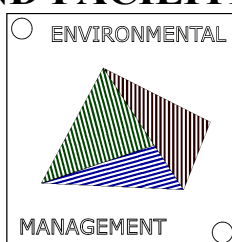


ŘÍZENÍ RIZIK TECHNICKÝCH ZAŘÍZENÍ A OBJEKTŮ


 Dana Procházková¹


RISK MANAGEMENT OF TECHNICAL EQUIPMENT AND FACILITIES




¹ Czech Technical university in Prague, Fakulta strojní, Technická 4, 166 07 Praha, Czech Republic

✉ Email: danuse.prochazkova@fs.cvut.cz

 ORCID iD: 0000-0002-4424-3974 ; <https://orcid.org/0000-0002-4424-3974>


 **Competing interests** : The author declare no competing interests.


 **Publisher's Note**: Slovak Society for Environment stays neutral with regard to jurisdictional claims in published maps and institutional affiliations. Copyright: © 2023 by the authors.



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use.

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

 **Slovak Society for the Environment** (Slovenská spoločnosť pre životné prostredie) Bratislava, Slovak Republic

ABSTRAKT

Článek shrnuje poznatky a principy inženýrských disciplín zacílených na bezpečnost. Zaměřuje se na kritické objekty a infrastruktury, které jsou důležité pro bezpečí a udržitelný rozvoj lidské společnosti a plní základní funkce státu. Shrnuje zásady pro řízení rizik ve prospěch bezpečnosti při projektování a provozu.

Klíčová slova: Inženýrství; kritické objekty a infrastruktury; riziko; bezpečnost; řízení bezpečnosti procesů a systém řízení bezpečnosti objektů.

ABSTRACT

The article summarizes the knowledge and principles of engineering disciplines focused on safety. It focuses on critical objects and infrastructures that are important for the security and sustainable

development of human society and perform the basic functions of the state. It summarizes the principles of risk management in favour of safety in design and operation.

Key words: *Engineering; critical objects and infrastructures; risk; safety; Process safety management and facility safety management system.*

1. ÚVOD

Inžénýrství zacílené na bezpečnost je inženýrská disciplína, tj. aplikovaná věda, která úzce souvisí s inženýrstvím systémů (v češtině systémovým inženýrstvím) a která zajišťuje, že inženýrské systémy mají přijatelnou úroveň bezpečnosti, tj. chovají se tak, jak je potřeba a neohrožují sebe ani své okolí. Představuje soubor znalostí a dovedností, které řeší určitý problém, tj. uspokojují požadavky, kterými jsou užitečnost, dostupnost a bezpečnost.

Dále sledujeme pojetí bezpečnosti, které se opírá o teorii systémů a je ve vyspělých zemích prosazované od 90. let. Je kodifikované deklarací a smlouvou OSN v r. 1994 [1] a v Evropské unii je kodifikované Maastrichtskou smlouvou z roku 1992 [2]. Dle Maastrichtské smlouvy je bezpečnost nejvyšším znakem kvality sledovaného objektu. V uvedeném pojetí dle poznatků shrnutých v pracích [3,4] platí:

- riziko je mírou ztrát a škod na objektu, zařízení, území, procesu, technickém vybavení i technickém díle, které může způsobit/způsobí škodlivý jev z pohledu lidské společnosti,
- bezpečnost je mírou kvality objektu, zařízení, systému, území, procesu, technického zařízení či technického díla, tj. vyjadřuje úroveň kvality souboru antropogenních opatření a činností, která vedou k zajištění bezpečí a rozvoje objektu, zařízení, území, procesu, technického zařízení i technického díla.

Dle současného poznání je riziko inherentní vlastností současného světa a je proměnné v čase i prostoru [3,4]. Proto bezpečnost každé entity lze zajistit jen permanentním řízením rizik, které aplikuje inženýrskédovednostiametodiky (risk engineering) ke zmírnění dopadů rizik [3,4]. Vzhledem k dynamickému vývoji světa, je zajištění bezpečnosti kontinuální proces. Protože riziko lze zmírnit nejen technickými, ale i organizačními opatřeními, tak doplňkovou veličinou k bezpečnosti není riziko, ale kritičnost (tj. míra rychlé změny kvality sledované entity).

Jelikož lidské znalosti, schopnosti a možnosti jsou omezené, tak se při řízení rizik soustředíme jen na podstatné položky, které označujeme jako položky kritické. Pojmy s vazbou na slovo „kritický“ se v oblasti bezpečnosti velmi rozšířily po roce 1998, ve kterém vydal prezident USA Bill Clinton Presidential Decision Directive 63, tzv. Bílou knihu [5], jejímž záměrem bylo přijetí nutných opatření pro snížení zranitelnosti důležitých sektorů kritické infrastruktury vůči fyzickým a kybernetickým útokům.

Pojem „kritický“ se v oblasti inženýrských disciplín používá u položek ve smyslu závažnosti/důležitosti pro funkčnost zařízení, objektu, území, organizace, území, státu [6], tj. je vždy spojen s pojmem bezpečnost. Označuje položku, která je zároveň potřebná a velmi zranitelná. Kritické jsou prvky, vazby mezi prvky či toky mezi prvky, procesy, funkce, komponenty, systémy či celé objekty. Pojem kritický není totožný s pojmem vyhrazený, který je v české legislativě (např. zákon č. 22/1997 Sb.), ani s pojmem krizový (např. zákon č. 240/2000 Sb.), což politici a další často používají.

2. SOUHRN POZNATKŮ O RIZIKU A BEZPEČNOSTI

Každé technické dílo zahrnuje technické prostředky, technické postupy, člověka, znalosti a dovednosti vytvářet cíleně nové produkty. Jeho vazby jsou povahy technické „stroj-stroj“, povahy smíšené „člověk-stroj“ a v posledních letech významnou roli hrají vazby „člověk-PC“ a „stroj-PC“. Toky v systému jsou energetické, materiálové, informační, finanční a instrukční aj.

Na základě současného poznání [4] je každý objekt otevřený systém, který se skládá z řady položek, které jsou vzájemně propojené. Jednotlivé položky i celek se dynamicky vyvíjí na základě procesů probíhajících uvnitř i vně systému. Propojení mezi položkami jsou fyzická, kybernetická, územní a logická a v řadě případů jsou zranitelnější než položky [3]. **Bezpečnost objektu či procesu vyjadřuje úroveň kvality souboru antropogenních opatření a činností, která vedou k zajištění bezpečí a rozvoje objektu či procesu** [3,4].

Vývoj objektu v čase je narušován jevy, které jsou světu vrozené / inherentní a mají od určité velikosti nežádoucí, a tudíž nepřijatelné dopady na objekty, které lidská společnost potřebuje pro život [4]. Mírou ztrát a škod objektu a jeho okolí je v inženýrských disciplínách riziko, které je definováno jako pravděpodobná velikost ztrát, škod a újmy na chráněných aktivech objektu a veřejných aktivech v okolí, která je normovaná na zvolené jednotky času a území. Riziko je závislé na velikosti konkrétního škodlivého jevu (pohromy) a na místní zranitelnosti aktiv [4]. Míra narušení bezpečnosti objektu se nazývá „**kritičnost**“ a závisí na velikosti škodlivého jevu a na zranitelnosti objektu, tj. zranitelnosti jeho aktiv a jejich propojení, tj. na velikosti rizika [4].

Cílem sledovaných inženýrských disciplín je snížit riziko a zvýšit bezpečnost, přičemž zvýšení bezpečnosti lze dosáhnout nejen snížením rizika, ale i vzděláním a připraveností lidí a lidské společnosti [3,4]. Řízení a vypořádání rizik vyžaduje rozměr a měření rizik, které bere v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Proto je třeba aplikovat holistický přístup a respektovat skutečnost, že riziko je rozdělené na lokální, regionální i státní úroveň.

V Evropské unii se od roku 1989 používá při řízení objektů, institucí i území řízení typu „Total Quality Management (TQM)“ [2], který je v oblasti technologických celků charakterizován v práci [7]. Předmětný typ řízení byl upraven soubory norem ISO 9000 a jejich formálními postupy certifikace v devadesátých letech 20. století. Dle tohoto konceptu jsou technická zařízení i technologické objekty (obecně entity) považovány za systémy systémů – SoS (otevřený soubor otevřených systémů) [3,4] a při jejich charakteristice se používají specifické pojmy, jako jsou: koherentnost (soudržnost); kompatibilita; operabilita; interoperabilita; integrita bezpečnosti; provozní spolehlivost; odolnost; atd. [4].

Při zajišťování bezpečnosti objektu [4] se odborně především posuzuje:

- očekávaná velikost ztrát, škod a újmy na chráněných aktivech,
- výčet nežádoucích jevů, které se mohou přihodit,
- přijatelnost dopadů rizik přímých i zprostředkovaných spletitou sítí vazeb a toků a jejich následků na aktiva, objekt jako celek a jeho okolí,
- míra schopnosti opatření zajistit ochranu
- a míra schopnosti systému řízení bezpečnosti zvládnout existující ohrožení, tj. zda zajistí, že riziko bude při realizaci akceptovatelné.

Způsob, jak rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet je prakticky vždy spojen se zvyšováním nákladů. Řízení rizika je proto vedeno snahou najít hranici, na kterou je únosné riziko snížit, aby vynaložené náklady byly společensky přijatelné. Míra určení přijatelného rizika je většinou předmětem vrcholového řízení a výsledkem politického rozhodování, a proto pro lidskou společnost je nutné, aby se přitom využily současné vědecké a technické poznatky a zohlednily ekonomické, sociální a další podmínky.

Základní principy pro práci a riziky dle [8] jsou:

- být proaktivní,
- domýšlet možné důsledky,
- správně určovat priority z pohledu veřejného zájmu,
- myslet na zvládnutí nepřijatelných dopadů,
- zvažovat synergie
- a být ostražitý.

Proto při stanovení rizika pro strategické rozhodování se musí používat hierarchický multikriteriální postup [4].

Je zřejmé, že nejsme-li schopni riziko identifikovat, analyzovat a ocenit, tak nejsme schopni se proti němu účinně bránit. Chyba, které se dopustíme při identifikaci, analýze a hodnocení 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. Platí moudrost uvedená v práci [9] „Vědět znamená přežít, ignorovat znamená říkat si o zničení“, ze které vyplývá, že ignorování či podceňování řízení a vypořádání rizik je důvodem většiny problémů, nezdarů a katastrof.

3. BEZPEČNOST A SPOLEHLIVOST

Bezpečný objekt je systém, který je zajištěn vůči všem škodlivým jevům, a který ani při svých kritických podmínkách neohrožuje sebe a své okolí, tj. prostor, ve kterém žijí lidé [4]. To znamená, že **bezpečnost systému** je vlastnost systému, která je nadřazena spolehlivosti [3].

Proto parametry, které určují kvalitu systému, jsou uspořádány do pořadí:

- *bezpečnost*, tj. schopnost systému předcházet kritickým stavům systému (aktivní bezpečnost využívá prvky řízení; pasivní bezpečnost využívá ochranné prvky) a při jejich výskytu neohrozit existenci ani sebe, ani svého okolí,
- *spolehlivost*, tj. schopnost systému poskytovat požadované funkce za daných podmínek, v dané kvalitě a v daném časovém intervalu,
- *dostupnost*, tj. schopnost systému poskytovat požadované funkce při výskytu procesu, který danou funkci využívá,
- *integrita*, tj. schopnost systému poskytovat časově korektní a platná hlášení uživatelům o poruchách systému,
- *kontinuita*, tj. schopnost systému poskytovat požadované funkce bez přerušení během vyvolání procesu,
- *přesnost*, tj. schopnost systému zajistit požadované chování systému v požadovaném rozmezí.

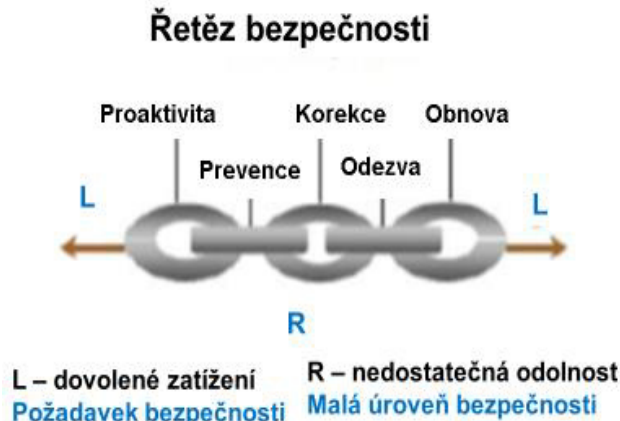
Z výzkumu shrnutého v práci [3] vyplývá, že:

- bezpečný systém je spolehlivý, ale obráceně to neplatí,
- systém bezpečných systémů není vždy bezpečný systém (problémy jsou vazby a toky mezi systémy), a proto je vždy nutno řešit zvláště otázky jak bezpečnosti jednotlivých systémů, tak jejich souboru,
- typy selhání objektů jsou příčinné, eskalující a kaskádovité,
- charakteristiky infrastruktur jsou prostorové (geografické), časové, provozní a organizační,
- vazby mezi položkami objektů a infrastruktur jsou volné, flexibilní nebo těsné s tím, že těsné vazby nedovolují přizpůsobení.

Nicméně je třeba vzít v úvahu, že v současné době se používají 3 vyhraněné inženýrské koncepty, které pracují s riziky: inženýrství spolehlivosti objektu či zařízení; inženýrství zacílené na zabezpečení objektu či zařízení; a inženýrství zacílené na bezpečnost objektu či zařízení. Všechny tři uvedené koncepty jsou založené na řízení rizik a používají stejné postupy, metody, nástroje i techniky. Praxe ukazuje, že mezi nimi jsou občas konflikty [3]. U kritických objektů, kterými jsou elektrárny, přehrady, doly, překladiště, kritické infrastruktury, průmyslové a dopravní stavby, překladiště, nádraží, letiště, nemocnice atd. je nutné inženýrství zacílené na bezpečnost, protože předmětné objekty zajišťují služby, které jsou důležité pro základní funkce státu.

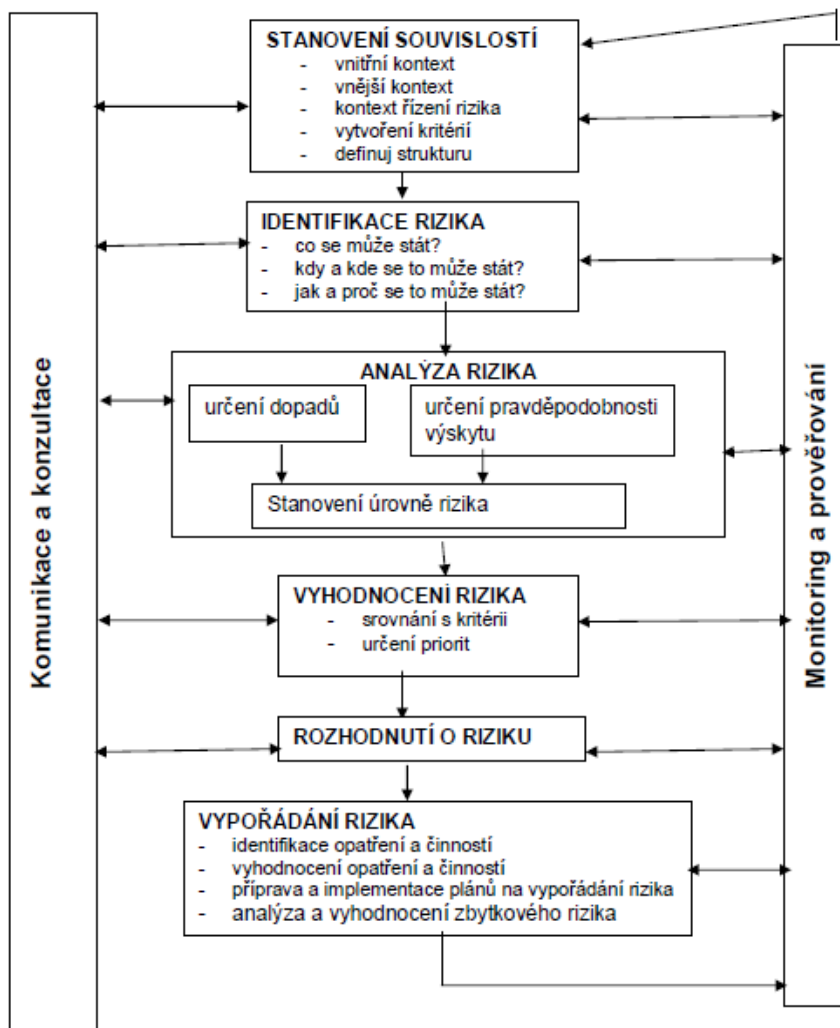
4. POSTUP ŘÍZENÍ RIZIK PŘI ZAJIŠŤOVÁNÍ BEZPEČNOSTI

Při řízení rizik se používá řetěz bezpečnosti, obrázek 1.



Obr. 1. Činnosti pro zajištění bezpečnosti sledovaného systému.

Logika postupu řízení rizik dle ISO 31000 je zobrazena na obrázku 2.



Obr. 2. Postup řízení rizik dle ISO 31000.

Při řízení rizik [4] hrají roli:

- cíle řízení rizik, tj. požadovaná úroveň bezpečnosti,
- metody a postupy k dosažení stanoveného cíle,
- kompetence institucí a osob, které rozhodují o opatřeních a financích potřebných na opatření pro zmírnění rizik,
- požadavky norem a standardů, které stanoví legislativa,
- a limity (znalostní, finanční, materiálové a popř. i jiné), které je nutné zvažovat v praxi.

Protože, jak již bylo výše uvedeno, nikdy není dostatek zdrojů, sil a prostředků, tak se v inženýrské praxi orientujeme jen na kritické atributy, tj. jen na kritické položky a nepřijatelná a podmíněně přijatelná rizika, která označujeme ALARA / ALARP. Používáme:

- a) ISO normy založené na projektovém řízení typu TQM (Total Quality Management) [7], tj. normy řady ISO 9000, 14000, 18000, 31000, 31010 aj. Příklad dalších je v tabulce 1.

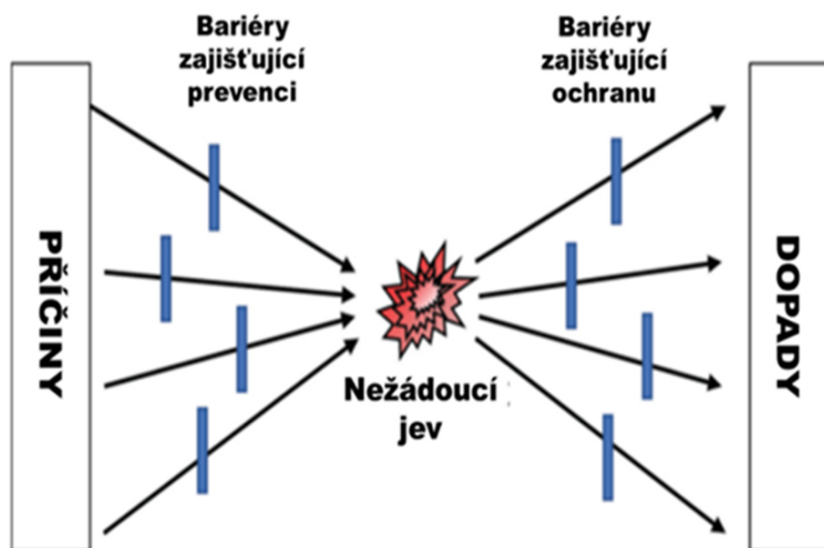
Tabulka 1. Příklady norem podporujících zajištění bezpečnosti technických zařízení.

Značka	Oblast
EN/ISO 12100	Bezpečnost strojních zařízení
EN/ISO 13849	Bezpečnost strojních zařízení - bezpečnostní části ovládacích systémů
EN/ISO 13855	Bezpečnost strojních zařízení - umístění ochranných zařízení
EN/ISO 13850	Bezpečnost strojních zařízení – funkce nouzového zastavení
EN/ISO 14120	Bezpečnost strojních zařízení – ochranné kryty
EN/ISO 10218	Roboty a robotická zařízení - Požadavky na bezpečnost
ISO/IEC 27000	Informační technologie - bezpečnostní techniky - systémy řízení bezpečnosti informací
ISO/IEC 15408	Informační technologie - bezpečnostní techniky - kritéria pro hodnocení bezpečnosti IT
IEC 62443	Průmyslová kybernetická bezpečnost
EN 61508	Funkční bezpečnost řídicích systémů. Harmonizovaná je pouze její sektorová norma EN 62061.
ISO 26262	Funkční bezpečnost elektrických a elektronických systémů ve vozidlech
IEC 62 443	Zabezpečení automatizovaných průmyslových a řídicích systémů
IEC 61511	Funkční bezpečnost v průmyslu
IEC 61513	Bezpečnost jaderné energetice
ISO/DIS 26262	Funkční bezpečnostv automotive
IEC 60601	Bezpečnost v medicíně
IEC 80001	Bezpečnost v medicíně
CENELEC EN 50126	Bezpečnost železnice
CENELEC EN 50128	Bezpečnost železnice
CENELEC EN 50129	Bezpečnost železnice
CENELEC EN 50159	Bezpečnost železnice
MIL-STD-882E	Bezpečnost systémů / produktů / zařízení / infrastruktur (hardware i software) po celou dobu existence – od návrhu, vývoje, testování, výroby, používání a likvidace.

- b) **Postup pro řízení rizik** [4], který zahrnuje:

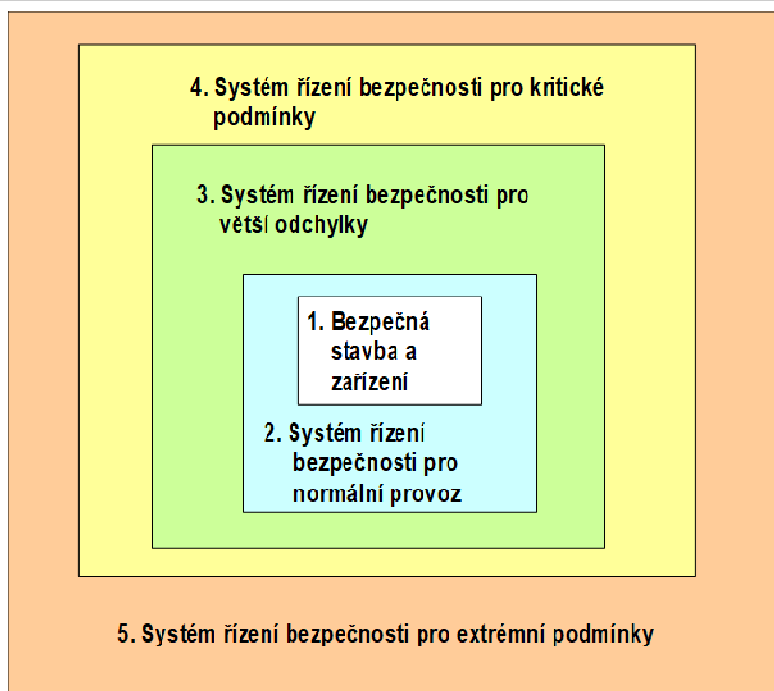
- identifikaci rizik dle principu All-Hazard-Approach [11,12]. Dle[3,4,10,13] je třeba u technických entit sledovat zdroje rizik:
 - chyby v řízení a ovládání entity (procesu /objektu/zařízení/systému/komponenty),
 - vnitřní zdroje rizik entity spojené s jejím projektem, konstrukcí, jejími propojeními a provozem,
 - chyby personálu obsluhy entity při provozu,
 - vnější zdroje rizik entity spojené s živelními pohromami,
 - vnější zdroje rizik entit spojené se selháním okolních entit a procesů (vazby a toky) – např. selhání dodávek elektřiny, vody, chladiva, dodávek materiálu, dopravy atd.,
 - vnější zdroje rizik entity spojené s chováním veřejné správy (daně, poplatky, pobídky apod.), konkurencí, trhem apod.,
 - útoky na entitu,
 - kybernetické zdroje rizik spojené s automatizací a komunikacemi uvnitř i vně entity,
 - válka,
 - chybný dozor veřejné správy,
- určení rizik a jejich klasifikace dle[4,7,10,13] na:
 - seznam vyhodnocených rizik,
 - seznam rizik vyžadujících nejvyšší pozornost
 - a seznam neaktuálních/vyřešených rizik,
- rozdělení rizik vyžadujících pozornost při provozu [3,10,13] dle postupu na obrázku 3 takto:
 - rizika, která se eliminují preventivními opatřeními v projektu,
 - rizika, která se zmírňují odezvou při provozu a pro která musí být vložena v projektu technická opatření, která umožňují kvalitní odezvu.

Um projektanta spočívá ve správném rozdělení rizik,



Obr. 3. Rozdělení rizik na ta, která se zvládnou preventivními opatřeními vloženými do projektu a na ta, pro která do projektu musí být vložena technická opatření, která umožní kvalifikovanou odezvu[13].

- aplikaci principů inherentní bezpečnosti,
- aplikaci principu ochrany do hloubky (obrázek 4),



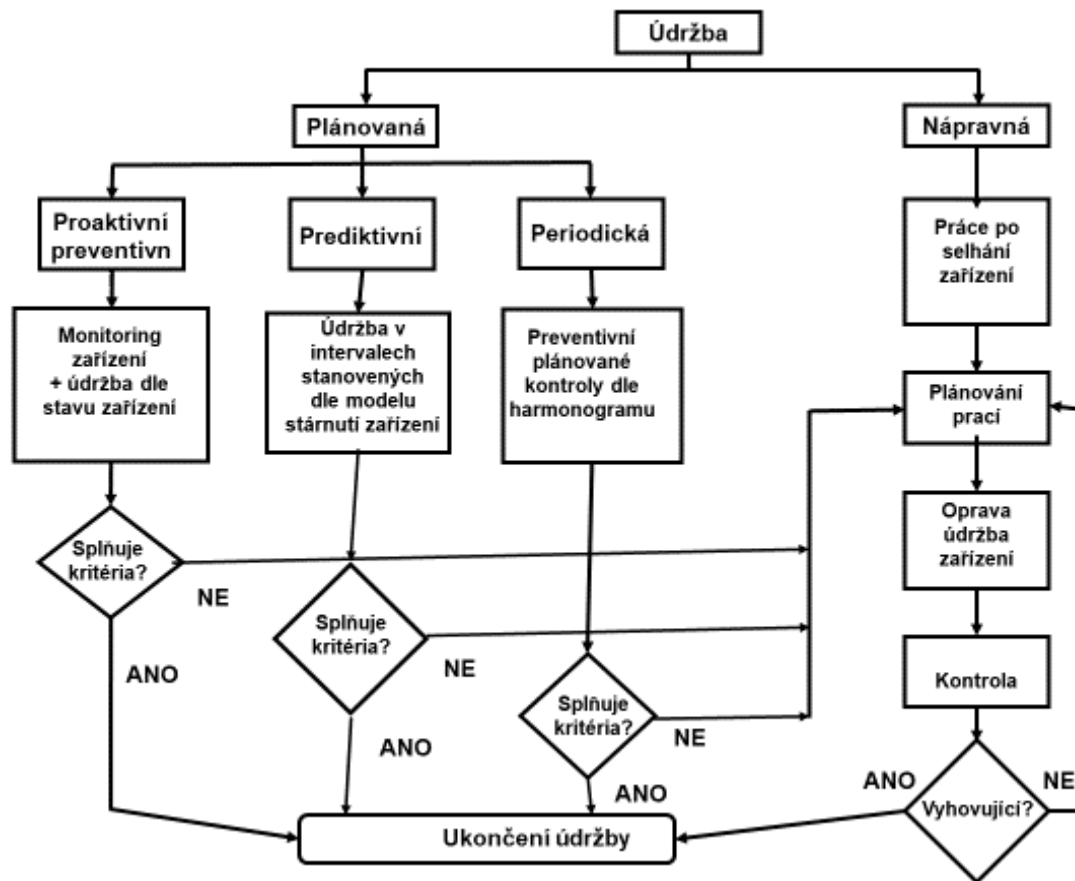
Obr. 4. Princip ochrany do hĺbky [13].

- monitoring provozu a řízení rizik výrobních a dalších procesů včetně údržby v čase [14,15] (obrázek 5).



Obr.5. Procesní model řízení bezpečnosti entity v čase. Procesy: 1- koncepce a řízení; 2 - administrativní po-stupy; 3 - technické záležitosti (technická problematika entity a jejího okolí); 4 - vnější spolupráce; 5 - nouzová připravenost; 6 - dokumentace a šetření havárií; a 7 - zabezpečení entity – zpracováno dle [15].

Na základě současných znalostí a zkušeností se dnes v praxi u kritických entit doporučuje aplikace proaktivní preventivní údržby [16] – obrázek 6, protože tento typ údržby vede k dlouhodobé životnosti kritických zařízení,



Obr. 6. Srovnání typů údržby; zpracováno dle [10,16].

- plán řízení rizik (ISO 31 000) pro případ selhání zařízení nebo procesu v entitě. Plán řízení rizik je nástroj proaktivního řízení rizik. V inženýrské praxi se zaměřuje pouze na kritické atributy, tj. pouze na nepřijatelná a podmíněně přijatelná rizika (ALARA/ALARP) [3,10]. Přijatelnost souvisí s veřejným zájmem, kterým je bezpečná kritická infrastruktura, která zajišťuje základní funkce státu, tj. její bezpečné objekty a jejich bezpečná propojení. Plán řízení rizik je vypracován ve formě tabulky, která obsahuje: příčiny rizika; popis dopadů rizik na veřejný majetek a služby poskytované danou entitou; četnost výskytu poruch a velikost dopadů selhání dané entity stanovené na základě místní databáze příčin selhání sledované entity; a zajištění odezvy na realizaci rizika:

- řízení rizik nebo alespoň jasně stanovená zmírňující opatření. Jde o opatření: technická; organizační; personální; metodická, vzdělávací a finanční,
- pro každou akci, je určena osoba fyzická nebo právnická (nebo její odpovědný zástupce), která zajistí odezvu,
- u každé akce je uvedena osoba odpovědná za správné a včasné provedení odezvy.

Plán řízení rizik je osvědčeným strategickým nástrojem, který se v evropských zemích používá k udržení a zvýšení bezpečnosti zařízení, objektů, organizací celých technických děl. Používá se k řízení prioritních rizik způsobených přírodními pohromami, technologickými haváriemi a poruchami, jakož i lidského faktoru tak, aby se:

- zvýšilo bezpečí lidí a entity samotné;
- zlepšily služby entity regionům, které jsou důležité pro životní podmínky lidí;

- podporoval rozvoj a konkurenceschopnosť regiónů;
- a zlepšila ochrana životného prostredia.

7. ZÁVĚR

Snížování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, apod., a proto se v praxi hledá hranice, na kterou je únosné riziko snížit tak, aby vynaložené náklady byly ještě rozumné. Tato míra rizika (určitá optimalizace) je většinou předmětem vrcholového řízení a výsledkem politického rozhodování, při kterém je z hlediska zajištění rozvoje nutné, aby se využily současné vědecké a technické poznatky a zohlednily ekonomické, sociální a další podmínky.

Ačkoliv koncept integrální bezpečnosti se rozšiřuje v praxi pomalu z důvodů uvedených v práci [12], je třebaho prosazovat, protože do pojetí integrální bezpečnosti patří i život podporující funkce, jejichž rizika s ohledem na zdraví člověka, ekosystémy a bezpečnost systému se minimalizují. Popsaný model pro řízení bezpečnosti objektů (a to hlavně kritických) ukazuje způsob řízení rizik, aby se předešlo, anebo alespoň zmírnilo možným nežádoucím a nepřijatelným dopadům. Jeho respektování zajišťuje, že všichni zúčastnění chápou řízení rizik ve prospěch bezpečnosti stejně. Jednotné chápání rizik, způsobů a cílů jejich řízení dovoluje odstranit příčiny havárií, které vznikly různým chápáním rizik specialisty různých oborů [17, 18].

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] UN. *Human Development Report*. New York: UN 1994, www.un.org.
- [2] EU. Maastricht Treaty (C 191, 29.7.1992, pp.s. 1–112) ve znění pozdějších předpisů
- [3] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN: 978-80-01-06180-0, e-ISBN 978-80-01-06182-4. Praha: ČVUT 2017, 364p.
Doi:[10.14311%2FBK.9788001061824](https://doi.org/10.14311/2FBK.9788001061824)
- [4] PROCHÁZKOVÁ D. *Analýza, řízení a vypořádání rizik spojených s technickými díly*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. Doi:[10.14311%2FBK.9788001064801](https://doi.org/10.14311/2FBK.9788001064801)
- [5] CLINTON, B. *Presidential Decision Directive 63*. Washington: White House 1988, 18 p.
- [6] EPRI. *Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications*. Revision 1 to EPRI NP-5652 and TR-102260. Palo Alto: EPRI 2014, 378 p.
- [7] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991.
- [8] HAIMES, Y. Y. 2009. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis* 29(2009), 12, pp. 1647–1654.
- [9] FAWCETT, H.H. *Hazardous and Toxic Materials. Safe Handling and Disposal*. New York: Willey 1984.
- [10] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Řízení rizik procesů spojených s provozem technického díla během jeho životnosti*. ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p., Doi:[10.14311%2FBK.9788001066751](https://doi.org/10.14311/2FBK.9788001066751)
- [11] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.
- [12] EU. *FOCUSProject*. Brussels: EU 2012, <http://www.focusproject.eu/documents/14976/-5d763378-1198-4dc9-86ff-c46959712f8a>
- [13] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. In: *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207p. Doi:[10.14311%2FBK.9788001066096](https://doi.org/10.14311/2FBK.9788001066096)

- [14] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191 p.
- [15] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. Praha: ČVUT 2022, 129 p. doi:10.14311/BK.978 80010 69950
- [16] EPRI. *Guideline on Proactive Maintenance. Technical Report*. Palo Alto: EPRI 2001, 82 p.
- [17] CEPIN, M., BRIS, R. (eds). *Safety and Reliability – Theory and Applications*. ISBN 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.
- [18] HAUGEN, S., VINNEM, J., E., BARROS, A., KONGSVIK, T., VAN GULIJK, C. (eds). *Safe Societies in a Changing World*. ISBN 978-0-8153-8682-7. London: Taylor & Francis Group 2018, 3234 p. <https://www.ntnu.edu/esrel2018>.