné pracovat s riziky všeho druhu [1]. Koexistence technického díla

s okolím (tj. s veřejnými aktivy, které zahrnují lidské životy, zdraví a bezpečí, majetek, veřejné blaho, životní prostředí, další technická díla), je zajištěna, pokud je úspěšně zvládnuta integrální (tj. celková) bezpečnost technického díla [2,3]. Úroveň integrální bezpečnosti závisí na kvalitě práce s integrálním rizikem [2,4]. Pro úspěšnou práci s riziky všech typů jsou nezbytné jak správné, efektivní nástroje, tak odpovědnost za jejich správné použití [1-5]. Článek pojednává o první položce; druhá byla řešena v [2,6].

Byla vyvinuta řada specifických nástrojů pro řešení rizik v oblasti inženýrských disciplín pracujících s riziky [2,4,7-9]. Protože v praxi jde o odlišné cíle inženýrských disciplín pracujících s riziky (bezpečnost stroje, bezpečnost procesu, bezpečnost celého díla atd. [3,9]) a používané nástroje mají v praxi odlišné požadavky na znalosti, data, čas a finance, je nutné ve skutečnosti použít takový nástroj, který splňuje daný cíl a je proveditelný. Skutečná praxe vyžaduje nástroje, které mají nejnižší nároky [10]. Dále jsou specifikovány takové nástroje pro vybrané úkoly, které jsou v praxi řešeny.

## 2. Shrnutí poznatků

Koexistence technického díla s okolím během celého životního cyklu technického díla je zajištěna, pokud je integrální bezpečnost technického díla udržována na určité úrovni kvalifikovaným řízením rizik [1]. Integrální bezpečností se rozumí vlastnost na úrovni celého technického díla a je určována kvalitou souboru antropogenních opatření a činností zaměřených na bezpečné technické dílo, a to i při jeho kritických podmínkách [4].

Hlavním současným cílem je rozpoznat, pochopit a řídit rizika, a tím zajistit bezpečné technické dílo a jeho bezpečný provoz po celou dobu jeho životnosti. Protože technická díla jsou charakterizována otevřenými systémy systémů (SoS), jde o výběr nástrojů, v nichž jsou výsledky analytických a expertních metod specificky propojeny [4,5,7].

Architektura technického díla je objektová nebo síťová [1,2]. Každý typ technického díla má svá specifika; např. proto existuje významný rozdíl mezi řízením stabilních a mobilníchtechnických děl. V současné době v praxi se nepoužívají jednoduché technické systémy, ale jsou používány soubory systémů. Podle typu organizace souborů systémů [1,2] se rozlišují:

- jednoduše uspořádané celky (např. stroje),
- složené systémy, které jsou chápány jako soubor elementů, které jsou uspořádány a spojeny určitým způsobem a vzhledem ke své náležité struktuře plní určité funkce, jsou charakterizovány vyšší úrovní uspořádání (např. složený soubor strojů – výrobní linka, která provádí v daném pořadí úkony tak, aby vytvořila určitý výrobek),
- komplexní systémy charakterizované organizovanou složitostí a složením, které jsou uspořádané tak, aby vykonávaly určité funkce (propojené výrobní linky s různými technologiemi, např. automatické systémy pro výrobu – např. tzv. digitální továrny, kategorizace a distribuce určitých komodit),
- velmi komplexní systémy reprezentující vzájemně propojené komplexní systémy v horizontální i vertikální struktuře vyznačující se velkou proměnností, která připomíná neorganizovanou složitost, tj. systémy systémů. Jednotlivé komplexní systémy mohou pracovat jak samostatně, tak společně. Při společné práci pak vykonávají zcela unikátní úkol, který je vzdálený od úkolů jednotlivých komplexních systémů (systémy pro výrobu, distribuci a spotřebu elektřiny, plynu atd.).

Na základě znalostí a zkušeností [1,2] pro charakteristiku a řízení:

- jednoduše organizovaných celků, jsou použity výsledky analytických řešení,
- složených systémů, se využívají výsledky statistických řešení, které jsou založeny na analytických funkcích, jejichž parametry jsou v určitých intervalech variabilní, což odráží náhodnost podmínek (náhodné chování systémů),
- složitých systémů, je třeba použít výsledky simulací, protože náhodné nejistoty jsou velké a způsobují, že chování scénářů je v širším rozsahu, než který zahrnuje náhodnost, tj. používají se metody operačního výzkumu [7].

- velmi složitých systémů, je třeba použít se multikriteriální metody, protože dané agregáty mají mnoho systémů, které jsou uspořádány do několika úrovní. Systémy spolu vzájemně interagují v závislosti na vnitřních a vnějších podmínkách, což způsobuje, že pozorujeme:
    - náhlé změny chování, které nelze získat z vědomostí o chování komponent, jde o náhlý vznik jevů, které nebyly očekávány,
    - různé hierarchie,
    - samo-organizovanost,
    - rozmanité struktury řízení, které se společně jeví jako chaos.

Předmětné systémy mají náhodné i znalostní nejistoty, a proto je třeba pro jejich charakteristiku používat expertní a heuristické metody [7]; někdy je nutné zvážit mnoho kritérií, z nichž některá jsou i protichůdná (konfliktní) [4,5].

Pro popis typu organizace technického díla zavádíme veličinu nazývanou „složitost“. Podle [4], složitost je vlastnost systému, která označuje, že systém má mnoho částí nebo prvků, které mají vzájemné vztahy odlišné od vztahů s jinými prvky venku a jejich chování závisí na mnoha vnitřních a vnějších parametrech. Charakterizuje chování systému, jehož části interagují různě v závislosti na momentálních podmínkách v daném místě a v daném čase [1]. Pro jeho popis je nutné zaujmout přístup založený na mnoha oborovém a mezioborovém přístupu a pro jeho řízení je tedy nutné použít přístupy založené na více kritériích, které umožňují zohlednit průřezová rizika [5]. Byla pro ně vyvinuta řada konkrétních nástrojů pro řešení rizik v oblasti inženýrských disciplín pracujících s riziky, a proto vzniká problém, který z přístupů je ten správný v daných podmínkách.

Podle současných znalostí se v praxi používají tři různé cíle řízení technických děl, konkrétně: spolehlivost; zabezpečení; a bezpečnost. Protože předmětné cíle vycházejí z různých konceptů, hodnoty rizik technických děl získané pro jednotlivé cíle nejsou stejné; jsou silně závislé na konceptu [2,5]. S ohledem na výše uvedené znalosti, míra integrálního rizika závisí na obou, na cíli řízení rizik a na míře složitosti technického díla [2-5].

Nástroje inženýrských disciplín pracujících s riziky jsou rozmanité a mají různé požadavky na data, znalosti, dobu zpracování, tj. i na finance, a praxe se samozřejmě zajímá o nejméně náročné nástroje [1-5]. Podle výsledků shrnutých v [3,8] jsou užitečnými metodami v praxi pro složitá technická díla:

- Benchmarking je metoda systematického porovnávání procesů, organizační struktury, produktů a výkonu dané části technického díla s jinými celosvětově úspěšnými technickými díly za účelem dosažení excelence. Obvykle se používá při řízení rizik v případech, kdy je cíl ideální, a podle zásad správné praxe je dobré řídit rizika způsobem, jakým to dělají nejlepší průmysloví provozovatelé.
- Modelování je technika, pomocí které vytváříme zjednodušený obrázek skutečného procesu, systému nebo objektu a poté sledujeme navázaná spojení. Jeho cílem je určit scénář procesu v čase a prostoru (např. průběh havárie, průběh řízení procesu, průběh reakce na havárii atd.), abychom mohli stanovit vhodná opatření a činnosti, která zajistí bezpečná technická díla (např. při prevenci, zmírnění a zvládnutí nehod, havárií a selhání) s dostupnými schopnostmi a možnostmi, což provádíme pomocí CBA (analýza nákladů a přínosů). Na základě zásady, že „vše souvisí se vším“ (regresus ad infinitum), je nutné ověřit výsledky získané podle modelu, protože vyhodnocení nehod a selhání technických děl často ukazuje, že klíčové příčiny havárií byly při modelování havárií nedostatečně zváženy. Ve vážných případech je třeba věnovat pozornost softwarovým aplikacím, zejména pokud nebyly ověřeny podmínky přenosu technologií [11].
- Scénář je systémový model, který popisuje vývoj procesu v jeho různých podobách (varianty, alternativy) v závislosti na podmínkách nebo rozhodnutích. Obsahuje sled událostí, které se v něm odehrávají v čase, území, či jiné entitě (včetně potenciálních variant), a popisuje interakce mezi sledovanými aktivy systému a procesem[7].Scénáře pohrom jsou pro řízení bezpečnosti

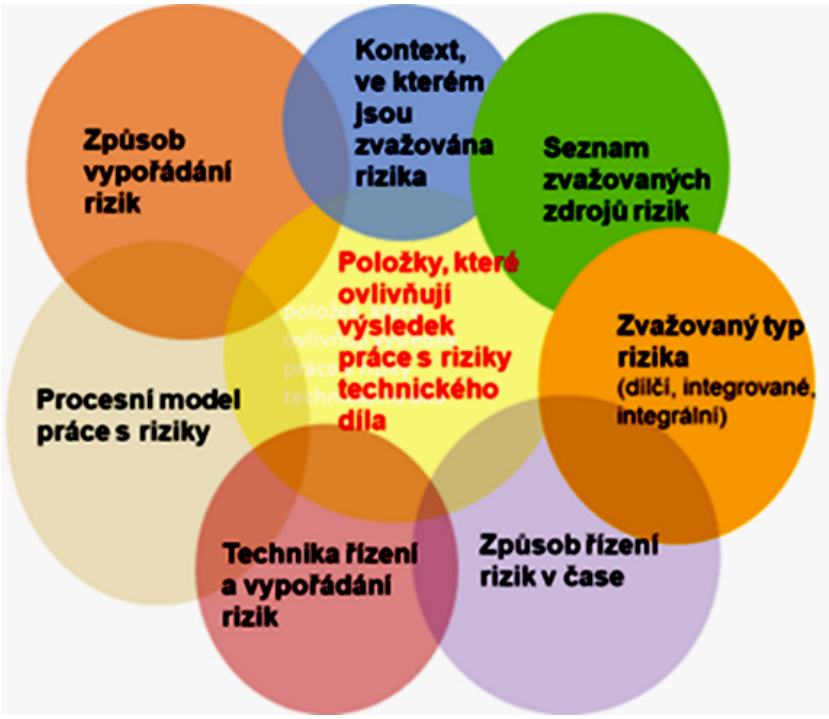
nejdůležitější, protože se používají k navrhování opatření prevence, zmírňování, reakce a obnovy.

- Multikriteriální hodnocení je hodnocení založené na uplatňování více kritérií, a to i nesouměřitelných nebo konfliktních, na celek [7]. Pro výsledné řešení musí být stanoveny restriktivní podmínky, které definují objektivitu (např. z hlediska vyčerpatelnosti systému, lidských zdrojů nebo hodnoty výhod). Vyčerpatelnost systému znamená maximální možnou úroveň užitečnosti (užitku, užitné hodnoty), kterou lze dosáhnout na dané úrovni vědeckotechnického rozvoje. Omezující podmínky vždy posuzujeme individuálně, a to na základě jejich dílčích hodnocení. Pro použití maximálního užitku ve spojení s riziky složitých systémů se osvědčilo použití: metody What, If ve formě tabulky, tabulka 1; a DSS (Decision Support System) s příslušnými hodnotovými stupnicemi zpracovanými podle teorie maximálního užitku [12].

*Tabulka 1. Standardní model pro použití metody What, If.*

| **Aktivum** | | **Potenciální dopad na aktivum** |
|---|---|---|
| Životy a zdraví lidí | | |
| Bezpečí lidí | | |
| Majetek | | |
| Veřejné blaho | | |
| Veřejné blaho | | |
| Infrastruktury a technologie | Energetika | |
| | Dodávky vody | |
| | Kanalizace | |
| | Doprava | |
| | Komunikace a informace | |
| | Bankovní a finanční sektor | |
| | Nouzové služby | |
| | Základní územní služby (průmysl, zemědělství, dodavatelské služby, zdravotní služby, nakládání s odpady, sociální služby, pohřební služby) | |
| | Veřejná správa | |
| Technické dílo | Kritická zařízení | |
| | Kritické komponenty | |
| | Kritické linky (provozy) | |
| | Kritické vnitřní infrastruktury | |
| | Kritické toky | |
| | Kritické zásoby | |
| | Kritický personál | |
| | Nakládání s odpady | |
| | Položky řízení kritických procesů | |
| | Položky řízení kritických projektů | |
| | Kritické položky řízení technického díla | |
| …….. | | |

Analýzy nástrojů řízení rizik uvedené v [9,13] a nashromážděné zkušenosti [10] ukazují, že nástroje řízení rizik závisí na mnoha faktorech; schematicky je záležitost znázorněna na obrázku 1.




*Obr. 1. Faktory, které ovlivňují velikost rizika daného subjektu.*

Je zřejmé, že strategické řízení technického díla, pokud jde o bezpečnost a dlouhodobou funkčnost, musí vzít v úvahu dva faktory:

- technická díla jsou složité víceúrovňové systémy,
- specifické zdroje rizika spojené s technickými díly nejsou na všech úrovních technického díla stejné.

Vzhledem ke složitosti technického díla je v praxi nutné pracovat s riziky na nejnižší úrovni (jednoduchá technickázařízení - stroje), stejně jako s riziky na vyšších úrovních (komponenty - např. tlaková zařízení, výrobní linky, sady výrobních linek, celé technické dílo) a na nejvyšší úrovni (technické dílo a jeho okolí). Bezpečnost na nejvyšší úrovni zajišťuje koexistenci technického díla s okolím po celou dobu jeho životnosti.

S cílem zajistit bezpečnost a rozvoj lidí a dalších veřejných aktiv jsou cíle řešení rizik na všech úrovních technického díla stejné, spolehlivý nebo zabezpečený, anebo bezpečný subjekt. Vzhledem k současným cílům lidské společnosti, které byly již několikrát zdůrazněny, se především zaměřujeme na konečný cíl, kterým jsou bezpečné entity.

## 3. Rizika používaná v praxi

V praxi se používají tři typy rizik: dílčí (vztahující se k jednomu aktivu); integrované (součet rizik souvisejících s několika aktivy); a integrální [4,5]. Integrální riziko je systémové riziko, které závisí na momentálních podmínkách v daném místě a daném čase. Proto je jeho stanovení velmi obtížné pro složitá technická díla, kde existuje velká variabilita vazeb a toků. V těchto případech je jeho analytické vyjádření obtížné z důvodu existence mnoha náhodných a epistemických nejistot [4,5]. Proto je třeba použít specifické technické nástroje jako specifickou metodu What, If (tabulka 1) pro

každý možný scénář a systém pro podporu rozhodování [4,5,7], jejichž kombinace má schopnost identifikovat velikost integrálního rizika předem.

Při výběru nástrojů řízení rizik pro technické zařízení a celá technická díla zaměřená na bezpečnost jsou podle argumentů v [1,2,5] důležité dva faktory:

- Prvním faktorem je poznání, že riziko je veličina místně a časově specifická, tj. závisí, jak na příčině škodlivého jevu (tj. povaze a velikosti škodlivého jevu), tak na charakteristikách subjektu (zranitelnost, houževnatost) v době vzniku jevu (např. neudržovaný pojistný ventil normálně nevykonává svou funkci při překročení limitu tlaku). Protože v průběhu času jsou proměnné, jak aktivum, nebo skupina aktiv, tak velikost škodlivých jevů nebo pohrom, existují tři kategorie situací, pokud jde o zvládání dopadů realizovaného rizika, a to: normální; nouzová; a kritická. S rostoucí kategorií rostou profesní, finanční, organizační a personální požadavky na řízení a řešení rizik spojených s těmito situacemi. Proto zde hraje důležitou roli legislativa, která ukládá vlastníkům a provozovatelům technických děl požadavky na řízení rizik a požadavky veřejné správě na dohled nad bezpečností technických děl ve veřejném zájmu [1,2,5]. Na základě analýz právních předpisů [1,2,5,10] je současná legislativa příliš obecná; nezmiňuje požadavky na data a metody zpracování dat, které zásadně určují kvalitu výsledku.
- Druhým faktorem je výběr typu rizika, který má být sledován v úkolu, který má být proveden, což závisí na stanovení:
    - počtu aktiv a jejich seznamu, tj. dále se zvažuje, která veřejná aktiva a která konkrétní aktiva technického díla v daném úkolu jsou důležitá; např. zda jde o výkon, konkurenceschopnost, zisk atd.,
    - zda vazby a toky mezi uvedenými aktivy hrají roli v úkolu, tj. mechanický koncept nestačí, ale je třeba zvážit systémový koncept.

Aby byla zajištěna bezpečnost entity v krátkodobém horizontu (např. bezpečný stav jednoduchého technického zařízení), stačí monitorovat stav aktiva, tj. dílčí riziko spojené s entitou. S ohledem na bezpečnost člověka vyžaduje legislativa ve vyspělých zemích také zajištění bezpečnosti a ochrany zdraví při práci (BOZP), tj. sledování dvou aktiv (život a zdraví osob na pracovišti, kvalita pracovního prostředí); při použití integrovaného rizika je zanedbávána vazba stroj –člověk, která ovlivňuje stav stroje.Poněvadž technická zařízení, lidé na pracovišti a pracovní prostředí jsou vzájemně propojené, je třeba ve střednědobém a dlouhodobém horizontu monitorovat propojení a toky mezi těmito subsystémy, tj. sledovat integrální riziko, aby byla zajištěna bezpečnost celku.

Proto při výběru nástrojů řízení rizik (identifikace, analýza, hodnocení, posouzení, řízení a vypořádání) zaměřených na bezpečnost vybraného subjektu by měly být v technické oblasti pro technická díla rozlišeny následující úkoly:

- výběr nástrojů pro práci s rizikem spojeným se stavem technického zařízení (cíl - bezpečné technické zařízení),
- výběr nástrojů pro práci s rizikem spojeným se stavem technické komponenty (cíl - bezpečná technická komponenta),
- výběr nástrojů pro práci s rizikem spojeným s výrobní linkou / výrobním procesem (cíl - bezpečný výrobní proces),
- výběr nástrojů pro práci s rizikem spojeným se stavem sady výrobních procesů (cíl – bezpečná sada výrobních procesů),
- výběr nástrojů pro práci s rizikem spojeným s celým technickým dílem (cíl - bezpečné technické dílo),
- výběr nástrojů pro práci s rizikem spojeným s technickým dílem a jeho okolím (cíl - bezpečné technické dílo a bezpečné okolí technického díla).

Na základě prací [1,2,5,7] při zaměření na technická díla nestačí zajistit bezpečnost lidského systému ve spojení s technickými díly a technologiemi (tj. koexistence technického díla s okolím během provozu ) jen orientací na bezpečnost technických děl, protože výběr nástrojů pro řízení rizik závisí na:

- povaze subjektu zájmu (tj. vybrané technické zařízení nebo vyšší systémy technického díla),
- povaze prostředí, ve kterém subjekt zájmu (tj. vybrané technické zařízení nebo vyšší systémy technického díla) pracuje,
- režimu, ve kterém subjekt zájmu (tj. vybrané technické zařízení nebo vyšší systém technického díla) pracuje,
- požadavcích na provoz subjektu zájmu (tj. vybrané technické zařízení nebo vyšší systémy technického díla),
- a zda je zapotřebí krátkodobé, střední nebo strategické, tj. dlouhodobé, řešení.

## 4. Použitá data

Pro řešení úkolu byla sestavena původní databáze havárií a selhání technických děl [10] ze světových dat a bylo podrobně analyzováno několik případových studií. Databáze obsahuje 7829 škodlivých jevů z celého světa, které byly pro autory přístupné za posledních 35 let; více než 90% škodlivých jevů vzniklo během provozu technických děl. Pro odhalení jejich příčin (realizovaných rizik) byla shromážděná data zpracována metodami inženýrských disciplín pracujících s riziky: What, If; Kontrolní seznam; Diagram rybí kosti; Případová studie; Strom událostí; FMECA; atd.[7]v závislosti na kvalitě a množství dostupných dat [10]. Byly také zváženy dostupné výsledky jiných autorů [14-19].

Studie nehod a selhání složitých technických děl [3,10,20] ukázala, že původci nehod a selhání technických děl s výjimkou velkých přírodních pohrom jsou:

- velké chyby v předcházení rizikům v technických dílech, pokud jde o zadávací podmínky, projektování a provoz,
- kumulace malých nepříznivých jevů, jejichž realizace v krátkém časovém intervalu je zničující.

Druhý případ je častější. Vyskytuje se, když integrální riziko překročí míru kritičnosti. V mnoha případech v technických dílech s velkou složitostí je překročení kritičnosti způsobeno kombinací většího počtu malých zdrojů rizika, které se vyskytnou v technickém díle v krátkém časovém období. Pro řízení chování technického díla v těchto případech je třeba používat integrální riziko [1,2].

## 5. Metoda pro ocenění účinnosti nástrojů

Inženýrské disciplíny pracující s riziky z povahy věci používají nástroje, které jsou založené na čtyřech modelech [2,7] podle typu problémů, které sledují; jde o:

- problémy, které lze popsat lineárním modelem [7] (jednoduše organizované struktury) - míra složitosti 1; např.: Kontrolní seznam; Bezpečnostní audit; Analýza lidské spolehlivosti - HRA; zde si je třeba uvědomit omezenou přesnost výsledků, protože se sleduje pouze jeden proces a zanedbávají se propojení s jinými procesy a životním prostředím,
- problémy, které lze popsat pomocí stromových modelů [7] (složené systémy, které jsou chápány jako znázornění prvků, které jsou uspořádány a určitým způsobem spojeny) - míra složitosti 2; např.: Předběžná analýza rizik - PHA; Kvantitativní analýza rizik - QRA; Analýzy ohrožení a provozuschopnosti - HAZOP); Analýza stromu událostí - ETA; Analýza režimů selhání a dopadů - FMEA; Analýza režimů selhání, dopadů a kritičnosti - FMECA; Analýza stromu poruch - FTA; Pravděpodobnostní posouzení bezpečnosti - PSA; zde je třeba poznamenat, že vývoj nehod, havárií a selhání pochází z jednoho místa, tj. modely nepopisují případy, kdy k dopadům na technické dílo dochází z jedné příčiny na několika místech, tj. kombinace škodlivých jevů se nezohledňují,

- problémy, které lze popsat pomocí modelů operačního výzkumu [7] (komplexní systémy, které jsou chápány jako reprezentace prvků, které jsou organizovány a spojeny určitým způsobem a jejich chování probíhá v jistém rozmezí a může být vyjádřeno variantami statistické funkce) - míra složitosti 3; např.: metoda kritické cesty; PERT; GERT; Petriho sítě; pro poslední tři jsou nyní vypracovány„barevné stochastické modely“, které simulují velký počet možných scénářů, které odborníci vytvářejí a hodnotí na základě svých zkušeností a údajů uvedených ve zkušenostních databázích zkušeností, které jsou sestavovány v posledních letech ve vyspělých zemích,
- nestrukturované problémy, které nelze jednoduše popsat kvůli velké variabilitě možných konfigurací, které působí těžko předvídatelné režimy chování [7] - míra složitosti 4: specifická forma What, If; scénáře; případové studie; multikriteriální metody založené na systému pro podporu rozhodování (DSS). V těchto případech jsou zkušenosti základ; řada scénářů je vyvinuta ve spolupráci s odborníky a optimální řešení je hledáno pomocí teorie maximálního užitku [12].

Zkušenosti z celosvětové praxe [5,7,10,13] ukazují, že často používané stromové modely nejsou schopny posoudit velikost integrálního rizika technického díla, protože vycházejí z jednoho bodu technického díla. To znamená, že nevystihují dopady vnějších pohrom, vnějších teroristických útoků a lidského faktoru, které obvykle současně ovlivňují mnoho míst najednou, a nepočítají s propojeními s okolím.

Systém pro podporu rozhodování (DSS) [7] je specializovaná technika pro získávání dat pro rozhodování o složitých problémech. Pomáhá vyřešit problém podporou analytického stylu rozhodování proti heuristickému rozhodování. To znamená, že:

- organizuje informace pro rozhodovací situace,
- interaguje se subjektem rozhodování (rozhodující osobou) v různých fázích rozhodování,
- rozšiřuje informační horizont rozhodujícího orgánu,
- usnadňuje multikriteriální hodnocení, protože má vestavěné multikriteriální metody, aniž by uživatel věděl o jejich matematické struktuře.

Jeho cílem je zajistit, aby výsledek odpovídal optimálnímu řešení. Při jejich tvorbě a aplikaci se používají:

- znalosti a údaje od odborníků, kteří znají technické a další parametry, limity a podmínky technického díla a místní zranitelnosti,
- princip teorie maximálního užitku [12], tj. „čím větší, tím lepší“ nebo „čím větší, tím horší“.

Pro mnoho z výše uvedených metod je k dispozici software, která byla odvozena pro konkrétní technické dílo v konkrétním místě. Pro zajištění správných výsledků v tomto případě je nutné před použitím každého software ověřit, zda jsou splněny podmínky přenosu technologií, tj. zda jsou podmínky pro řešení a řešení stejné jako pro technické dílo a místo, pro které byl software odvozen [7].

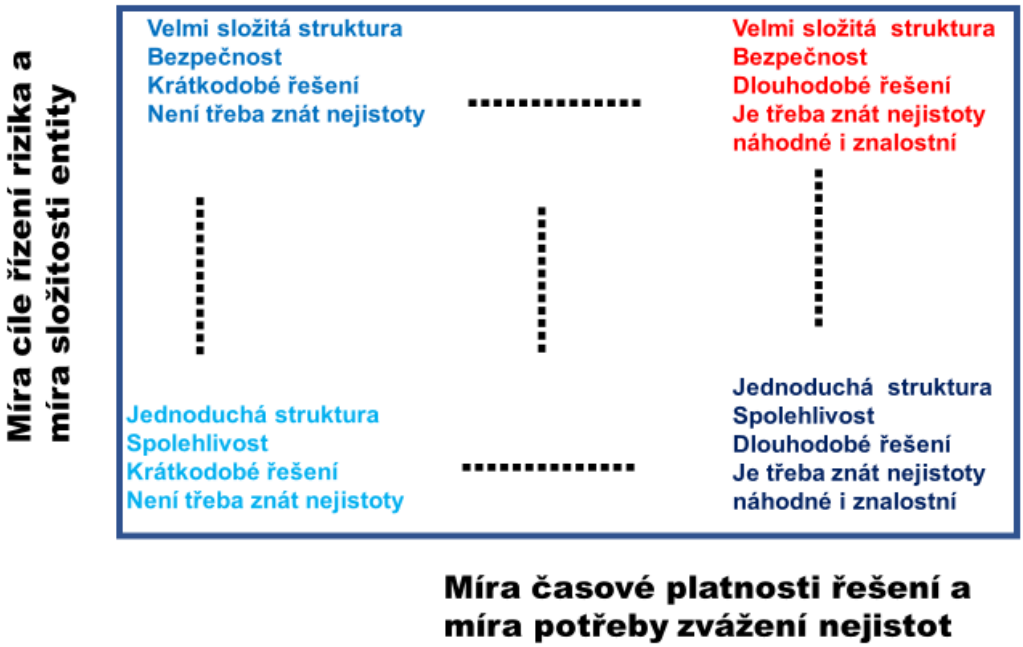
Vzhledem k tomu, že:

- jednotlivé nástroje inženýrských disciplín pracujících s riziky mají různé cíle a různé požadavky na znalosti, data, zkušenosti, čas, a tudíž i finance,
- v praxi jsou preferovány nástroje s nejmenšími nároky,
- stanovení integrálního (celkového) rizika technického díla je velmi závislé na jeho složitosti,

kritickým vyhodnocením schopnosti jednotlivých inženýrských nástrojů (uvedených výše) odhalit většinu závad, které vedly k nehodám a poruchám (111 případů z [10] mohlo být použito z důvodu nároků sledovaných metod na data),jsme určili nejméně náročné nástroje závislé na složitosti technického díla a na cíli řízení rizik technického díla.

Na základě dlouholeté zkušenosti z praxe jsme prostanovení optimálních metod pro úlohy spojené s technickými díly, ve kterých je třeba zvažovat cíl řízení rizika, složitost technického díla, dobu platnosti řešení a existenci neurčitostí, použili u výše popsaných dat metodu skórování [7]. Její aplikací jsme získali 4 základní kategoriepodmínek pro ocenění účinnosti(schopnosti) metod dát přijatelné řešení za nejmenších nákladů (znalosti, čas, finance); obrázek 2:

- úloha je založená na jednoduché struktuře technického díla, je zaměřená na spolehlivost technického díla, vyžaduje krátkodobou platnost výsledku a nepotřebuje zvažovat ani náhodné, ani znalostní nejistoty,
- úlohaje založená na velmi složité struktuře technického díla, je zaměřená na integrální bezpečnost technického díla, vyžaduje krátkodobou platnost výsledku a nepotřebuje zvažovat ani náhodné, ani znalostní nejistoty,
- úloha je založená na jednoduché struktuře technického díla, je zaměřená na spolehlivost technického díla, vyžaduje dlouhodobou platnost výsledku a potřebuje zvažovat náhodné i znalostní nejistoty,
- úloha je založená na složité struktuře technického díla, je zaměřená na integrální bezpečnost technického díla, vyžaduje dlouhodobou platnost výsledku a potřebuje zvažovat náhodné i znalostní nejistoty.




*Obr. 2. Skórování důležitých aspektů pro práci s riziky technických děl.*

Míra cíle řízení rizika a složitosti entity pro jednotlivé úlohy byla určena součtem následovně:

- cíl řízení rizika: spolehlivost – 1 bod; zabezpečení – 2 body; bezpečnost – 3 body,
- složitost struktury entity: bodová – 1 bod; lineární – 2 body, stromová – 3 body, plošná – 4 body, prostorová – 5 bodů.

Míra časové platnosti řešení a potřeby zvážení nejistot pro jednotlivé úlohybyla určena součtem následovně:

- potřeba zvážení nejistot: není třeba – 1bod; jen náhodných – 2 body; náhodných i znalostních - 2 body
- platnost řešení: krátkodobá – 1 bod; střednědobá – 2 body; dlouhodobá – 3 body.

## 6. Optimální metody pro řízení rizik závislé na míře složitosti a cíli řízení

Na základě výsledků výše popsaného způsobu hodnocení metod pomocí údajů o haváriích a selháních technických děl [2,7,10] a zkušeností autorů z praxe je sestavena tabulka 2. Obsahuje optimální nástroje inženýrských disciplín pracujících s riziky vhodné pro různé cíle technického díla a jeho částí, závislé na dvou proměnných.

Kromě složitosti entity jsou zvažovány tři cíle řízení rizik entity, a to uspořádané podle rostoucí náročnosti dosažení cíle [2,7,10]:

- spolehlivost entity zajišťující provozní bezpečnost entity,
- zabezpečení entity zajišťující procesní bezpečnost entity (provoz komponenty, výrobní linky),
- bezpečnost entity, tj. integrální bezpečnost, zajišťující bezpečnost jak entity, tak jejího okolí.

Protože čím vyšší je typ nástroje, tím vyšší jsou náklady (znalosti, finance, čas) na jeho použití, tabulka 2 ukazuje v každém případě pouze nástroje s nejnižšími náklady, které na základě současných znalostí a zkušeností mají schopnost vyřešit úkol, pokud jsou dodržována základní pravidla kultury bezpečnosti, provozní pravidla odpovídající provozním podmínkám; to znamená, že není uvažován žádný záměr poškodit entitu.

*Tabulka 2. Nástroje pro práci s riziky seřazené podle cíle sledovaného úkolu[*)].*

| **Cíl práce s riziky** | **Míra složitosti** | **Nástroj** | **Předmět sledování** |
|---|---|---|---|
| Spolehlivost jednotlivého technického zařízení (např. stroje) | 1 | Kontrolní seznam/bezpečnostní audit / What, If | Jedno aktivum |
| Zabezpečení jednotlivého technického zařízení (stroj je spolehlivý a je zajištěno jeho zabezpečení a bezpečí obsluhy) | 2 | Kontrolní seznam/ bezpečnostní audit /What, If | Dvě aktiva - protože může dojít ke konfliktům, je pro agregaci vyžadováno pravidlo |
| Bezpečnost jednotlivého technického zařízení (stroj neohrožuje sebe ani v kritických podmínkách a nemá škodlivé dopady na okolí), tj. je zajištěna bezpečnost jeho obsluhy a výrobky jsou bezpečné | 3 | DSS | Několik vzájemně propojených aktiv - protože mohou nastat konflikty, nejčastěji se používá teorie maximálního užitku [9] |
| Spolehlivost technické komponenty (několik vzájemně propojených technických zařízení) | 2 | Kontrolní seznam/ bezpečnostní audit /What, If / stromové modely | Několik vzájemně propojených technických a dalších aktiv - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, anebo použití teorie maximálního užitku [9] |
| Zabezpečení technické komponenty (několik vzájemně propojených technických zařízení je spolehlivé a je zajištěno jejich zabezpečení a bezpečí obsluhy) | 3 | Kontrolní seznam/ bezpečnostní audit /What, If / stromové modely / metody operačního výzkumu / DSS | Několik vzájemně propojených technických a dalších aktiv - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, anebo použití teorie maximálního užitku [9] |
| Bezpečnost technické komponenty (několik vzájemně propojených technických zařízení se neohrožuje ani v kritických podmínkách a nemá škodlivé dopady na okolí), tj. je zajištěna bezpečnost obsluhy a výrobky jsou bezpečné | 4 | Kontrolní seznam/ What, If / stromové modely / metody operačního výzkumu / DSS | Několik vzájemně propojených technických a dalších aktiv a okolí - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, anebo použití teorie maximálního užitku [9] |
| Spolehlivost výrobního procesu (výrobní linka) | 2 | Kontrolní seznam/ bezpečnostní audit /What, If / stromové modely | Několik vzájemně propojených technických a dalších aktiv - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, anebo použití teorie maximálního užitku [9] |
| Zabezpečení výrobního procesu (výrobní linka je spolehlivá a je zajištěno její zabezpečení a bezpečí | 3 | What, If / stromové modely / metody operačního výzkumu / DSS | Několik vzájemně propojených technických a dalších aktiv - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, |

| | | | |
|---|---|---|---|
| obsluhy) | | | anebo použití teorie maximálního užitku [9] |
| Bezpečnost výrobního procesu / výrobní linka se neohrožuje ani při kritických podmínkách a nemá škodlivé dopady na okolí), tj. je zajištěna bezpečnost obsluhy a výrobky jsou bezpečné | 4 | What, If / metody operačního výzkumu / DSS | Několik vzájemně propojených technických a dalších aktiv a okolí - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, anebo použití teorie maximálního užitku [9] |
| Spolehlivost souboru procesů v technickém díle | 3 | What, If / stochastické metody operačního výzkumu / DSS | Několik vzájemně propojených technických a dalších aktiv - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, anebo použití teorie maximálního užitku [9] |
| Zabezpečení sady procesů v technickém díle (sada procesů je spolehlivá a je zajištěno jejich zabezpečení a bezpečí obsluhy) | 4 | What, If / / metody operačního výzkumu / DSS | Několik vzájemně propojených technických a dalších aktiv a okolí - protože může dojít ke konfliktům, je pro agregaci nutné pravidlo, anebo použití teorie maximálního užitku [9] |
| Bezpečnost sady procesů v technickém díle (sada procesů ani při kritických neohrožuje sebe a své okolí); je bezpečná a její výrobky jsou bezpečné | 4 | DSS | Několik vzájemně propojených technických a dalších aktiv a okolí - protože může dojít ke konfliktům, je třeba použití teorie maximálního užitku [9] |
| Spolehlivost technického díla | 4 | DSS | Několik vzájemně propojených technických a dalších aktiv a okolí - protože může dojít ke konfliktům, je třeba použití teorie maximálního užitku [9] |
| Zabezpečení technického díla (technické dílo je zabezpečené a bezpečí obsluhy je zajištěné) | 4 | DSS | Několik vzájemně propojených technických a dalších aktiv a okolí - protože může dojít ke konfliktům, je třeba použití teorie maximálního užitku [9] |
| Bezpečnost technického díla (technické dílo ani při svých kritických podmínkách neohrožuje sebe a své okolí), tj. je bezpečné a jeho výrobky jsou bezpečné | 4 | DSS | Několik vzájemně propojených technických a dalších aktiv a okolí - protože může dojít ke konfliktům, je třeba použití teorie maximálního užitku [9] |

*) *V daném kontextu si je třeba uvědomit, že spolehlivost znamená správné provádění úkolů entity s pravděpodobností rovné nebo vyšší než 0,95; zabezpečení znamená spolehlivost a zajištění ochrany entity; a bezpečnost znamená zabezpečení (zahrnující spolehlivost) zajištění ochrany entity a jejího okolí.*

## 7. Závěr

Kritická analýza závislosti nástrojů na datech ukazuje, že čímvyšší typ nástroje pro řízení rizik je použit, tím vyšší jsou náklady (znalosti, finance, čas) na jeho použití. Kritickým vyhodnocením údajů o konkrétních haváriích a selháních technických děl s různou složitostí byly identifikovány nejnižší nákladově efektivní nástroje, které na základě současných znalostí a zkušeností by měly mít schopnost vyřešit úkoly splněním základních pravidel kultury bezpečnosti, provozních předpisů odpovídajících provozním podmínkám; tj. nezvažoval se úmysl poškodit technické dílo.

Na základě zkušeností je v provozní praxi technických děl a jejich částí pouze široce použitelný nástroj, který je rychlý a nenáročný na znalosti a čas. Proto byla posouzena věrohodnost nástrojů pro řízení rizik při provozu technických děl [5,13]. Výsledek tohoto výzkumu ukázal, že pro:

- nepříliš složitouentitu, jeosvědčeným nástrojem, kontrolní seznam specifický pro danou lokalitu se správně kalibrovanou stupnicí pro hodnocení rizik,
- nepříliš vzájemně propojené entity, je osvědčeným nástrojem, soubor kontrolních seznamů, které jsou specifické pro danou lokalitu a mají správně kalibrované škály rizik, a výsledky těchto kontrolních seznamů jsou agregovány specifikovaným a specifickým způsobem pro konkrétní lokalitu,
- složité objekty, je osvědčeným nástrojem DSS, který zohledňuje jak konektivitu, tak změny v čase a externí zdroje rizik.

Tabulka 2 ukazuje rozdělení nástrojů inženýrských disciplín pracujících s riziky pro optimální řešení praktických úkolů v závislosti na složitosti technických děl a cíli řízení jejich rizik.

## ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] PROCHAZKOVA, D. *Safety of Complex Technological Facilities.*ISBN978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244p.

[2] PROCHAZKOVA, D. *Zásady řízení rizik složitých technologických zařízení.*ISBN 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364p. http://hdl.handle.net/10467/72582

[3] PROCHAZKOVA, D., PROCHAZKA, J. Tools for Risk Management of Technical Facilities Operation. *European Journal of Engineering Research & Science (EJERS).* ISSN 2506-8016. 5 (2020), 4, pp. 494-500. doi10.24018/ejers.2020. 5.4.1854

[4] PROCHAZKOVA, D., PROCHAZKA, J. *Analysis, Management and Trade-off with Risks of Technical Facilities*. ISBN 978-80-01-06714-7. Praha: ČVUT 2020, 172p. http://hdl.handle.net/10467/87451

[5] PROCHAZKOVA, D. *Analýza, řízení a vypořádání rizik spojených s technickými díly.*ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222p.

[6] PROCHAZKOVA, D., PROCHAZKA, J. Complex Technical Facilities Risk Management Responsibilities. In: *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* ISBN: 978-981-11-2724-3. Singapore: ESRA 2019, pp.1735-1742, doi:10.3850/978-981-11-2724-3_0095-cd,

[7] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství.* ISBN 978-80-01-04842-9, Praha: ČVUT 2011, 369p.

[8] PROCHAZKOVA, D., PROCHAZKA, J. Risk Management Plan for Technical Facility Designing, Manufacturing and Commissioning. *International Journal of Economics and Management Systems.* ISSN: 2367-8925. 5 (2020), pp. 75-85. https://www.iaras.org/iaras/home/caijems/risk-management-plan-for-technical-facility-designing-manufacturing-and-commissioning

[9] PROCHAZKOVA, D., PROCHAZKA, J. Alternatives of Work with Risks Used at Technological Facilities Safety Management. *Universal Journal of Management.* ISSN

2331-950X, 6(2018), 8, pp. 287-294. ISSN 2331-9577, http://www.hrpub.org DOI: 10.13189/ujm.2018.060804

[10] ČVUT. Archiv. *Databáze pohrom, havárií a selhání technických děl – příčiny, dopady a poučení.*Praha: CVUT 2020.

[11] OTA. *Public Law 92-484.*www.princeton.edu

[12] KEENEY, R. L, RAIFFA, H. *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1976, 1993, 569p.

[13] US EPA. PHA Techniques in Chemical Emergency Prevention & Planning. *Newsletter* 2008, No. 8, pp. 3-6.

[14] HEINRICH, H .W. *Industrial Accident Prevention: A Scientific Approach*. New York, NY, US: McGraw-Hill 1931.

[15] LEES, F. P. *Loss Prevention in the Process Industry*, *Volumes 1-3*. Oxford: Butterworth-Heinemann 2001.

[16] PAUL SCHERRER INSTITUTE. *Database ENSAD.* Zuerich: Paul Scherrer Institute 2019.

[17] BURGHERR, P., HIRSCHBERG, S. A Comparative Analysis of Accident Risks in Fossil, Hydro, and Nuclear Energy Chains. Human and Ecological Risk Assessment. 14 (2008), 5, pp. 947-973.

[18] BURGHERR, P., ECKLE, P., HIRSCHBERG, S. Comparative Risk Assessment of Severe Accidents in the Energy Sector Based on the ENSAD database: 20 years of Experience. In: *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013.

[19] BIRD, F. E. , GERMAIN, G. L. *Damage Control.* New York: American Management Associations, Inc. 1966.

[20] GEYSEN, W. The Acceptance of Systemic Thinking in Various Fields of Technology and Consequences on Respective Safety Phylosophies. In: *Safety of Modern Systems. Congress Documentaion Saarbruecken 2001*. ISBN 3-8249-0659-7. Cologne: TŰV- Verlag GmbH, 2001, pp. 19-27.

## CONTACT ADRESS

**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.*