Řízení rizik procesů, zařízení a složitých technických děl zacílené na bezpečnost 2023

Praha 2023

Recenzenti:

Doc. Ing. Hana Bartošová, CSc. Dr.h.c.

Doc. Ing. Branislav Lacko, CSc.

RNDr. Jan Procházka, Ph.D.

Editor:

Doc. RNDr. Dana Procházková, CSc., DrSc.

ISBN 978-80-01-07239-4

Doi: https://doi.org/10.14311/BK.9788001072394

OBSAH

ÚVODNÍ SLOVO EDITORA

Publikace „***Řízení rizik procesů, zařízení a složitých technických děl zacílené na bezpečnost 2023***“ je věnována rizikům a jejich řízení ve prospěch bezpečnosti především v oblasti technologií. Publikace obsahuje úvodní přehled problematiky bezpečnosti a 25 odborných sdělení. Sdělení obsahují výsledky:

- teoretických studií,
- experimentálních prací,
- řešení závažných úkolů praxe,
- identifikace a řešení problémů kyber-fyzických systémů
- a vyhodnocení zkušeností z praxe.

Údaje i výsledky uvedené ve sděleních ukazují řadu problémů, které je třeba řešit s cílem zajistit bezpečnost zařízení, celých kompletních technických celků i experimentů. Ukazují, že bezpečnost sledovaných entit, tj. procesů i objektů, je významně ovlivněna nejen vnitřními podmínkami, ale také vnějšími podmínkami a jejich vývojem v čase a s tím spojeným nedostatečným lidským poznáním a schopnostmi.

Lidský faktor se projevuje jako základním činitel při řízení rizik ve prospěch bezpečnosti na všech úrovních řízení a provádění činností; a to ve smyslu pozitivními i negativním. Proto u řízení rizik ve prospěch bezpečnosti veřejných aktiv, zařízení, procesů i složitých technických děl je důležité zvažovat jak systémové pojetí světa, který má povahu socio-kyber-fyzickou, tak proměnnosti limitů a podmínek v prostoru a čase.

Odborná sdělení ve sborníku jsou uspořádána alfabeticky dle příjmení prvního autora s přihlédnutím k počtu autorů. Řada sdělení obsahuje výsledky národních projektů České republiky či výsledky projektů ČVUT, Fakulta strojní. Všechna sdělení byla editována a recenzována s cílem zajistit vysokou odbornost při dodržení požadavků platné legislativy; všechny připomínky recenzentů byly vypořádány a do konečné verze zapracovány.

Velký dík patří recenzentům publikace *paní Doc. Ing. Haně Bartošové, CSc., Dr.h.c., panu Doc. Ing. Branislavu Lackovi, CSc. a panu RNDr. Janu Procházkovi, Ph.D.,* kteří uvedli konkrétní připomínky k článkům z publikace a u článků, které vyžadovaly větší úpravy, uvedli konkrétní připomínky a doporučení.

Vybraná sdělení byla navíc prezentována na stejnojmenném semináři ČVUT v Praze, Fakulta strojní v budově Praha 6, Technická 4, dne 9. listopadu 2023.

Poděkování editora za podporu semináře patří vedení Fakulty strojní; speciálně ústavům energetiky a technologií, za podporu při přípravě semináře. Osobní poděkování vyslovuje editor panu doc. Ing. Václavu Dostálovi, Ph.D. za jeho podporu semináře i zpracování publikace a paní Dušaně Táborské za pomoc při semináři.

SUMMARY

The publication "Risk Management of Processes, Equipment and Complex Technical Installations Targeted for Safety 2023" is dedicated to risks and their management in favour of safety, especially in the field of technologies. The publication contains an introductory overview of safety issues and 25 professional papers. Each paper has English abstract. The papers contain the results of:

- theoretical studies,
- experimental works,
- solving serious tasks of practice,
- identification and solution of cyber-physical
- and systems evaluation of practical experience.

The data and results presented in the papers show a number of problems that need to be addressed in order to ensure the safety of the equipment, the entire technical units and the experiments. They show that the safety of the monitored entities, i.e. processes and objects, is significantly influenced not only by internal conditions, but also by external conditions and their development over time and the associated lack of human knowledge and abilities.

The human factor emerges as an essential factor in risk management for the benefit of safety at all levels of management and execution of activities; both in a positive and negative sense. Therefore, in risk management in favour of the safety of public assets, facilities, processes and complex technical installations, it is important to consider both, the systemic concept of the world, which is socio-cyber-physical in nature, and the variability of limits and conditions in space and time.

The professional papers in the proceedings are arranged alphabetically according to the surname of the first author, considering the number of authors. A number of papers contains the results of national projects of the Czech Republic or the results of projects of the Czech Technical University, Faculty of Mechanical Engineering.

All communications have been reviewed and edited in order to ensure a high level of professionalism while complying with the requirements of applicable legislation; all of the reviewers' comments have been incorporated into the final version.

SOUHRN POZNATKŮ O BEZPEČNOSTI PROCESŮ, TECHNICKÝCH ZAŘÍZENÍ A TECHNOLOGICKÝCH OBJEKTŮ

SUMMARY OF KNOWLEDGE ABOUT THE SAFETY OF PROCESSES, TECHNICAL EQUIPMENT AND TECHNOLOGICAL OBJECTS

Dana Procházková

ČVUT v Praze, fakulta strojní, Technická 4, 166 07 Praha, danuse.prochazkova@fs.cvut.cz

Abstrakt: Článek je úvodem k dalším sdělením ve sborníku, která se týkají bezpečnosti a rizik. Shrnuje současné pojetí bezpečnosti a řízení rizik ve prospěch bezpečnosti u procesů a technologických celků, které je prosazované ve vyspělých zemích od 90. let.

Klíčová slova: Inženýrství, riziko, bezpečnost, řízení bezpečnosti procesů, řízení bezpečnosti systémů.

Abstract: The article is an introduction to other papers in the proceedings, which related to safety and risks. It summarizes the current concept of safety and risk management in favour of safety in processes and technological units, which has been promoted in developed countries since the 1990s.

Key words: Engineering, risk, safety, process safety management, system safety management.

1. ÚVOD

Inženýrství zahrnuje mnoho specializací, které se věnují problémům spojeným s vývojem a užíváním určitého druhu výrobku nebo objektu, s využíváním určité technologie pro zajištění základních služeb podporujících bezpečí a rozvoj lidské společnosti. Jde o proces, kterým je vyvíjena a provozována technologie. Představuje širokou disciplínu, která řeší problémy od jejich pochopení, přes návrh řešení až po realizaci v daných podmínkách. Inženýrské disciplíny jsou hnací silou lidského vývoje, protože se zabývají i problémy, které je obtížné přesně řešit a k dosažení cíle používají kreativitu lidských jedinců a přístupy označované jako dobrá praxe.

V životě společnosti se stále více ukazuje, že neschopnost řídit rizika ve prospěch bezpečnosti má za následek obrovské náklady, lidské i ekonomické [1-7]. Multidisciplinární povaha disciplíny, která řídí rizika ve prospěch bezpečnosti vyžaduje širokou škálu odborníků. Proto vznikla speciální disciplína, tj. inženýrství zabývající se řízením rizik zacíleným na bezpečnost (používá se i název forenzní inženýrství).

Inženýrství 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, disponibilita a bezpečnost, a to na základě principů systémových disciplín. Inženýrské disciplíny:

- jsou hnací silou lidského vývoje, protože se zabývají i problémy, které je obtížné přesně řešit,
- k dosažení cíle používají kreativitu lidských jedinců a přístupy označované jako dobrá praxe.

V práci 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 [8] a v Evropské unii je kodifikované Maastrichtskou smlouvou z roku 1992 [9]. Dle Maastrichtské smlouvy je bezpečnost nejvyšším znakem kvality sledovaného objektu. V uvedeném pojetí dle poznatků uvedených v pracích [10,11] 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 [10,11]. Proto bezpečnost každé entity lze zajistit jen permanentním řízením rizik, které aplikuje inženýrské dovednosti a metodiky (risk engineering) ke zmírnění dopadů rizik [10,11]. 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).

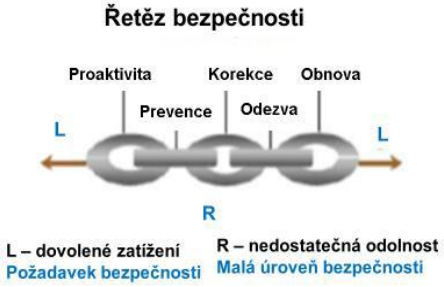
Jelikož lidské znalosti, schopnosti a možnosti jsou omezené, tak se při řízení rizik soustřeďujeme jen na podstatné položky, které označujeme jako položky kritické. Pojmy s vazbou na slovo „kritický" se v oblasti bezpečnosti velmi rozšířily po roce 1998, ve kterém vydal prezident USA Bill Clinton Presidential Decision Directive 63, tzv. Bílou knihu [12], 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 [13], 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.

V Evropské unii se od roku 1989 používá při řízení objektů, institucí i území řízení typu „Total Quality Management (TQM)" [9], který je v oblasti technologických celků charakterizován v práci [14]. Předmětný typ řízení je 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) [10,11] a při jejich charakteristice se používají specifické pojmy jako jsou: koherentnost (soudržnost); kompatibilita; operabilita; interoperabilita; integrita bezpečnosti; provozní spolehlivost; odolnost; atd. [11].

2. SOUČASNÉ POSTUPY PRO ZAJIŠŤOVÁNÍ BEZPEČNOSTI

V ideálním případě inženýři zabývající se bezpečností zvažují první návrh systému zařízení nebo technického díla, analyzují jej, aby zjistili, jaké poruchy se mohou vyskytnout, a poté navrhnou požadavky na bezpečnost, které musí být specifikovány v konstrukčních specifikacích a změny v návrhu s cílem zvýšit bezpečnost. To znamená, že řízení rizik ve prospěch bezpečnosti se v technice provádí od projektování až po ukončení provozu sledovaného objektu, a to procesu nebo objektu [10,11,15]. Při řízení rizik se používá řetěz bezpečnosti, obrázek 1.



Obr. 1. Činnosti pro zajištění bezpečnosti sledovaného systému.

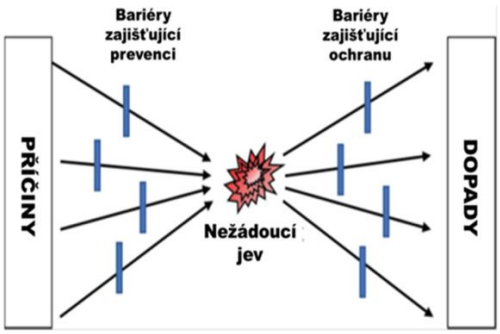
Při řízení rizik [11] hrají roli:

- cíle řízení, tj. požadovaná úroveň bezpečnosti,
- metody a postupy k dosažení cílů,
- kompetence institucí a osob, které rozhodují o opatřeních a financích,
- 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:*

1. ISO normy založené na projektovém řízení typu TQM (Total Quality Management) [14], tj. ISO 9000, 14000, 18000, 30 000, 30 010 aj.
2. ***Postup pro řízení rizik*** [11], který zahrnuje:

- identifikaci rizik dle principu All-Hazard-Approach [16,17]. Dle [10,11,15,18] 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 [11,14,15] na:
  - seznam vyhodnocených rizik,
  - seznam rizik vyžadujících nejvyšší pozornost
  - a seznam neaktuálních/vyřešených rizik,
- rozdělení rizik vyžadujících pozornost při provozu [10,15,18] dle postupu na obrázku 2 takto:
  - rizika, která se eliminují preventivními opatřeními v projektu,
  - rizika, která se zmírňují odezvou při provozu a pro která musí být vložena v projektu opatření, která umožňují kvalitní odezvu,

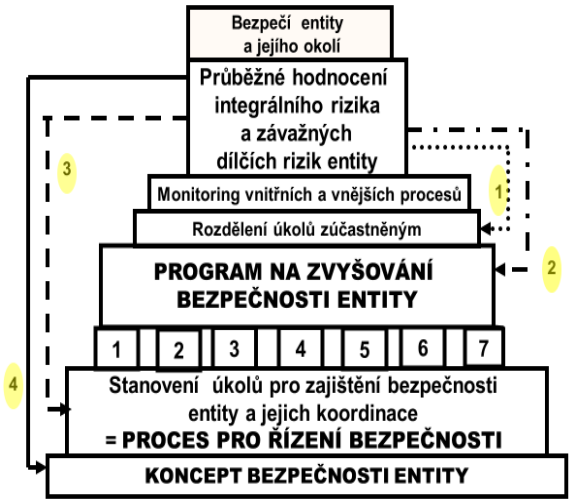


Obr. 2. Rozdělení rizik na ta, která se zvládnou preventivními opatřeními vloženými do projektu a na ta, pro která do projektu musí být vložena technická opatření, která umožní kvalifikovanou odezvu.

- aplikaci principů inherentní bezpečnosti,
- aplikaci principu ochrany do hloubky,
- monitoring provozu a řízení rizik výrobních a dalších procesů včetně údržby v čase (obrázek 3) [19,20]. Na základě současných znalostí a zkušeností se v praxi u kritických entit doporučuje aplikace proaktivní preventivní údržby [21],
- 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) [10,15]. 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,
- 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.



Obr. 3. 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 [19,20].

Plán řízení rizik je osvědčeným strategickým nástrojem, který se ve vyspělých zemích používá k udržení a zvýšení bezpečnosti zařízení, objektů, organizací a 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 konkurenceschopnost regionů
- a zlepšila ochrana životního prostředí.

Při řízení bezpečnosti rozlišujeme 2 zásadní postupy, a to: řízení bezpečnosti procesů; a řízení bezpečnosti technologických celků.

2.1. Řízení bezpečnosti procesů

Bezpečnost procesů je soubor opatření a činností, který zajišťuje bezpečný provoz, tj. bezpečný průběh procesů, např. v případě chemických procesů se zaměřují na prevenci požárů, výbuchů a úniků nebezpečných látek do životního prostředí [22]. Specifická disciplína řízení bezpečnosti procesů (PSM – Process Safety Management) se vyvíjí posledních 40 let minulého století a jejím cílem je zajistit bezpečné procesy, které probíhají v technologiích. Jde o řízení principů a systémů pro identifikaci možných ohrožení, pochopení a zvládnutí procesů vedoucích k realizaci rizik. Jedná se o složitý postup, který vyžaduje vícerozměrný přístup, který kombinuje technologie a jejich řízení [10].

Řízení bezpečnosti procesů je široce používáno v továrnách a dalších automatizovaných prostředích k zajištění efektivity výroby. Technologie řízení bezpečnosti procesů je obecně navržena tak, aby monitorovala senzory a nastavovala důležité veličiny podle naměřených hodnot. Tato technologie umožňuje relativně malé skupině lidí řídit složité operace a pomáhá zajistit, aby bylo trvale dosaženo požadovaného výsledku. Řízení bezpečnosti procesů je spojeno s kulturou bezpečnosti a *pro hodnocení bezpečnosti se často používají kontrolní seznamy* [23].

2.2. Řízení bezpečnosti technologických celků

Každý technologický celek je systém, který se skládá z několika propojených systémů, tj. tvoří více či méně složitý systém systémů. *Bezpečnost systému* je soubor opatření a činností, který zajišťuje bezpečné technické dílo a jeho bezpečné okolí. Předmětná disciplína vznikla na základě systémového přístupu ve strojírenských oborech. Integrální (celková, objektová) bezpečnost má své kořeny v inženýrství bezpečnosti průmyslu , které sahá až do 19. století a které po 2. světové válce aplikovalo disciplíny: systémové inženýrství; a systémovou analýzu k řešení nových a složitých inženýrských problémů. V daném případě je bezpečnost chápaná jako vlastnost, která vystupuje na úrovni systému, když jsou komponenty provozovány společně. Události vedoucí k nehodě jsou pak složitou kombinací chyb zařízení, nesprávné údržby, problémů s informačním a řídicím systémem, lidského zásahu a konstrukčních chyb [19].

Bezpečnost systému ve sledovaném pojetí spočívá v aplikaci technických a manažerských dovedností při identifikaci, analýze, hodnocení a řízení škodlivých jevů a souvisejících rizik pomocí systémového přístupu [11,15]. Z praktických důvodů musí být přístupy používané e sledované oblasti účinné a cenově dostupné. Orientace na bezpečnost musí být součástí systému řízení podniku a zároveň musí respektovat omezení, která vyplývají z vnějšího světa.

Bezpečnost systému aplikovaná na technická díla využívá teorii systémů a systémové inženýrství k prevenci předvídatelných nehod a k minimalizaci následků nepředvídatelných nehod. V moderním pojetí se obecně zajímá o všechny ztráty a škody, a to nejen o smrtelné nehody nebo zranění a škody na majetku, ale také o nesplnění poslání (mise, účelu) nebo poškození životního prostředí. Klíčovým bodem disciplíny je považovat ztráty za natolik závažné, aby se na jejich prevenci věnoval dostatek času, úsilí a zdrojů. Výše investic věnovaných na prevenci nehod a/nebo jejich dopadů do značné míry závisí na sociálních, politických a ekonomických faktorech. Proto u technologií, které mohou mít vážné důsledky, je požadavek předběžné opatrnosti uložen právními předpisy, aby byla zajištěna ochrana veřejných aktiv [15].

Řízení bezpečnosti systémů je používáno při řízení technologických celků, celých továren, elektráren atd. Jde o integrované řízení 7 procesů (obrázek 3) [19,20]:

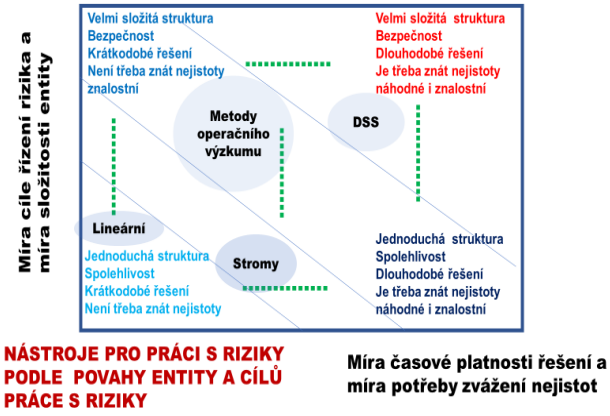
1. Proces návrhu a realizace koncepce a řízení, který je dále rozdělen do dílčích procesů, aby byly zajištěny: celková koncepce bezpečnosti; dílčí cíle bezpečnosti; řízení/správa bezpečnosti; systém řízení bezpečnosti; zaměstnanci (podproces se dále dělí do následujících oddílů: řízení lidských zdrojů, školení a vzdělávání, interní komunikace/povědomí a pracovní prostředí); a přezkoumání a hodnocení plnění cílů bezpečnosti.
2. Proces provádění administrativních postupů, který se dále dělí na dílčí procesy, aby byly zajištěny: identifikace ohrožení od možných pohrom hodnocení rizik; vedení dokumentace; administrativní postupy (včetně systémů pracovního povolení); řízení změn; bezpečnost ve spolupráci s dodavateli; a dohled nad bezpečností výrobků.
3. Proces technických záležitostí, který je dále rozdělen do dílčích procesů pro: výzkum a vývoj; projektování a montáž; inherentní bezpečnost procesu; průmyslové normy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů.
4. Proces externí spolupráce, který se dále dělí na: spolupráci se správními orgány; spolupráci s veřejností a dalšími zúčastněnými stranami (včetně akademických pracovišť); a spolupráci s jinými podniky.
5. Proces havarijní připravenosti a odezvy na havárie a nehody, který se dále dělí na dílčí procesy pro: plánování připravenosti na odezvu uvnitř technického díla; usnadnění plánování připravenosti na odezvu vně technického díla (které spadá do odpovědnosti veřejné správy);a koordinaci, jakož i činnosti resortních organizací při zajišťování havarijní připravenosti a odezvy.
6. Proces zpracování hlášení a vyšetřování havárií/skoronehod, který se dále dělí na podprocesy pro: zpracování zpráv o haváriích, nehodách, skoronehodách a dalších významných zkušenostech; vyšetřování nežádoucích jevů; a r odezvu na havárie a nehody a následná opatření (včetně uplatňování získaných zkušeností a sdílení informací).
7. Proces fyzické a kybernetické bezpečnosti technického zařízení, který se dále dělí na podprocesy pro zajištění: fyzické bezpečnosti; a kybernetické bezpečnost proti hackerům a teroristům.

Inženýrství orientované na bezpečnost cíleně provádí úkoly řízení bezpečnosti, tj. úkoly řízení rizik ve prospěch bezpečnosti a vývoje lidského systému. V technickém slangu hovoříme o vytvoření inherentní bezpečnosti technického díla proti projektovým pohromám pomocí řízení bezpečnosti. Při uplatňování zásady předběžné opatrnosti zajišťujeme zvýšení odolnosti vůči nepřijatelným dopadům nadprojektových pohrom, jejichž výskyt je tak

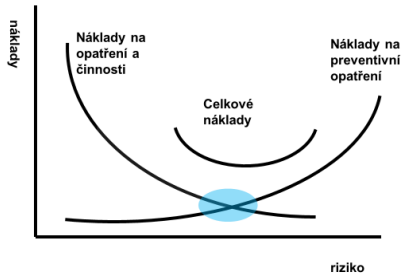
nepravděpodobný, že je nepředvídatelný. Do praxe se v technologiích na základě zmíněných cílů zavádí principy jako „selži bezpečně“, „prováděj jen určené funkce, tj. když nemůžeš splnit cíl, tak nic nedělej“… [10].

Při práci s riziky ve prospěch bezpečnosti u technologických celků se používají složitější metody [11]; obrázek 4. Vzhledem k tomu, že zdroje každé entity jsou omezené, je třeba porovnávat náklady na snížení rizika a náklady na nutná opatření, tj. jde o aplikaci metody CBA [24] s vyhověním požadavkům na bezpečnost; obrázek 5.

U důležitých technických děl jde v praxi nejen o bezpečnost, ale i o výkonnost [24], protože je tak může být technologický celek konkurenceschopný. To znamená, že technologický celek musí mít velkou resilienci (houževnatost), tj. schopnost udržet si i v náročných situacích vnitřní kontinuitu, která zajišťuje požadovanou výkonnost, což vyžaduje rychle se zotavit z nouzových situací, které entitu postihnou. Proto v dynamicky proměnném světě používáme kontinuální řízení rizik ve prospěch bezpečnosti a výkonnosti [25,26].



Obr. 4. Rozložení nástrojů řízení rizik ve prospěch bezpečnosti v závislosti na cílech a složitosti entity.



Obr. 5. Interval celkových nákladů, ve kterém je zajištěna bezpečnost; oblast optimálních nákladů je vyznačena modře.

V inženýrských disciplínách sleduje několik druhů resilience (houževnatosti):

- v inženýrství a stavebnictví jde o vytvoření schopnosti budov a infrastruktury absorbovat dopady pohrom a útoky, aniž by došlo k úplnému selhání,
- v energetice jde o jde o vytvoření schopnosti energetických zdrojů a energetických sítí absorbovat dopady pohrom a útoky, aniž by došlo k úplnému selhání,
- v nauce o materiálech jde o jde o vytvoření schopnosti materiálu absorbovat energii při deformaci a uvolnit tuto energii při odstranění zatížení,
- u počítačové sítě jde o jde o vytvoření schopnosti počítačové sítě udržovat službu tváří v tvář poruchám,
- v lidských sídlech jde o jde o vytvoření schopnosti zajistit základní funkce pro obyvatele v minimálním rozsahu, který zajistí přežití lidí,
- v oblasti informační bezpečnosti jde o jde o vytvoření schopnosti kybernetické sítě zajistit základní propojení, která jsou nutná pro základní funkce v lidské společnosti.
- v oblasti řídících systémů jde o jde o vytvoření schopnosti řídicích systémů vytvářet kognitivní, kybernetickofyzickou houževnatost vůči hrozbám.

2.3. Normy pro zajištění bezpečnosti

Na základě velkého důrazu na bezpečnost technických zařízení a technologických objektů vznikla od 90. let minulého století řada norem kodifikující proces zajištění bezpečnosti ve sledované oblasti. Normy ISO 9000 a ISO 31 000, ISO 31010 již byly citovány. Příklady dalších norem jsou 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 v jaderné energetice
ISO/DIS 26262	Funkční bezpečnost v 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.

3. ZÁVĚR

Na základě analýzy konkrétních místních podmínek a konkrétní struktury a složitosti entity jde v České republice o zvažování příčin rizik, kterými jsou:

- živelní pohromy (povodeň, zemětřesení, sesuv podloží, blesk, vichřice, tornádo, požár v území, pád letadla, nadměrné srážky, požár či výbuch v okolí aj.),

- agresivní vnější prostředí,
- selhání či havárie infrastruktur nutných pro provoz entity,
- nevhodné umístění entity,
- chyby v projektu a v konstrukci entity a jejího uložení (např. materiál, ze kterého je entita zhotovena není dostatečně odolný vůči působení přepravovaného média; špatné svary; nevhodná těsnění; nevhodné armatury; nevhodné senzory; špatné podpory entity dovolující průhyby a vibrace, nevhodné senzory nebo špatně umístěné senzory atd.),
- nevhodné nebo neexistující provozní předpisy,
- špatná údržba,
- vnitřní technické problémy: koroze; zanášení propojujících potrubí; extrémní teploty; opotřebovaná těsnění; atd.),
- nedodržení limit pro provoz entity,
- chyby při opravách a modernizacích,
- chyby obsluhy,
- chybné řízení provozu entity,
- nedostatečná dokumentace a chybné řízení bezpečnosti ve všech oblastech,
- nedostatečně stanovené odpovědnosti v provozu entity,
- zanedbání předpisů pro zajištění bezpečnosti,
- nedostatečný dozor veřejné správy,
- hackerský útok
- teroristický útok.

Inženýrství zacílené na bezpečnost [11] při stanovení rizika používá principy:
- riziko je určováno během celého životního cyklu technického díla, tj. během výběru lokality, projektování, výstavby, provozu a vyřazení z provozu, a případně i při uvedení území do původního stavu,
- stanovení rizik se zaměřuje na požadavky uživatelů a úroveň poskytovaných služeb,
- rizika jsou určována podle kritičnosti dopadů na procesy, poskytované služby a aktiva stanovená veřejným zájmem,
- nepřijatelná rizika jsou zmírňována pomocí nástrojů řízení rizik, tj. pomocí technických a organizačních opatření, standardizací provozních postupů nebo automatizovanými kontrolami.

Předmětné inženýrství je z odborného hlediska proces, který vyhledává všechny možné podmínky, které by ohrožovaly úspěšné fungování monitorovaného technického díla ve všech fázích jeho životnosti, a identifikuje možnosti jejich řízení prevencí, připraveností, reakcí a obnovou. Provoz entit má: začleněn systém včasného varování; postupy pro řízení přijatelné úrovně rizik; a postupy pro zvládání abnormálních, nouzových a kritických podmínek během provozu a odstávky. Specifičnost sledovaného řízení rizik spočívá v tom, že se jedná o řízení rizik [16], které hledá optimální řešení pro místně specifické pohromy a přitom se uplatňují zásady předběžné opatrnosti, které zahrnují udržitelný rozvoj.

Respektováním inženýrství zacíleného na permanentní řízení rizik ve prospěch bezpečnosti lze zajistit zvládnutí:
- slabin v zabezpečení entity vůči vnějším vlivům,
- vnitřních náhodných poruch entity,
- vnitřních systémových poruch zařízení,
- poruch v procesech; lidských chyb,
- nedostatku zdrojů,
- konfliktů mezi požadavky na bezpečnost, spolehlivost a zabezpečení,
- chybné nebo nedostatečné identifikace ovlivňujících činitelů,
- chybné práce s riziky (volba metody, definice stupnice, ohodnocení rizika),
- neodpovědnosti manažerů či personálu; nekompetence manažerů či kritického personálu
- a závislosti a nedůvěryhodnosti řešitelských subjektů.

LITERATURA

[1] DHILLON, B.S. *Engineering Safety: Fundamentals, Techniques, and Applications.* ISBN 981-23832-8X. London, UK: World Scientific 2003, 219 p.

[2] MARSHALL, G. *Safety Engineering.* ISBN 978-1885581280. American Society of Safety Engineers 2000, 425 p.

[3] SPELLMAN, F. R. *Safety Engineering: Principles and Practices.* ISBN 086-58797-02. Lanham, MD: Government Institutes 2004, 688 p.

[4] US DOD. *Standard Practice for System Safety*. MIL-STD-822D. Washington, DC: U.S. Department of Defense 2000, 31 p.
[5] US FAA. *System Safety Handbook*. Washington, DC: U.S. Federal Aviation Administration 2000, 506 p.
[6] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů.* ISBN 978-80-01-05771-1. Praha: ČVUT 2015, 208 p.
[7] LACKO, B. Kořenový soubor znalostí inženýrství rizik REBOK australských inženýrů. In: *ExFos 2022*. ISBN 978-80-214-6033-1 Brno: VUT 2022, pp. 338-345.
[8] UN. *Human Development Report*. New York: UN 1994, www.un.org.
[9] EU. Maastricht Treaty (C 191, 29.7.1992, pp.s. 1–112) ve znění pozdějších předpisů
[10] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364 p. Doi:10.14311%2FBK.9788001061824
[11] 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
[12] CLINTON, B. Presidential Decision Directive 63. Washington: White House 1988, 18 p.
[13] 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.
[14] ZAIRI, M. *Total Quality Management for Engineers.* Cambridge: Woodhead Publishing Ltd, 1991.
[15] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OU-HRABKA, 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.9788 001066751
[16] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.
[17] EU. *FOCUS Project*. Brussels: EU 2012, http://www.focusproject.eu/documents /14976/-5d7 63378-1198-4dc9-86ff-c46959712f8a
[18] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. Doi:10.14311%2FBK.9788001066096
[19] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Autho-rities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191 p.
[20] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. Praha: ČVUT 2022, 129 p. Doi:10.14311/BK.978 80010 69950
[21] EPRI. *Guideline on Proactive Maintenance. Technical Report*. Palo Alto: EPRI 2001, 82 p.
[22] EU. *Seveso III Directive (2012/18/ EU).* Brussels: EU 2012.
[23] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessee: US DOE 1996, 180 p.
[24] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369 p.
[25] HOLLNAGEL, E., WOODS, D.D. *Resilience Engineering*. ISBN 978-131560-5685. London: CRC Press 2017, 416 p.
[26] RASMUSSEN, J. Risk Management in a Dynamic Society. *Safety Science*, 27 (1997), 2, pp.183-213.

KVALITA PŘEDÚPRAV NÍZKOUHLÍKOVÉ OCELI A HLINÍKOVÉ SLITINY

QUALITY OF LOW CARBON STEEL AND ALUMINIUM ALLOY PRE-TREATMENTS

Nikol Bachurová, Jan Kudláček

České vysoké učení technické v Praze, Fakulta strojní, Technická 4, Praha 6, Česká republika, nikol.bachurova@fs.cvut.cz

Abstrakt: Článek se zabývá chemickou a mechanickou předúpravou materiálů hliníkové slitiny a nízkouhlíkové oceli. Problematika je poukázána na čistotu materiálů, s níž jsou spojeny aspekty jako drsnost, povrchové napětí. Metoda k odhalení případných ulpělých nečistot je založena na principu fluorescence.

Klíčová slova: Chemická předúprava, rizika, fluorescence, odmašťování, předúpravy.

Abstracts: The article deals with the chemical and mechanical pre-treatment of aluminium alloy and low carbon steel materials. The issue is highlighted on the purity of the materials with which aspects like roughness, surface tension are associated. The method to detect any adhering impurities is based on the principle of fluorescence.

Key words: Chemical pre-treatments, fluorescence, degreasing, pre-treatment.

1. ÚVOD

Celkově předúpravy slouží k dobré přilnavosti povrchu. Z mechanických předúprav bylo použito tryskání [1]. Práce [2,3] uvádí, že tryskání se provádí vrháním tryskacího prostředku velikou rychlostí proti povrchu tryskaného předmětu. Dochází k odstranění rzi, okují a korozních produktů způsobených oxidací. Dle drsnosti povrchu se volí použité abrazivo, záleží na volbě velikosti zrna, hrubosti, tlaku, úhlu či vzdálenosti tryskaného předmětu [2,3] Tryskacím prostředkem může být ocelová drť, různé druhy korundu, křemičitý písek a další [4].

Ve sledovaném případě z chemických předúprav byly použity různé druhy řízené pasivace. V případě řízené pasivace vzniká na povrchu předmětu pasivační vrstva, která je slabá, neviditelná, plní ochranou funkci povrchu kovu a vytváří adhezní vazbu [5]. Vzorky bez úpravy před nanesením pasivační vrstvy byly odmaštěny v ultrazvukové čističce Kraintek [6]. Jejich čistota byla kontrolována zařízením Recognoil QB [11].

2. MOŽNÁ RIZIKA CHEMICKÝCH A MECHANICKÝCH PŘEDÚPRAV

Rizika mechanických předúprav tryskaných vzorků mohou být v částicích ulpělého abraziva na otřískaném povrchu, což může být ovlivněno nevhodně zvoleným tryskacím prostředkem, který ulpěl na povrchu a tím pádem se vytvořila špatná adhezní vrstva mezi povrchem vzorku a následnou povrchovou úpravou [6].

Tryskaný povrch je náchylnější k tvorbě koroze protože k tomu napomáhá část zaseknutého abraziva v povrchu, protože pod ním zůstanou nečistoty [7]. Další nežádoucí faktory tryskacího prostředku, které mohou mít dopady na nedokonale otryskaný povrch jsou dle [2] např.:

- velikost zrna,
- hrubost,
- vzdálenost trysky od tryskaného předmětu,
- volba úhlu, pod kterým se provádí tryskání nebo tlaku, který se používá při tryskán í.

Rizika chemických předúprav tkví v nerovnoměrně nanesené pasivační vrstvě [6]. Další zdroje rizik jsou zbytky neodstraněných okují, oxidů bez nečistot, olejů a jiných mazacích prostředků [8]. Nežádoucím způsobem se projevují také vlivy vnějšího prostředí, proti kterým jsou uvedena opatření, popsaná v práci zváženy v práci [12].

3. EXPERIMENTÁLNÍ ČÁST

V experimentální části se na nízkouhlíkové oceli a hliníkové slitině detekoval kontaminovaný povrch zařízením Recognoil QB citace. U mechanické předúpravy byl vzorek sledován z pohledu čistoty před i po tryskání. Tryskání se provádělo na tlakovém tryskacím zařízení. Abrazivem byl hnědý korund F60. U vzorků byla měřena drsnost, povrchové napětí a čistota povrchu zařízením Recognoil [6].

U chemických předúprav detekce nežádoucích nečistot probíhala před odmaštěním povrchu a po odmaštění s důrazem na čistotu povrchu. Všeobecný postup pasivovaných vzorků byl následující:

- v prvním kroku proběhlo odmaštění vzorků v ultrazvukové čističce Kraintek K-2LE s patřičným čistícím prostředkem za určité teploty a daný čas,
- v druhém kroku se prováděl dvoustupňový oplach v demineralizované vodě,
- třetí krok bylo sušení vzorků horkým vzduchem
- a posledním krokem byla samotná pasivace vzorků.

Tabulky 1 a 2 uvádí přehled použitých vzorků.

Tabulka 1. Přehled použitých vzorků z nízkouhlíkové oceli, bez úpravy před mechanické předúpravy až po chemické předúpravy [6].

Nízkouhlíková ocel			
Bez úpravy	Chemické předúpravy		Mechanické předúpravy
	Fosfátování	Multimetalická předúprava	Tryskání
			

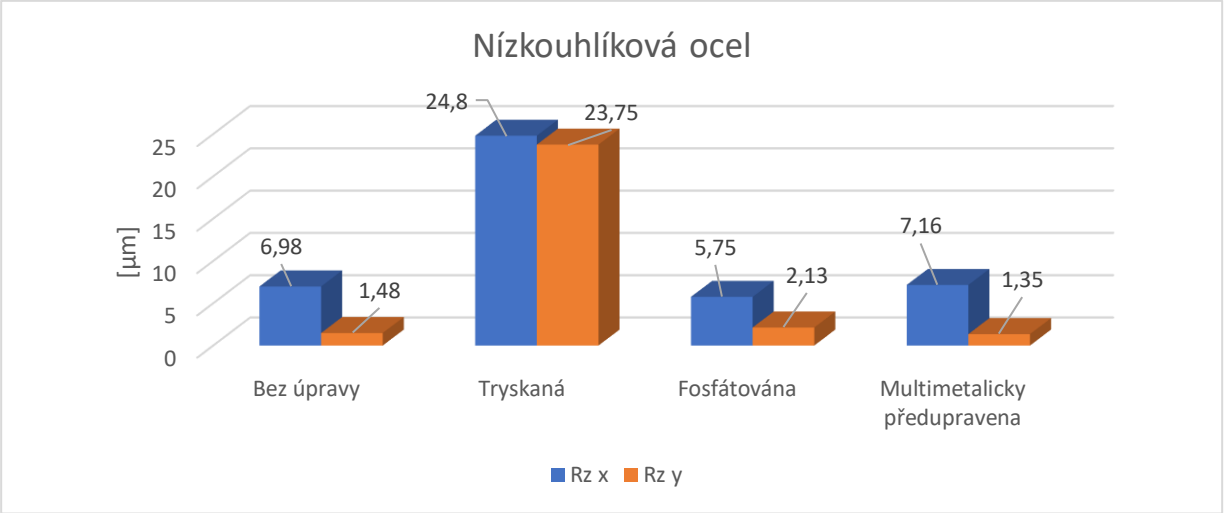
Tabulka 2. Přehled použitých vzorků z hliníkové slitiny, bez úpravy před mechanické předúpravy až po chemické předúpravy [6].

Hliníková slitina				
Bez úpravy	Chemické předúpravy			Mechanické předúpravy
	Fosfátování	Multimetalická předúprava	Předúprava na bázi zirkonia s obsahem Cr^3	Tryskání
				

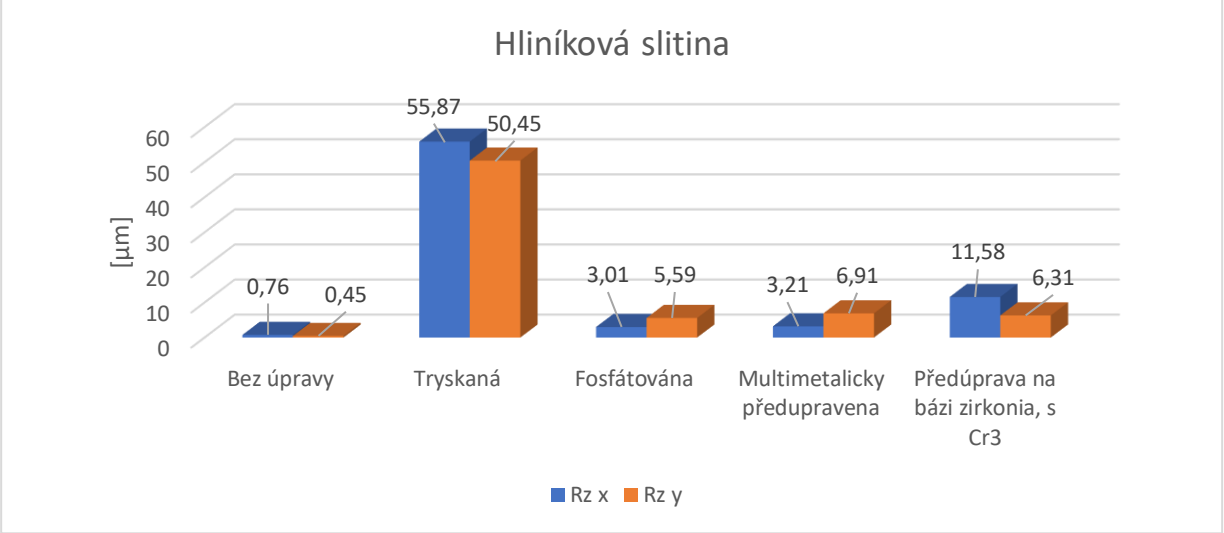
4. POPIS EXPERIMENTŮ A JEJICH VYHODNOCENÍ

Drsnost byla měřena zařízením SURFTEST SJ-210, MITUTOYO ve dvou směrech, a to v ose x a y. Ze srovnání grafů 1 a 2 vyplývá, že nejvyšší naměřená hodnota se objevila u mechanické předúpravy, konkrétně u

tryskané hliníkové slitiny. Nejnižších čísel dosahovala opět hliníková slitina bez úpravy. Pasivace neměla u nízkouhlíkové oceli takový vliv na drsnost jako pasivace u hliníkové slitiny [6].



Graf 1. Drsnost vzorků s/bez předúpravami u nízkouhlíkové oceli [6].



Graf 2. Drsnost vzorků bez/s předúpravami u hliníkové slitiny [6].

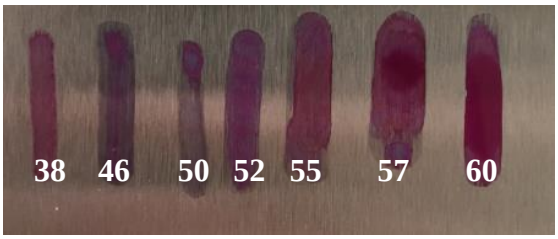
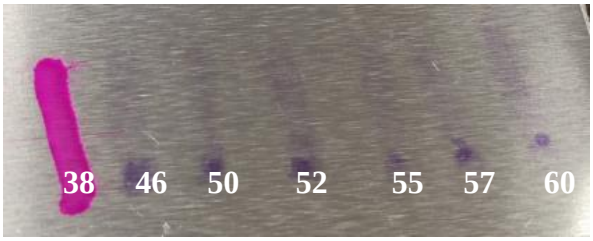
Měření ***povrchového napětí*** stanovovalo čistotu povrchu a pomocí inkoustů se zjišťovaly možné kontaminace povrchu ať z hlediska cizích či chemických nečistot. Hodnoty povrchového napětí byly zvoleny takto:

- 38 $mN.m^{-1}$,
- 46 $mN.m^{-1}$,
- 50 $mN.m^{-1}$,
- 52 $mN.m^{-1}$,
- 55 $mN.m^{-1}$,
- 57 $mN.m^{-1}$
- a 60 $mN.m^{-1}$.

Vzorky bez úpravy byly měřeny před odmaštěním i po odmaštění [9]. Výsledky jsou uvedeny v tabulce 3. Všeobecně lze konstatovat, že povrchové napětí bylo velmi vysoké, což se prokázalo inkousty firmy ArcoTest. Nanesený inkoust na povrchu předmětu vytvářel celistvou, jednolitou a nepřerušovanou vrstvu. Pouze v jediném

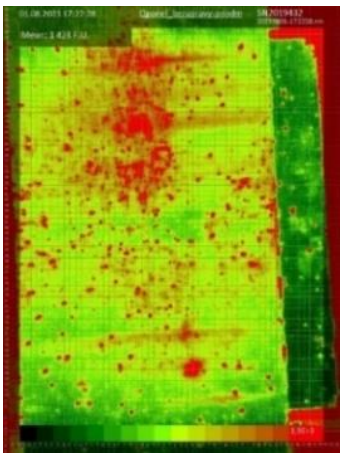
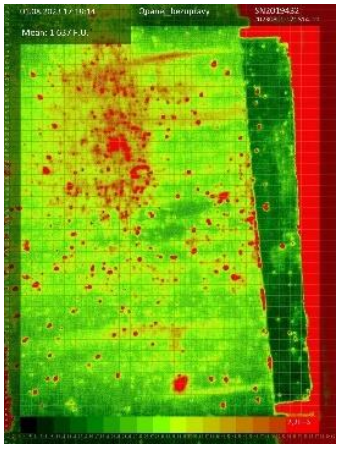
případě došlo k oddělení a vytvoření jednotlivých kapiček, což značilo znečistění povrchu a nedocházelo k dostatečnému smáčení povrchu [6].

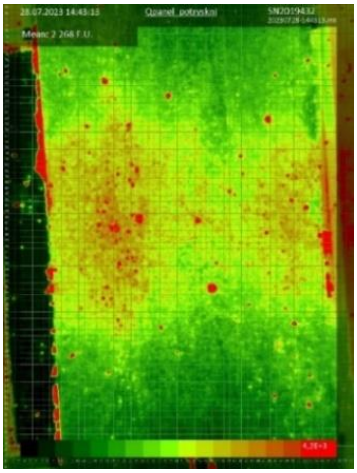
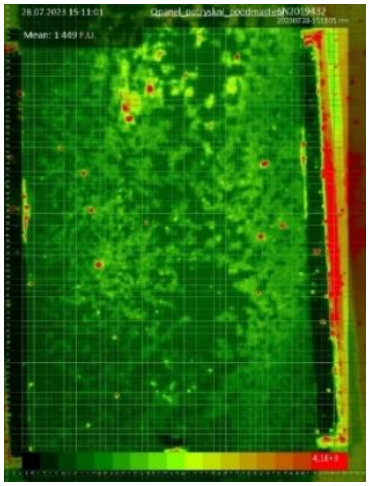
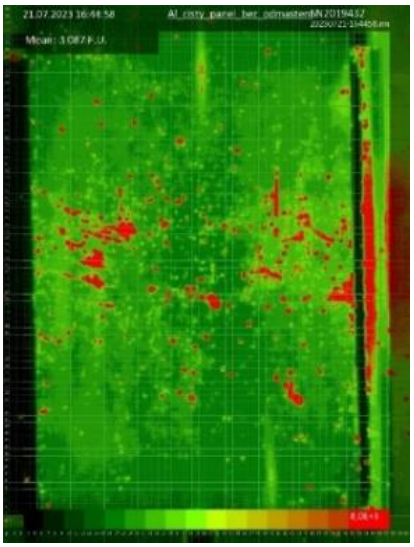
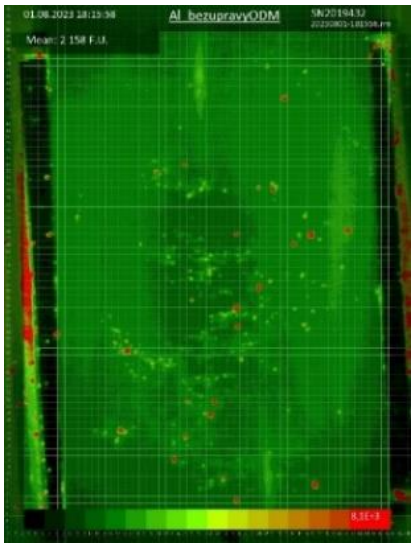
Tabulka 3. Ukázka naneseného inkoustu u vybraných vzorů bez úpravy před/po odmaštění [6].

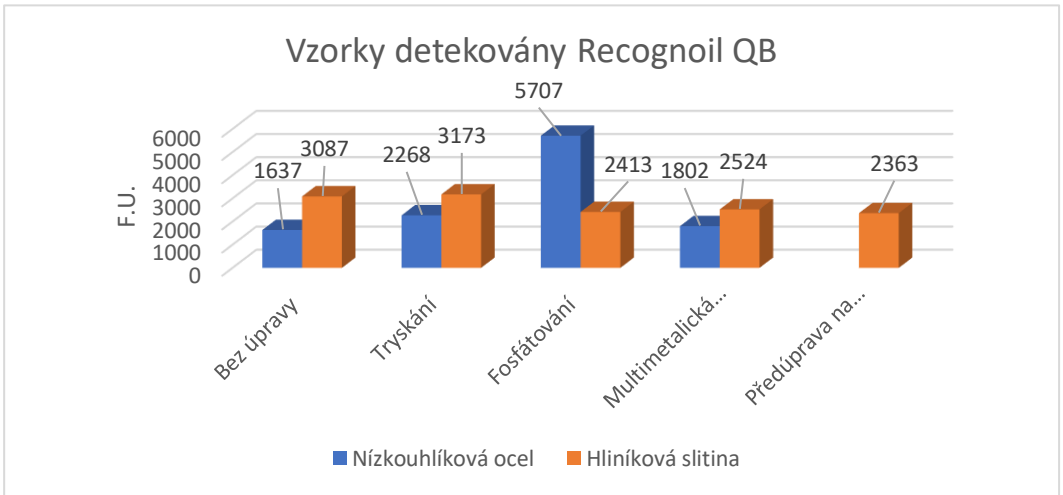
Nízkouhlíková ocel – bez úpravy před odmaštěním	Nízkouhlíková ocel – bez úpravy po odmaštění
	
Hliníková slitina – bez úpravy před odmaštěním	Hliníková slitina – bez úpravy po odmaštění
	

Stanovení fluorescence bylo provedeno Recognoilem QB, což je stolní zařízení sloužící k detekci kontaminovaných předmětů [10]. Výsledkem analyzovaných vzorku jsou fluorescenční mapy, které jsou znázorněny v tabulce 4; jednotky intenzity fluorescence jsou F.U. [11]. Graf 3 ukazuje intenzitu fluuorescence.

Tabulka 4. Ukázka vybraných vzorků před odmaštěním a po odmaštění pomocí Recognoilu QB [6].

Recognoil QB	
Nízkouhlíková ocel – bez úpravy před odmaštěním	Nízkouhlíková ocel – bez úpravy po odmaštění
	
Nízkouhlíková ocel – po otryskání	Nízkouhlíková ocel – po otryskání a odmaštění

	
Hliníková slitina – Před odmaštěním	Hliníková slitina – po odmaštění
	



Graf 3. Vzorky jednotlivých materiálů měřeny zařízením Recognoil QB [6]

Vyhodnocení grafu 3 ukazuje, že nejvyšší hodnota intenzity fluorescence byla naměřena u nízkouhlíkové oceli s předúpravou fosfátování a u tytéž předúpravy u hliníkové slitiny klesla jednotka F.U. o dvojnásobek.

Zajímavý poznatek přináší pasivační vrstvy na hliníkové slitině, kdy jednotka intenzity fluorescence klesá v řádů stovek F.U. oproti vzorku bez úpravy. Vzorky, které byly mechanicky před upraveny vždy na fluorescenční mapě svou hodnotu zvýšily při srovnání se vzorky bez předúpravy - u nízkouhlíkové oceli je rozdíl cca 600 F.U. a u hliníkové slitiny je rozdíl nepatrný [6].

5. ZÁVĚR

Zkoumaná problematika kvality předúprav hliníkové slitiny a nízkouhlíkové oceli byla zhodnocena následovně:

1. Při porovnání vzorků bez úpravy vykazovala nejvyšší hodnotu intenzity fluorescence hliníková slitina.
2. U tryskaných vzorků vykazovala hodnota F.U. vyšší stupeň znečištění u tryskané hliníkové slitiny.
3. Provedená pasivace ovlivnila jednotku intenzity fluorescence porovnaných vzorků bez úpravy. U nízkouhlíkové oceli se F.U. zvyšovala, naproti tomu u hliníkové slitiny se snižovala ve všech třech případech.
4. U vzorků, které nebyly pasivovány a byly hodnoceny i po odmaštění v ultrazvukové čističce, jednotka F.U. klesala ve všech případech. To znamená, že lázně, které byly v ultrazvukové čističce, byly bez kontaminace cizích látek, a proto tomu mohla být zajištěna souvislá pasivační vrstva, která nevykazovala nadměrné znečištění. Tento úsudek potvrdilo i vysoké povrchové napětí, které vycházelo až na výjimku u všech vzorků velmi vysoké [6].

Práce [12] ukázala, že pro sestavení postupu pro praxi je nutné používat specifický postup, který zohledňuje zásady řízení bezpečnosti procesu, které zajišťují kvalitu na požadované úrovni.

Poděkování: Článek byl podpořen projektem SGS22/156/OHK2/3T/12 (Vliv povrchových úprav na kvalitu výrobních technologií).

LITERATURA

[1] TULKA, J. *Povrchové úpravy materiálů*. ISBN 80-214-3062-1.Brno: Vysoké učení technické v Brně, Fakulta chemická, 2005, 136 p.
[2] KUBÁTOVÁ, H. *Nátěry kovů*. ISBN 80-247-9035-1. Praha: Grada, 2000. Profi & hobby.
[3] JIAOJIAO LI, AN DU, YONGZHE FAN, XUE ZHAO, RUINA MA, JIANJUN WU. Effect of Shot-Blasting Pretreatment on Microstructures of Hot-Dip Galvanized Coating. *Surface and Coatings Technology*, ISSN 0257-8972. 364 (2019), pp. 218-224. Doi:10.1016/j.surfcoat.2019.02.075.
[4] PKIT. *Pískovací materiály*. https://www.pkit.cz/piskovaci-materialy/1/
[5] INFOCUBE. *Pasivace*. https://www.oneindustry.cz/lexikon/pasivace/
[6] BACHUROVÁ, N. Hodnocení čistoty povrchu u definovaných materiálů a povrchových úprav. *Diplomová práce.* Praha: České vysoké učení technické v Praze 2023..
[7] KALNÝ, P. *Moření a pasivace jako konečná povrchová úprava legovaných antikorozních ocelí*. https://www.fksystem.cz/blog/clanek-o-moreni-a-pasivaci
[8] EURO INOX. Moření a pasivace korozivzdorných ocelí. ISBN 978-2-87997-139-1. https:// www.worldstainless.org/Files/issf/non-image-files/PDF/Euro_Inox/Passivating_Pickling_CZ.pdf
[9] PROINEX INSTRUMENTS, s.r.o. *Testovací inkousty pro testování povrchové energie/ povrchového napětí.* https://www.proinex.cz
[10] TECHTEST. *Recognoil QB Laboratorní přístroj pro kontrolu plošné kontaminace.* https://www.techtest.eu/download/RecognoilQB%20-%20Informa%C4%8Dn%C3%AD%20bro%C5% BEura.pdf
[11] TECHTEST. Katalog z firmy TechTest s.r.o. www.techtest.cz
[12] KUCHAR, J., KREIBICH, V., PROCHAZKOVA, D., BACHUROVA, N. Mitigating the Risks of Energetic Facilities by Cleaning Internal Surfaces. . ISBN-13: 978-981-18-8071-1. Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023). Singapore: Research Publishing 2023, pp. 1113-1121. Doi: 10.3850/978-981-18-8071-1_driver

REAKTORY SMR PRO ČESKOU REPUBLIKU

SMALL MODULAR REACTORS FOR THE CZECH REPUBLIC

Michal Cihlář[1, 2], Dana Procházková[1], Alžběta Endrychová[1, 3], Matyáš Junek[1], Jan Komrska[1, 4], Vojtěch Smolík[1], Jakub Špaček[1, 5], Václav Dostál[1]

[1]*Ústav energetiky, FS ČVUT v Praze, Technická 4, 160 00 Praha 6 Dejvice, Česká republika, michal.cihlar@fs.cvut.cz*
[2] *Zpracování a ukládání nebezpečných odpadů, Centrum výzkumu Řež, Hlavní 130, Řež, 250 68 Husinec, Česká republika,*
[3]*UJP Praha, Nad Kamínkou 1345, 156 00 Zbraslav, Česká republika,*
[4]*ÚJV Řež, Hlavní 130, Řež, 250 68 Husinec, Česká republika,*
[5]*Státní ústav radiační ochrany, Bartoškova 1450/28, 140 00 Praha 4 Nusle, Česká republika*

Abstrakt: Malé modulární reaktory (SMR) jsou trendem posledních let a jednou z možných cest pro jadernou renesanci. V České republice plánuje společnost ČEZ výstavbu prvního SMR v lokalitě Temelín. Mezi uvažované návrhy reaktorů patří AP300 (Westinghouse), BWRx-300 (GE-Hitachi), NuScale (NuScale), Nuward (CEA, EDF, Naval Group a Technicatome), SMART 100 (KAERI a KEPCO E&C), SMR-160 (Holtec) a UK-SMR (Rolls-Royce). Důležitým krokem k úspěšnému řešení plánu je volba vhodného návrhu. Jednou z metod hodnocení, která přispěje ke kvalitnímu rozhodnutí, které povede k jaderné i celkové bezpečnosti objektu a jeho okolí je metoda multikriteriální. V článku uvádíme položky, které je třeba zvážit a navrhujeme další postup v aplikaci multikriteriální metody.

Klíčová slova: SMR, malý modulární reaktor, bezpečnost, multikriteriální hodnocení.

***Abstract*:** Small modular reactors (SMRs) are a trend of recent years and one of the possible paths for a nuclear renaissance. In the Czech Republic, CEZ plans to build the first SMR at Temelín. The reactor designs under consideration include AP300 (Westinghouse), BWRx-300 (GE-Hitachi), NuScale (NuScale), Nuward (CEA, EDF, Naval Group and Technicatome), SMART 100 (KAERI and KEPCO E&C), SMR-160 (Holtec) and UK-SMR (Rolls-Royce). An important step towards successful plan realization is the choice of the appropriate design. One method of evaluation that contributes to quality decision, which will result in nuclear and integral safety of object and its surrounding is the multi-criteria method. In article, we show items, which would be considered and propose the further procedure at multicriteria method application.

***Key words*:** SMR, small modular reactor, safety, multicriteria evaluation.

1. ÚVOD

Malé modulární reaktory (SMR) jsou trendem posledních let a jednou z možných cest pro jadernou renesanci. Mezinárodní agentura pro atomovou energii definuje objekty se SMR jako "malé" elektrárny s výkonem do 300 MWe a jako "střední" elektrárny s výkonem do 700 MWe. Společně je označuje jako malé a střední reaktory (SMR). Termín "SMR" se však častěji používá jako zkratka pro "malý modulární reaktor", který je určen k sériové výstavbě a společně tvoří velkou jadernou elektrárnu.

V tomto příspěvku je v následujících kapitolách popsáno sedm vybraných návrhů reaktorů kategorie SMR, dle spolupráce ČEZ 0. Mezi těchto sedm vybraných návrhů patří tyto:

- AP300 od americké společnosti Westinghouse Electric Company LLC,
- BWRx-300 od americké společnosti GE-Hitachi, resp. Hitachi GE Nuclear Energy,
- NuScale od stejnojmenné americké společnosti,
- Nuward od francouzského konsorcia CEA, EDF, Naval Group a Technicatome,
- SMART 100 od jihokorejské skupiny KAERI a KEPCO E&C,
- SMR-160 od americké společnosti Holtec a
- UK-SMR od britské společnosti Rolls-Royce

Přehled typů, tepelných a elektrických výkonů, tlaku v I.O., teplot na vstupu a výstupu z AZ, použitého moderátoru a chladiva a délka palivové kampaně pro všech sedm vybraných SMR je uveden v tabulceTabulka 5. V poslední kapitole je navržen možný postup výběru vhodného reaktoru na základě multikriteriální metody.

Tabulka 5. Přehled základních informací o vybraných návrzích reaktorů SMR.

Název	**Typ**	**Výkon**	**Výkon**	**Tlak I.O.**	**Vstupní/výstupní teplota AZ**	**Chladivo/ moderátor**	**Palivová kampaň**
-	**-**	**MWt**	**MWe**	**MPa**	**°C/°C**	**-**	**Měsíců**
AP300	PWR	900	300	(15,5)[1]	(279/325)[1]	Lehká voda	(18) [1]
BWRx-300	BWR	870	270 – 290	7,2	270/288	Lehká voda	12-24
NuScale	PWR	160[2]	50[2]	12,75	258/283	Lehká voda	24
Nuward	PWR	540[3]	170[3]	15	280/307	Lehká voda	24
SMART 100	PWR	365	107	15	296/322	Lehká voda	30
SMR-160	PWR	525	160	15,5	243/321	Lehká voda	24
UK-SMR	PWR	1358	470	15,5	295/325	Lehká voda	18-24

2. SOUHRN POZNATKŮ O ZVAŽOVANÝCH SMR

Pro zajištění dobrého výběru typu SMR pro Českou republiku je dále shromážděn souhrn dostupných poznatků.

2.1. AP300 – Westinghouse, USA

Reaktor AP300 0 (obrázek 1) od firmy Westinghouse Electric Company LLC byl veřejnosti představen před několika měsíci0. Jedná se o jednosmyčkový lehkovodní, tlakovodní reaktor s výkonem 900 MWt. Bude využívat pasivní systém kontejnmentu, systém chlazení aktivní zóny a celkový inženýrský přístup přejatý z reaktoru AP10000.

Podle dostupných informací by se mělo jednat v podstatě jen o „reaktor AP1000 bez jednoho parogenerátoru“. Odstranění jednoho parogenerátoru může mít za následek odlišnou fenomenologii rozvoje některých událostí v porovnání s původním návrhem AP1000 [3. Nicméně, historické dobré zkušenosti s návrhem a provozem jednosmyčkových energetických reaktorů existují.

Obr. 1. Vizualizace reaktoru AP300 0.

Není známo, zda bude AP300 (Obr. 1) využívat reaktorovou nádobu AP1000 s upravenou vnitřní částí, modifikovanou nádobu, nebo zcela odlišnou nádobu.

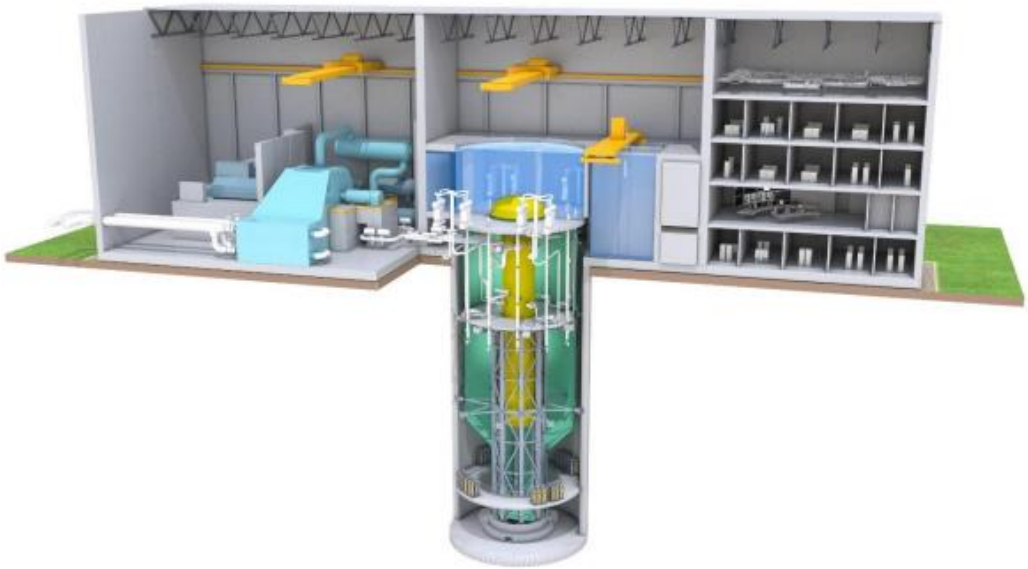
Jedna pravděpodobná změna oproti AP1000 je to, že kompenzátor objemu je umístěn na vlastní smyčce a není napojen na smyčku parogenerátoru 0. Velmi pravděpodobně bude reaktor AP300 obsahovat zásobník vody pro výměnu paliva v kontejnmentu IRWST, který je typickým prvkem designu reaktoru AP1000. Zásobník vody IRWST funguje jako jímač tepla pro pasivní systém odvodu zbytkového tepla, poskytuje vodu pro nízkotlaké nouzové chlazení aktivní zóny, slouží jako jímač tepla pro první tři stupně pokročilého systému odtlakování a v případu těžké havárie zajišťuje chlazení trosek díky sběru kondenzované vody z kontejnmentu.

Při návrhu reaktoru a celé elektrárny AP1000 byl kladen důraz na jednoduchost. Proběhlo zjednodušení všech bezpečnostních systémů, běžných provozních systémů, blokové dozorny, postupů výstavby a systémů kontroly a řízení. Zjednodušení přináší méně komponentů, kabelů a betonu, což dále vede ke snížení počtu seizmicky odolných stavebních objektů. AP300 pokračuje v této filozofii a zdá se, že topologie elektrárny bude velmi podobná.

Společnost Westinghouse očekává získání „design certification“ v roce 2027. Používáním technologií z projektu AP1000 Westinghouse předpokládá, že se vyhne problémům s first-of-a-kind (FOAK) citace realizací. Dalším očekávaným benefitem velké podobnosti s AP1000 by měla být nižší cena 0.

2.2. BWRx-300 – GE Hitachi, USA

Malý modulární reaktor BWRx-300 (obrázek 2) je projektem společnosti General Electric Hitachi Nuclear Energy (dále jen GE). Jedná se o lehkovodní varný reaktor s výkonem 300 MWe. Výrobce citace uvádí ~~(GE, 2023)~~, že BWRx-300 bude založen na přirozené cirkulaci chladiva v reaktoru a nebude se v okruhu tedy nacházet hlavní cirkulační čerpadlo ani parogenerátory 0.



Obr. 2. Ilustrační obrázek elektrárny s reaktorem BWRx-300 0.

Systém distribuce páry (NSSS) vede páru z tlakové nádoby na turbínu a kondenzát zpět do tlakové nádoby. Tento systém vychází z reaktoru ABWR [7] a ESBWR [7]. V aktivní zóně se nachází palivo GNF2 [8], které je používané v současných varných reaktorech. Palivová kazeta je čtvercová mřížka 10x10 se 78 normálními palivovými proutky, 14 zkrácenými palivovými proutky a se 2 centrálními tyčemi pro vodu 0. Regulace reaktivity probíhá pomocí vyhořívajících absorbátorů a regulačních tyčí. Regulační tyče mají 2 typy pohonu. Motor posouvá tyče při normálním provozu reaktoru a rychlý hydraulický pohon slouží k rychlému odstavení reaktoru.

Tlaková nádoba je svařená z několika prstenců a je ze shora zakončena eliptickým krytem. Uvnitř tlakové nádoby se nachází aktivní zóna s palivovými soubory a regulačními tyčemi, mechanická podpora AZ a paliva, podpůrné konstrukce, vodič páry, separátor páry a sušič páry 0.

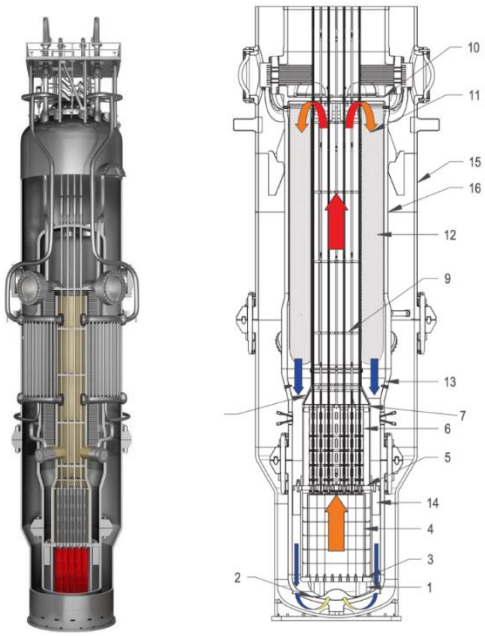
Základní filozofie bezpečnosti BWRx-300 je založena na inherentní bezpečnosti a pasivních bezpečnostních systémech. Odvod tepla v nehavarijních stavech (např. při odstavování reaktoru) je zajištěn dvěma redundantními tepelnými výměníky s čerpadly. Havarijní chlazení zajišťuje izolační kondenzátor se čtyřmi nezávislými větvemi a tepelnými výměníky. Další systém havarijního chlazení je chlazení kontejnmentu pomocí několika smyček s výměníky. Bazény pro vyhořelé palivo jsou chlazeny tepelnými výměníky. Zbytkové teplo by mělo být odváděno bez vnějšího zásahu po dobu nejméně 7 dní. Kontejnment je suchý, válcový s průměrem 16 m a výškou 44 m. Je integrovaný do budovy elektrárny a je téměř celý pod úrovní terénu 0.

V souvislosti s BWRx-300 GE uzavřelo memorandum o porozumění, či jiné smlouvy s několika státy. Patří mezi ně i Česká republika, USA, Kanada, UK, Polsko a Estonsko [10]. V roce 2024 se podle plánů má začít budovat první BWRx-300, a to v Darlingotonu v Kanadě [10]. Reaktor má být spuštěn v roce 2028. Ve Spojených státech amerických bude vybudován BWRx-300 v lokalitě Clinch River. Místní společnost Tennessee Valley Authority nyní usiluje o získání licence pro BWRx-300 od amerického regulačního úřadu. Podání žádosti je naplánováno na začátek roku 2024 00.

Předpokládá se, že náklady na projekt BWRX-300 budou činit maximálně 1 miliardu USD [11]. Po získání zkušeností z prvních jednotek by měly náklady klesnout na cca 2 250 USD/kW. Hlavním cílem projektu BWRX-300 je dosažení konkurenceschopné sdružené ceny energie (LCOE). Toho se má docílit minimalizací potřebných nákladů na personál, provoz, údržbu a počátečních nákladů. Tato opatření by měla vést k dosažení LCOE 35 až 50 USD/MWh v závislosti na řadě faktorů včetně nákladů na financování. GE [11] dále uvádí, že díky jednoduchosti, modularitě a pasivním systémům bude mít BWRx-300 až o 40 % menší počáteční náklady než ostatní tlakovodní SMR 0.

2.3. NuScale – NuScale, USA

Modulární reaktor NuScale (Nuscale Power Module) je integrální tlakovodní reaktor (PWR) s jmenovitým elektrickým výkonem 77 MW(e), resp. tepelným výkonem 250 MW(t), obrázek 3. Koncept NuScale spočívá v umístění několika (4, 6 nebo 12) reaktorů v jedné lokalitě s využitím společných systémů (turbína, generátor) mezi jednotlivými reaktory, tyto elektrárny se nazývají VOYGR. Mezi hlavní charakteristiky návrhu reaktoru NuScale patří kromě integrální konstrukce také využití přirozené cirkulace primárního chladiva reaktoru. Z důvodů zajištění bezpečnosti je kompaktní tlaková nádoba reaktoru za provozu zcela ponořena do vody. Průběh havarijního chlazení je projektován na odvod tepla do vody v okolí reaktoru 00.



Obr. 3. Řez reaktorem NuScale a schéma přirozené cirkulace I.O.0.

Integrální konstrukce umožňuje umístění reaktoru, parogenerátoru i kompenzátoru objemu do reaktorové nádoby. Parogenerátory se skládají z trubiček šroubovicového tvaru, který umožňuje dostatečný přestup tepla i při nízkých rychlostech proudění chladiva přirozené cirkulace. Reaktor NuScale využívá keramické palivo UO2 s obohacením až 4,95 %, aktivní zóna se skládá ze 37 palivových souborů (17x17 palivových proutků). Návrh umožňuje také využití MOX paliva.

Návrh NuScale klade důraz na zajištění stabilního a dlouhodobého chlazení aktivní zóny a kontejnmentu v situaci úplného výpadku elektrického napájení. Elektrárna se může skládat z až 12 reaktorových modulů. Za běžného provozu jsou reaktory ponořeny do vodou naplněného betonového bazénu obloženého nerezovou ocelí, který je uložen pod zemí. Bazén je navržen s ohledem na seismickou odolnost a zároveň je škálován tak, aby zajistil 30denní chlazení aktivní zóny a kontejnmentu bez nutnosti doplnění další vody. Po 30 dnech je produkce zbytkového tepla aktivní zóny tak malá, že přirozený konvekční přenos tepla do vzduchu na vnějším povrchu kontejnmentu spolu s tepelným vyzařováním zcela postačují k odvádění zbytkového tepla aktivní zóny po neomezenou dobu. Tyto pasivní bezpečnostní systémy mohou plnit svou funkci, aniž by vyžadovaly externí dodávku vody nebo elektrické energie 0,15].

Testování a hodnocení bezpečnostních systémů elektrárny NuScale, včetně výpočetních a experimentálních hodnocení pasivních bezpečnostních systémů, probíhá na několika institucích. Jedním z příkladů je experimentální model reaktoru NuScale v měřítku 1:3 zkonstruovaný na Oregons State University [16]. Tento experiment potvrdil schopnost dostatečného odvodu tepla pasivními systémy. Oregons State University je také místem, kde byl započat vývoj konceptu reaktoru NuScale 0,0.

V současné době je reaktor NuScale v pokročilém stádiu certifikace USNRC [16]. Dostupné jsou tak dokumenty popisující jednotlivé aspekty návrhu NuScale včetně revizí z předešlých let, ze kterých je znatelný postupný vývoj návrhu.

2.4. Nuward – CEA, EDF, Naval Group a Technicatome, Francie

Nuward („NUclear forWARD“) je francouzská koncepce SMR od firmy EDF (obrázek 4) s předpokládanou dobou výstavby kolem roku 2030 [18]. První referenční elektrárna je plánována jako dvou-modulová s čistým elektrickým výkonem 340 MWe (tj. 170 MWe na modul). Doba výstavby by měla trvat 36 měsíců (od první betonáže po dosažení kritičnosti) 0, 0.

Obr. 4. Reaktorový modul elektrárny Nuward 0.

Ve sledovaném případě se jedná o SMR GEN 3+ typu PWR s plnou integrací hlavních komponent v tlakové nádobě reaktoru [7]. Tlaková nádoba s hlavními komponenty je ponořena do velkého objemu vody, aby bylo zajištěno pasivní chlazení v případě nehody. Projekt Nuward zahrnuje pasivní bezpečnostní systémy, které zaručují zvládnutí DBC (Design Basic Condition) bez jakéhokoliv vnějšího zásahu po dobu 3 dnů.

Projekt Nuward využívá konstrukci palivového souboru 17x17 se zkrácenou výškou aktivní zóny a tyčemi z UO2 obohacenými na méně než 5 hm. % 235U [7]. Bezborová koncepce reaktoru umožňuje použití různých obohacení

235U a vyhořívajících absorbátorů. Předpokládaný interval doplňování paliva do reaktoru Nuward je 24 měsíců 0.

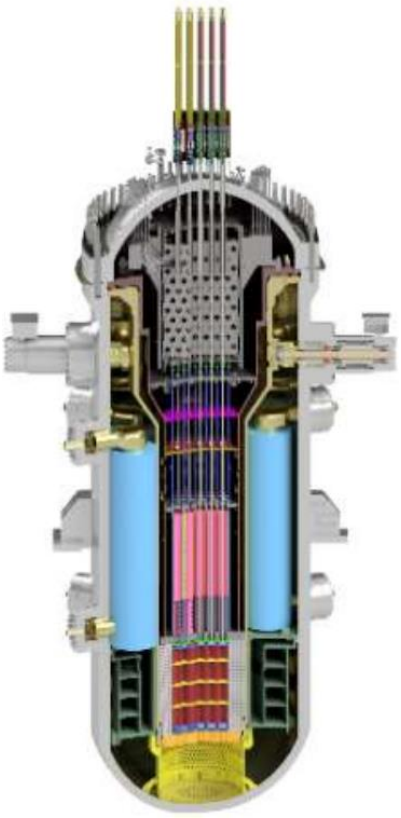
Aktivní zóna reaktoru, mechanismy pohonu regulačních tyčí, parogenerátory a kompenzátor objemu jsou integrovány do tlakové nádoby reaktoru. Cirkulace v reaktoru je nucená pomocí šesti čerpadel horizontálně namontovaných na TNR a umístěných pod parogenerátory na studené větvi. Projekt byl odstartován v září 2019 francouzskou Komisí pro alternativní energie a atomovou energii (CEA – Commissariat à l'énergie Atomique et aux Énergies Alternatives), společnostmi EDF, Naval Group a TechnicAtome [7].

NUWARD je od roku 2021 zapojen do prvního evropského předlicenčního procesu pod vedením francouzského úřadu pro jadernou bezpečnost (ASN) společně s ČR (SÚJB) a Finska (STUK). V červnu 2023 francouzská společnost Nuward předložila francouzskému jadernému dozoru ASN dokumentaci o bezpečnostních variantách, čímž byl zahájen předlicenční proces pro tuto elektrárnu 0.

2.5. SMART 100 – KAERI a KEPCO, Jižní Korea

Systémově integrovaný modulární pokročilý reaktor SMART je integrální tlakovodní reaktor s jmenovitým elektrickým výkonem 110 MW(e), resp. Tepelným výkonem 365 MW(t) [7]. Reaktor SMART využívá pokročilé konstrukční prvky pro zvýšení bezpečnosti, spolehlivosti a hospodárnosti. Reaktor SMART byl navržen Korea Atomic Energy Research Institute (KAERI) pro výrobu elektrické energie, odsolování mořské vody a případné další průmyslové aplikace 0,0.

Reaktor SMART (obrázek 5) využívá integrovaný primární systém, modularizaci a pokročilé pasivní bezpečnostní systémy pro zlepšení bezpečnosti, spolehlivosti a ekonomiky. Bezpečnost SMART je zajištěna přijetím pasivních bezpečnostních systémů spolu s funkcemi pro zmírnění vážných nehod. Zlepšení ekonomiky je dosaženo zjednodušením systému, potenciální sériovou výrobou, zkrácením doby výstavby a vysokým koeficientem využití.0. Reaktor SMART využívá integrovanou koncepci a jeho primární okruh se skládá z aktivní zóny reaktoru, 8 parogenerátorů, 4 zapouzdřených čerpadel I.O., 25 mechanismů pohonu regulačních tyčí a vnitřních částí reaktoru. Proudění chladiva I.O. je za normálního provozu založeno na nucené cirkulaci čerpadel chladiva reaktoru. Systém má schopnost přirozené cirkulace pro použití v abnormálních podmínkách [21].



Obr. 5. Řez reaktorem SMART 100 0.

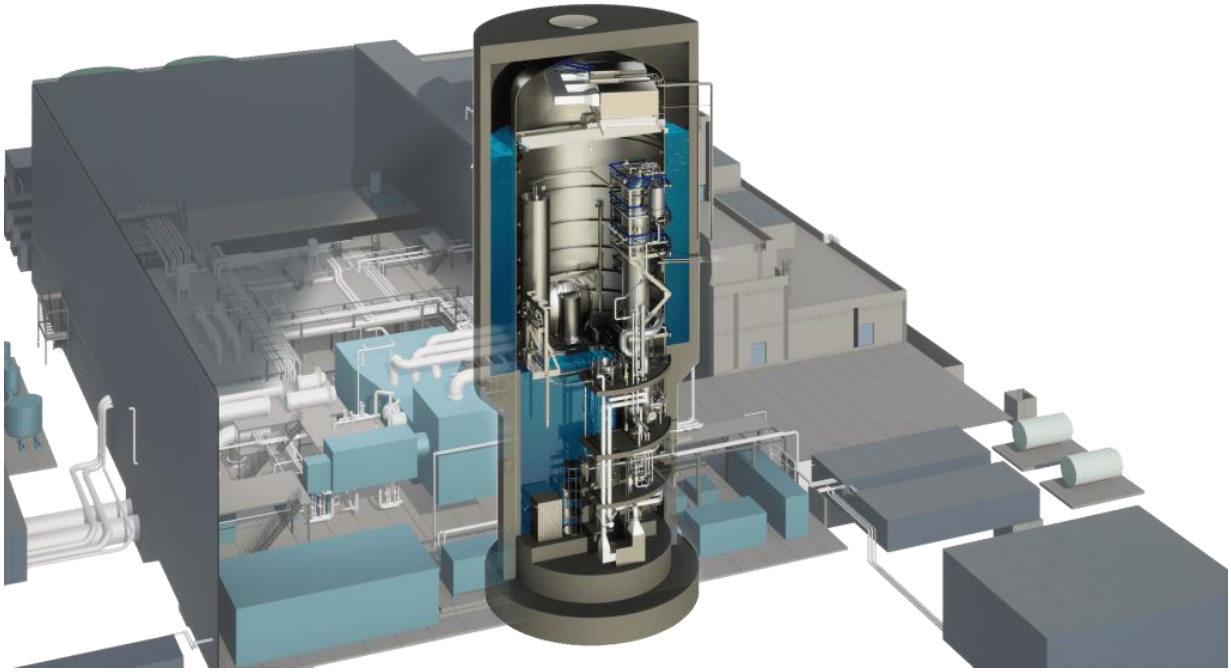
Aktivní zóna reaktoru SMART má relativně nízkou hustotou výkonu zajišťující vysokou tepelnou rezervu [7]. Reaktor používá běžné tlakovodní palivo, tj. keramické pelety UO2 obohacené na méně než 5 % uspořádané do čtvercových palivových souborů 17x17. Aktivní zónu tvoří 57 těchto palivových soborů s délkou přibližně 2 m. Kompenzátor objemu je integrovaný a představuje ho volný objem v horní vnitřní části TNR. Reaktor SMART využívá osm parních generátorů průtočného typu se spirálovitě stočenými trubkami. PG jsou umístěny na obvodovém okraji mezi nosným válcem vnitřní části reaktoru a TNR. Bezpečnostní systémy SMART jsou navrženy tak, aby fungovaly automaticky. Systém odvodu zbytkového tepla zajišťuje svou funkci po dobu 72 hodin bez jakéhokoli nápravného opatření ze strany operátorů pro postulované projektové havárie [22].

Na začátku tohoto tisíciletí, Jižní Korea započala výzkum a vývoj reaktoru SMART jako národní projekt pro komercializaci. V březnu 2015 byla podepsána dohoda mezi KAERI a Saudskoarabskou KA-CARE pro budoucí stavbu reaktoru SMART [23]. V prosinci 2018 KEPCO E&C dokončilo design SMART100 využívající pasivní systémy. V dubnu 2021 KHNP oznámila, že ve spolupráci s KAERI navrhují nový design reaktoru SMART s vylepšenou ekonomikou. Jejich cílem je získat licenci do roku 2028. V současné době KEPCO E&C zaměřuje své síly na získání SDA pro design SMART100.

2.6. SMR-160 – Holtec, USA

Reaktor SMR-160 vyvíjí společnost Holtec International jako pokročilý malý modulární reaktor PWR s tepelným výkonem 525 MW a čistým elektrickým výkonem 160 MW. Konstrukce elektrárny zahrnuje pasivní bezpečnostní systémy. V souladu s konstrukční filozofií společnosti Holtec je reaktor SMR-160 navržen pro zvládnutí projektových havárií a bezpečné odvedení zbytkového tepla z radioaktivního rozpadu bez nutného zásahu obsluhy. Modulární plán výstavby SMR-160 zahrnuje výrobu a montáž největších přepravitelných komponent před příjezdem na místo 0.

Primárním plánovaným využitím SMR-160 (obrázek 6) je výroba elektřiny s volitelným kogeneračním zařízením (tj. výroba vodíku, skladování tepelné energie, dálkové vytápění, odsolování mořské vody apod.). Konstrukce umožňuje umístění v lokalitách s nedostatkem vody s využitím patentované technologie vzduchem chlazeného kondenzátoru. Zařízení SMR-160 je schopné izolovaného provozu, což z něj činí ideální zařízení pro destinace s nestabilními energetickými sítěmi 0.



Obr. 6. Elektrárna s reaktorem SMR-160 0.

Naplnění filozofie ochrany do hloubky je dosaženo tím, že do systému I.O. jsou zahrnuty pasivní bezpečnostní chladicí systémy a aktivní nezabezpečené systémy, přičemž všechny kritické komponenty jsou instalovány pod

úrovní terénu a chráněny robustní konstrukcí ochranného krytu [24]. Elektrárna je navržena tak, aby byla bezpečná při odchodu, s malým bazénem vyhořelého paliva v kontejnmentu a malým zdrojovým členem, což vede k řádovému zvýšení bezpečnosti, např. v CDF, ve srovnání s elektrárnami současné generace, bez závislosti na činnosti obsluhy.

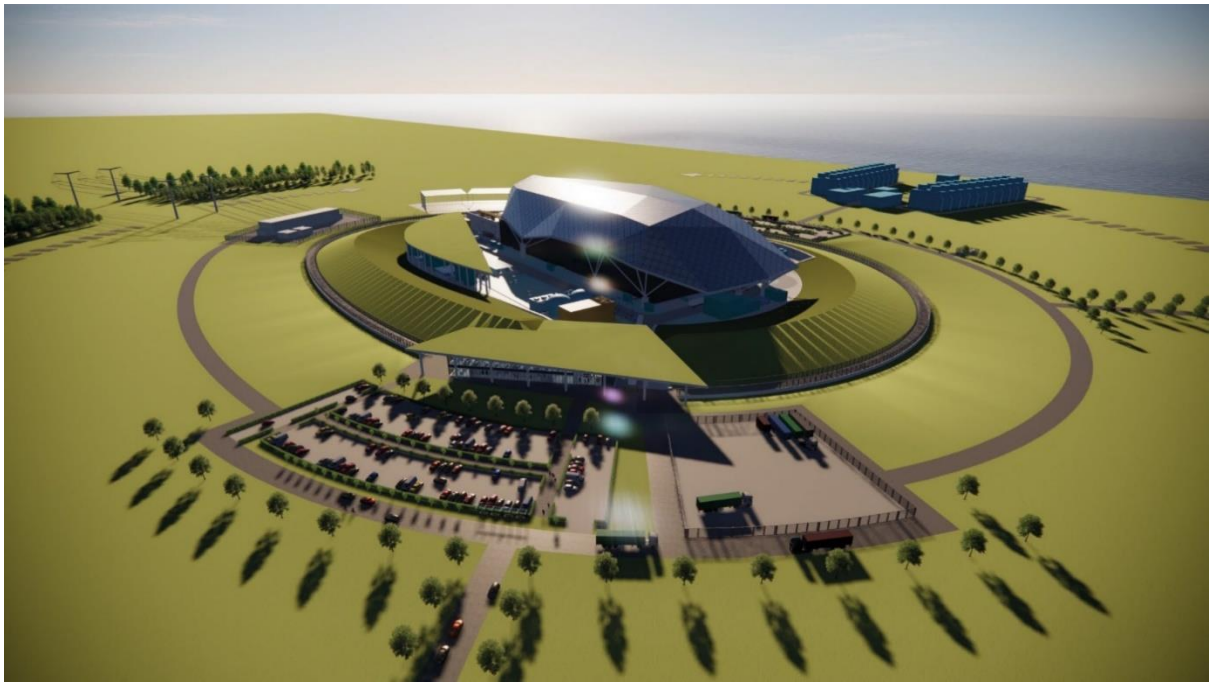
V roce 2012 byly zahájeny práce na koncepčním návrhu reaktoru SMR-160. Ty byly dokončeny v roce 2015. V roce 2020 pak byl dokončen předběžný projekt. Na rok 2023 bylo plánováno, že bude projekt reaktoru SMR-160 připraven ke komercionalizaci pomocí procesu založeném na stavebním povolení. Zároveň byla dokončena fáze 1 posuzování návrhu kanadskou CNSC 0, 0.

Souběžně s rozvojem komerčních možností projektu byly zahájeny předběžné předaplikační činnosti pro posouzení SMR-160 u několika mezinárodních regulačních orgánů. Formální předaplikační činnosti, předkládání žádostí a přezkumy jsou prováděny s USNRC v souladu s dohodnutým plánem zapojení regulačních orgánů [26].

2.7. UK-SMR – Rolls-Royce, UK

Malý modulární reaktor UK-SMR (obrázek 7) je projektem firmy Rolls-Royce. Je vyvíjen jako kompletní řešení jaderné elektrárny, které je založené na optimalizovaném a rozšířeném využití osvědčených technologií [27]. Firma Rolls-Royce uvádí že návrh využívá inovace tam, kde přinášejí přidanou hodnotu, a zaměřuje se na zajištění nízkých nákladů a výstavby při zachování jaderné bezpečnosti, zabezpečení, záruk a ekologických standardů. Tvrdí, že toho je dosaženo použitím modulárních stavebních technik a výrobou mimo staveniště v továrních podmínkách, což nejsou nové přístupy, ale v jaderném průmyslu nebyly nikdy použity v tak velkém rozsahu.0

Vývoj projektu byl zahájen na podzim roku 2015, kdy byly vybrány hlavní parametry projektu, včetně rozhodnutí využít stávající technologii tlakovodního reaktoru s modulárními a továrními stavebními technikami. Rolls-Royce vypracoval soubor klíčových cílů návrhu projektu na základě funkčních a obchodních potřeb, včetně řady cílů souvisejících s bezpečností, ochranou nebo ekologickými parametry, které byly následně použity při rozhodování a dalším vývoji návrhu 0,0.



Obr. 7. Vizualizace reaktoru UK-SMR společnosti Rolls-Royce 0.

Rolls-Royce uvádí, že pro své projekční činnosti používá kombinovaný přístup systémového inženýrství a posuzování bezpečnosti. Ten se opírá o rámec řízení návrhu, aby bylo zajištěno, že řešení je optimalizováno tak, aby splňovalo všechny klíčové požadavky na jadernou bezpečnost, zabezpečení objektu a fyzickou ochranu [29]. To zahrnuje například bezpečnostní požadavky, které podporují prokázání, že rizika jsou přijatelná a snížená na úroveň ALARP (As Low As Reasonably Practicable), a ekvivalentní požadavky na bezpečnost a záruky 0.

3. METODY VÝBĚRU VHODNÉHO ŘEŠENÍ SLOŽITÉHO PROBLÉMU

Z údajů uvedených výše, je zřejmé, že typy SMR se liší v mnoha oblastech, které nejsou jednoduše srovnatelné. Rozhodnutí o vhodném řešení pro Českou republiku není proto jednoduchá záležitost, protože musí být založeno na komplexním systémovém hodnocení [31]. Z metodologického hlediska je to vícekriteriální hodnocení, které posuzuje přínos dané technologie pro společnost podle jejích dopadů a užitků na základě kritérií ze všech oblastí života společnosti (technické, ekologické, sociální, společenské, ekonomické, právní). Jednotlivé aspekty nelze od sebe uměle oddělovat, protože jsou vzájemně propojeny složitou sítí jemných vazeb, odrážejících reálně existující souvislosti jednotlivých oblastí života společnosti. Z uvedeného důvodu je nutné vytvořit srovnávací platformu, aby výsledky byly logické, průkazné a opakovatelné. Při hodnocení používáme několik souborů kritérií, a to:

- kritéria posouzení uspokojení potřeb,
- kritéria posouzení technické realizovatelnosti,
- kritéria porovnávající úroveň věcného řešení se světem,
- kritéria ekonomické povahy (analýza nákladů a užitků),
- kritéria na dopady techniky a jejich zpětných vazeb na zdraví lidí, životní prostředí, odpady, společnost,
- kritéria na materiálové a energetické nároky i zdroje surovin.

Systém pro podporu rozhodování [31] podporuje analytický styl rozhodování vůči heuristickému rozhodování a vylepšuje rozhodování v případě složitých systémů, když je do něho zabudována strategie multikriteriálního rozhodování.

Rozhodování připravuje tým kompetentních odborníků [31], kteří:

- mají vlastní odborné výsledky v oblasti, do které spadá posuzovaný problém,
- jsou schopni provádět syntézu poznatků, pochopit problém v širokých souvislostech,
- jsou nezaujatí a nezávislí.

Posuzování kompetentnosti odborníků na posuzování daného problému má svá pravidla, která jsou obsažena v odborné literatuře a v mnoha zemích, např. USA, Japonsko a EU jsou obsaženy v právních předpisech.

V případech, že rozhodovaný problém je složitý, tj. zasahuje do více oblastí používáme metody pro podporu rozhodování [31], kterými jsou: metoda používající strom hierarchie kritérií; metoda používající víceúčelový strom hierarchie kritérií; metoda párového srovnání; bodovací metoda; a metoda založená na dílčí funkci užitku. Předmětné metody se obvykle skládají ze 4 metod, a to: metoda identifikace problému; metoda analýzy problému a strukturování problému; metoda tvorby variant řešení; a metoda vyhodnocení variant. Rozdělujeme je na kvantitativní a kvalitativní. Mezi základní kvantitativní metody patří: základní a popisná statistika; výpočet pravděpodobnosti; rozhodovací analýza; řízení kvality; metody vyrovnávání; regresní analýza; lineární programování; řízení zásob; projektové řízení; simulace; a finanční rozhodování.

V praxi se osvědčila metoda multikriteriálního (vícekriteriálního) hodnocení [32] založená na posuzování zranitelnosti jednotlivých prvků systému. Používá se ve strategickém řízení, kdy jde o dlouhodobé řešení. Při hodnocení se oklasifikuje poměrně složitý systém vazeb, ve kterém působení jednotlivých faktorů na výsledný efekt nelze kvantifikovat. Celkové hodnocení je proto relativní a může být ovlivněno subjektivním přístupem jednotlivých hodnotitelů. Je proto výhodné, jestliže hodnocení provede několik na sobě nezávislých expertů. Výsledky hodnocení platí pouze pro hodnocený systém a nelze porovnávat výsledky hodnocení různých systémů posuzovaných zvlášť. V USA a některých dalších zemích se proto kodifikují expertní metody pro tato složitá hodnocení.

Multikriteriální hodnocení založené na systému pro podporu rozhodování zahrnuje:

- vytvoření účelově orientované soustavy kritérií hodnocení,
- stanovení vah kritérií hodnocení,
- stanovení vzorových / mezních hodnot kritérii hodnocení,
- hodnocení dosažených výsledků variant (např. dopady, užitky, škody, ztráty, újmy), jde o dílčí hodnocení každé položky, která pak bude v celkovém hodnocení rozhodující,
- posouzení rizika spojeného s aplikací vybraného způsobu hodnocení položky
- určení preferovaného pořadí variant,
- doporučení nejlepší varianty.

Vytvoření účelově orientované soustavy kritérií hodnocení pochopitelně ovlivňuje nejvíce výsledné hodnocení. Podstata tvorby kritérií spočívá v pečlivém poznání objektu hodnocení a v systému chápání jeho struktury a funkce. Soubor kritérií musí být úplný a také musí být známy podstatné vlastnosti hodnocených objektů. V opačném případě obvykle dojde ke zkreslení celkového výsledku. Akt výběru a uspořádání kritérií hodnocení je složitým a náročným procesem, který nelze nahradit procesně (tj. určeným algoritmem). Jeho nedílnou součástí je i klasifikace možných kritérií.

Souměřitelnost hodnocení kritérií z různých oblastí dosáhneme tím, použijeme hodnoty užitku položky pro rozhodovaný problém. Příkladem tabulky pro dosažení souměřitelnosti je např. tabulka 2 [33].

Tabulka 2. Hodnotová stupnice pro klasifikaci dopadů pohromy.

Oblast	**Hodnotová stupnice pro primární dopady**	**Poznámka**
Sociální	1 – postiženo do 50 lidí 2 – postiženo 50 - 500 lidí 3 – postiženo 500 - 5000 lidí 4 – postiženo 5000 – 50 000 lidí 5 – postiženo 50 000 – 500 000 lidí 6 – postiženo nad 500 000 lidí	U technologických pohrom je třeba uvedená čísla snížit tak, aby byl soulad s právními předpisy, které uvádí limitní hodnotu 1 úmrtí á 10 let.
Technická a ekonomická	1 – škody do 5 000 Kč 2 – škody 5 000 – 50 000 Kč 3 – škody 50 000 – 500 000 Kč 4 – škody 500 000 – 5 000 000 Kč 5 – škody 5 000 000 – 50 000 000 Kč 6 – škody nad 50 000 000 Kč	Při použití ve strategickém plánování je nutno zohlednit skutečnosti se kterými pracuje OSN [34,35], tj. limitní hodnota pro škody je desetina ročního rozpočtu a že výskyt škod větších než desetina rozpočtu po tři roky za sebou je likvidační pro subjekt.
Infrastruktury	1 – výpadkem služby je postiženo méně než 50 lidí 2 – výpadkem služby je postiženo 50 - 500 lidí 3 – výpadkem služby je postiženo 500 - 5000 lidí 4 – výpadkem služby je postiženo 5000 – 50 000 lidí 5 – výpadkem služby je postiženo 50 000 – 500 000 lidí 6 – výpadkem služby je postiženo nad 500 000 lidí	Podle typu infrastruktury je ještě třeba zvážit dobu trvání výpadku služby. V současné době se testují doby trvání 3 hod., 6 hod., 1 den, 3 dny, 14 dní u životně důležitých infrastruktur. Zároveň se počítá s tím, že všude, kde jde o životy lidí, jsou infrastruktury jistým způsobem zálohovány, aby bylo zajištěno přežití lidí.
Ekologická	1 – malé poškození životního prostředí 2 - poškození životního prostředí, které vyrovná příroda během času 3 – mírné poškození neobnovitelných zdrojů přírody a přírodních rezervací 4 - střední poškození neobnovitelných zdrojů přírody a přírodních rezervací 5 – nevratné poškození neobnovitelných zdrojů přírody a přírodních rezervací 6 – devastace krajiny neobnovitelných zdrojů přírody a přírodních rezervací	

Výsledek vícekriteriálního rozhodování je většinou určitý konsensus [31].

4. NÁVRH KRITÉRIÍ PRO VÝBĚR VHODNÉHO REAKTORU PRO ČESKOU REPUBLIKU

Výběr vhodného reaktoru bude zásadním krokem nejen pro úspěšnou realizaci projektu výstavby, ale i pro následné rozšíření reaktorů SMR a jejich dlouhodobý bezpečný, spolehlivý a ekonomický provoz. Na základě výše uvedené metody maximálního užitku [32], znalostí získaných z analýzy dostupných dat, které jsou uvedeny v odstavci 2 a zkušeností z praxe navrhujeme [34], pro výběr typu SMR navrhujeme použít systém pro podporu rozhodování uvedený v tabulce 3 a vyhodnotit je dle tabulky 4.

Kritéria v tabulce 3 navrhujeme hodnotit stupni 1,2,…5 s tím, že čím vyšší je hodnota, tím je přijatelnost nižší. Pro správné vyhodnocení tabulky 3 je třeba dále stanovit hodnotící tým, který vyhovuje kritériím uvedeným v odstavci 3. Zároveň je třeba stanovit člena týmu, který bude řešit konflikty, tj. případy, kdy hodnocení jednotlivých členů expertního týmu budou mít velký rozptyl. Pro vyplňování odpovědí na otázky v tabulce 3 je třeba vytvořit stupnici pro souměřitelnost odpovědí, která je podobná té stupnici v tabulce 2, protože otázky nejsou z jednoho oboru - jsou technické, ekonomické, environmentální, sociální a společenské, a jde o velmi specifickou oblast.

Tabulka 3. Systém pro podporu rozhodování pro výběr vhodného SMR pomocí multikriteriální metody, která je založená na největším užitku; 1-7 označují reaktory popsané v tabulce 1.

Kritérium	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Posouzení výkonu z hlediska podmínek a potřeb praxe v ČR							
Posouzení tlaku I.O. z hlediska podmínek a potřeb praxe v ČR							
Posouzení rozmezí výstupní a vstupní teploty AZ z hlediska podmínek a potřeb praxe v ČR							
Posouzení dostupnosti typu chladiva z hlediska podmínek a potřeb praxe v ČR							
Posouzení délky palivového cyklu z hlediska podmínek a potřeb praxe v ČR							
Posouzení složitosti postupu výměny paliva z hlediska podmínek a potřeb praxe v ČR							
Posouzení bezpečnosti kontejnmentu z hlediska podmínek a potřeb praxe v ČR							
Posouzení počtu záloh kritických komponent z hlediska podmínek a potřeb praxe v ČR							
Posouzení bezpečnosti jaderného paliva z hlediska podmínek a potřeb praxe v ČR							
Posouzení dostupnosti jaderného paliva z hlediska podmínek a potřeb praxe v ČR							
Posouzení prostorových nároků reaktoru z hlediska podmínek a potřeb praxe v ČR							
Posouzení prostorových nároků elektrárny s daným typem reaktoru z hlediska podmínek a potřeb praxe v ČR							
Posouzení nároků elektrárny s daným typem reaktoru na tvar a strukturu základové desky z hlediska podmínek a potřeb praxe v ČR							
Posouzení odborné úrovně reaktoru a jeho bezpečnostních funkcí							
Posouzení odborné úrovně parogenerátoru a jeho bezpečnostních funkcí							
Posouzení bezpečnosti I.O. z hlediska podmínek a potřeb praxe v ČR							
Posouzení bezpečnosti propojení primárního a sekundárního okruhu z hlediska podmínek a potřeb praxe v ČR							
Posouzení odborné úrovně systémů, které zajišťují bezpečnost							
Posouzení odborné úrovně systémů, které přispívají k zajištění bezpečnosti							
Posouzení odborné úrovně tlakové nádoby							
Posouzení odborné úrovně konfigurace kritických komponent jaderného zařízení							
Posouzení odborné úrovně řídícího (ovládacího) systému reaktoru							
Posouzení odborné úrovně aplikace inherentní bezpečnosti							
Posouzení odborné úrovně zajištění ochrany do hloubky							
Posouzení odborné úrovně záloh							
Posouzení nároků na údržbu							
Posouzení odborné úrovně technických systémů, které pomáhají zvládnout nehody a havárie							
Posouzení nároků na obsluhu z hlediska podmínek a potřeb praxe v ČR							
Posouzení odborné úrovně způsobu nakládání s vyhořelým palivem							
Posouzení odborné úrovně ochrany proti vibracím, zemětřesením, vichřici, sesuvu podloží, povodní a proti pádu letadla							
Posouzení výsledků testu provozu reaktoru							
Posouzení počátečních nákladu z hlediska podmínek a potřeb praxe v ČR							
Posouzení nákladů na provoz z hlediska podmínek a potřeb praxe v ČR							
Posouzení nároků na skladování jaderného paliva							
Posouzení nároků na skladování vyhořelého paliva							
Posouzení nároků na dodávky elektřiny z vnější sítě							
Posouzení nároků na množství chladiva							
Posouzení cenové dostupnosti z hlediska podmínek a potřeb praxe v ČR							
CELKEM							

Tabulka 4. Hodnotová stupnice pro určení míry rizika položky a jejího okolí; N = pětinásobku počtu kritérií v systému pro podporu rozhodování dané položky.

Míra přijatelnosti	**Hodnoty v % N**
Zanedbatelná – 5	Více než 95 %
Nízká – 4	70–95 %
Střední - 3	45–70 %

Vysoká - 2	25–45 %
Velmi vysoká – 1	5–25 %
Extrémně vysoká - 0	Méně než 5 %

5. ZÁVĚR

Malé modulární reaktory SMR mohou být novým impulsem pro jadernou energetiku. V České republice jejich stavbu zvažuje společnost ČEZ. V současné době je ve výběru těchto sedm reaktorů AP300 (Westinghouse), BWRx-300 (GE-Hitachi), NuScale (NuScale), Nuward (CEA, EDF, Naval Group a Technicatome), SMART 100 (KAERI a KEPCO E&C), SMR-160 (Holtec) a UK-SMR (Rolls-Royce). Uvedené reaktory se liší v mnoha ohledech, jako jsou typ reaktoru (PWR/BWR), filozofie konceptu (integrální, smyčkový, více modulový atd.), elektrickém výkonu (50-470 MWe) a dalších.

Pro výběr vhodného řešení jsme navrhli na základě multikriteriálního přístupu kritéria. Naším dalším cílem je vytvořit tabulku, dle které zajistíme, že odpovědi na otázky z různých oborů budou souměřitelné.

Poděkování: Předložený výsledek byl vytvořen se státní podporou Technologické agentury ČR v Programu THÉTA v rámci projektu TK05010146. Práce byla podpořena grantem Studentské grantové soutěže ČVUT SGS22/102/OHK2/2T/12. Prezentované výsledky byly realizovány v rámci Institucionální podpory Ministerstva průmyslu a obchodu ČR.

LITERATURA

[1] ČEZ. *Spolupráce a partnerství: Projekty SMR*. Praha: ČEZ 2023, www.cez.cz.
[2] WESTINGHOUSE. *AP300 SMR*. Cranberry Township 2023.
[3] WORLD NUCLEAR NEWS. *Westinghouse Unveils AP300 Small Modular Reactor*. London 2023.
[4] WESTINGHOUSE. *AP300 SMR Flysheet*. Cranberry Township 2023.
[5] WESTINGHOUSE. *AP300 SMR Brochure*. Cranberry Township 2023.
[6] WESTINGHOUSE. *AP300 Small Modular Reactor Pre-Application Regulatory Engagement Plan*. Cranberry Township 2023.
[7] GE. *GE Hitachi BWRX-300 Small Modular Reactor Achieves Pre-Licensing Milestone in Canada*. Boston 2023.
[8] IAEA. *Advances in Small Modular Reactor Technology Developments: A Supplement to the IAEA Advanced Reactor Information System* (ARIS), (2022 Edition). Vienna: International Atomic Energy Agency 2022.
[9] GE. *Licensing Topical Report – BWRX-300 Reactor Pressure Vessel Isolation and Overpressure Protection*. Washington D.C.: United States Nuclear Regulatory Commission 2020.
[10] GE. *Licensing Topical Report – BWRX-300 Containment Performance*. Washington D.C., United States Nuclear Regulatory Commission 2022.
[11] GE. *Licensing Topical Report – BWRX-300 Reactivity Control*. Washington D.C.: United States Nuclear Regulatory Commission 2021.
[12] IAEA. *Status Report – BWRX-300 (GE Hitachi and Hitachi GE Nuclear Energy)*. Vienna: International Atomic Energy Agency 2019.
[13] REYES, J. N .Jr, YOUNG, E. The NuScale Advanced Passive Safety Design. *ASME 2011 Small Modular Reactors Symposium*, September 28–30, 2011, Washington, D.C.: ASME 2011.
[14] WELTER, K., REYES, J.N.JR, BRIGANTIC, A. Unique Safety Features and Licensing Requirements of the NuScale Small Modular Reactor. *Frontiers in Energy Research* (2023), 11.
[15] NUSCALE POWER. *Design Certification - NuScale US600, Standard Design Certification for an Integrated Pressurized Water Reactor Assembly Comprised of Twelve NuScale Small Modular Reactors (SMR)*. Washington D.C.: United States Nuclear Regulatory Commission 2023 .
[16] IAEA. *NuScale SMR: Status report*. Vienna: International Atomic Energy Agency 2011.
[17] FAKHRAEI, A., FAGHIHI, F., RABIEE, A., SAFARINA, M. Coolant Flow Rate Instability during Extended Station Blackout Accident in NuScale SMR: Two Approaches for Improving Flow Stability. *Progress in Nuclear Energy* (2021), 131.
[18] REYES, J.N.JR. NuScale Plant Safety in Response to Extreme Events. *Nuclear Technology* (2017), 178.
[19] IAEA. *Nuward (EDF lead consortium): Status Report*. Vienna: International Atomic Energy Agency 2019.

[20] EDF. *The NUWARD™ SMR Solution.* Paris: Electricité de France 2023.
[21] EDF. BioAge Group, LLC. CEA, EDF, Naval Group, and Technic Atome unveil "NUWARD": *Jointly Developed Small Modular Reactor (SMR) Project*. Paris: Electricité de France 2019.
[22] IAEA. *System-Integrated Modular Advanced Reactor (SMART): Status Report 77*. Vienna: International Atomic Energy Agency 2011.
[23] KEUNG, K.K.K., WONJAE, L., SHUN, Ch., HARK, R.K., JAEJOO, H. SMART: The First Licensed Advanced Integral Reactor. *Journal of Energy and Power Engineering* (2014), 8, pp. 94-102.
[24] KEPCO. *SMART*. https://www.kepco-enc.com/eng/contents.do?key=1539
[25] HOLTEC. *SMR-160.* https://holtecinternational.com/products-and-services/smr/
[26] HOLTEC. *SMR-160 Project Overview.* Washington D.C.: US Nuclear Regulatory Commission 2023.
[27] HOLTEC. *Pre-Licensing Vendor Design Review.* Ottawa: Canadian Nuclear Safety Commission 2023.
[28] ROLLS-ROYCE. *Our Technology.* https://gda.rolls-royce-smr.com/our-technology#:~:text=The %20Rolls%2DRoyce%20SMR%20draws,of%20reactors%20around%20the%20world
[29] ONR. *Generic Design Assessment of the Rolls-Royce SMR-Step 1 Summary*. London: Rolls-Royce 2023.
[30] IAEA. *Status Report – UK SMR*. Vienna: International Atomic Energy Agency 2020.
[31] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369 p.
[32] KEENEY R. L., RAIFFA H. *Decisions with Multiple Objectives: Preferences and Value Trade-Offs.* New York: J. Wiley & Son 1976, 1993, 368 p.
[33] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. ČVUT, Praha 2013, 223p.
[34] ČVUT. Návrhy technických řešení. *Archiv.* Praha: ČVUT 2023.

AKUMULACE TEPELNÉ ENERGIE JAKO PODPORA ENERGETICKÉ BEZPEČNOSTI

THERMAL ENERGY STORAGE AS A SUPPORT FOR ENERGY SAFETY

Daniel Černý, Viktor Kreibich, Jiří Kuchař

ČVUT v Praze, Fakulta strojní, Technická 4, 166 07, Praha 6; d.cerny@fs.cvut.cz

Abstrakt: Článek se zabývá akumulací tepelné energie, která má potenciál napomoci zajištění energetické bezpečnosti při snaze o dosažení nulové uhlíkové stopy. Jsou popsány metody akumulace tepelné energie, zkušební zařízení sestavené pro hodnocení vlastností akumulačních médií a provedené měření simulovaného pracovního cyklu.

Klíčová slova: Akumulace, tepelná energie, energetická bezpečnost, akumulační médium.

Abstract: The article deals with thermal energy storage which has potential to help ensuring energy security during the pursuit of Net Zero Emissions. The existing thermal energy storage methods, testing device built for evaluation of select storage media and a simulated work cycle of the testing device are also described.

Key words: Energy storage, thermal energy, energy safety, storage medium.

1. ÚVOD

Základem energetické bezpečnosti je zajištění nepřerušované přístupnosti zdrojů energie za dostupné ceny. Z energetické situace posledních let vyplynulo, že jsou pro energetickou bezpečnost dle [1] hlavní hrozbou neshody mezi dodávkou a spotřebou. Při snaze o dosažení nulové uhlíkové stopy a přechodu na obnovitelné zdroje je třeba předcházet riziku, které jsou příčinou těchto neshod budováním flexibilní infrastruktury. Jednou z rozmanitých možností vyrovnání neshod mezi dodávkou a spotřebou energie je dle [2] skladování energie ve formě tepla pomocí tepelných akumulátorů.

2. ENERGETICKÁ BEZPEČNOST PŘI SNAZE O UHLÍKOVOU NEUTRALITU

V zájmu zachování energetické bezpečnosti při snaze o dosažení uhlíkové neutrality je nutné vytvořit infrastrukturu umožňující výrobu dostatečného množství energie z obnovitelných zdrojů pro pokrytí energetické spotřeby. Infrastruktura musí dle [1] poskytovat dostatečnou flexibilitu pro pokrytí fluktuací při výrobě obnovitelné energie. Té je dnes někdy dosahováno pomocí uhelných či paroplynových elektráren, které je možné nahradit například přečerpávacími vodními elektrárnami [1,3]. Nedostatkům ve výrobě energie z obnovitelných zdrojů je možné předejít skladováním přebytečné vyrobené energie na střední či dlouhou dobu (týdny až měsíce), například ve formě tepla.

Pro energetickou bezpečnost je dle [1] podstatná efektivita využití veškeré energie. Význam efektivity při přechodu k obnovitelným zdrojům energie narůstá. V zájmu navýšení efektivity je možné zavést infrastrukturu umožňující využití odpadního tepla, bioenergie a dalších možných odpadních či vedlejších produktů, které vznikly ekonomickou aktivitou.

Závislost výroby energie převážně na větru a slunečním záření přináší potřebu plánu pro vyrovnání náhlých nepředpokládaných změn. S rostoucím poměrem energie z obnovitelných zdrojů je nutné zajištění dostatečných kapacit pro její skladování. Dle [1] hraje v plánování a předpovědi velkou roli digitalizace. Digitální technologie jako strojové učení mohou značně zvýšit přesnost předpovědi dodávky a spotřeby energie a umožnit tak efektivní využití skladovacích kapacit.

3. AKUMULACE TEPELNÉ ENERGIE

Hlavním významem akumulace tepelné energie je vyrovnání nesouladů mezi výrobou a spotřebou energie. Nesouladem může být např. časový rozdíl mezi výrobou a spotřebou energie, či rozdíl v umístění. Ke skladování tepelné energie slouží zařízení označovaná jako tepelné akumulátory. Tato zařízení pracují v cyklech, které lze dle [2] rozdělit na následující fáze:

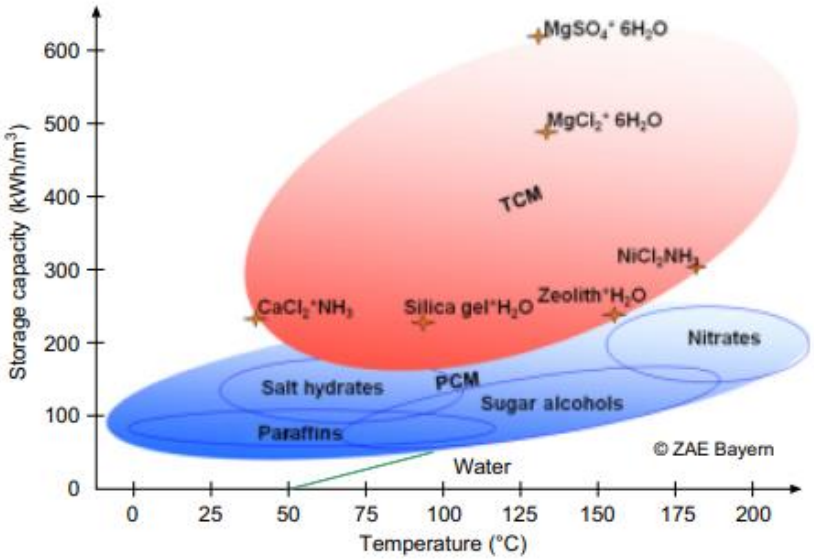
1. Fáze nabíjení (akumulátor energii přijímá).
2. Fáze skladování energie.
3. Fáze vybíjení (akumulátor energii odevzdává).

Nejdůležitějším požadavkem na tepelný akumulátor je hustota uložené energie, která je závislá na zvoleném akumulačním médiu [2]. Na základě současných poznatků dané akumulační médium by také mělo disponovat vlastnostmi vhodnými pro přenos tepla, chemickou a mechanickou stabilitou a nízkými tepelnými ztrátami v průběhu fáze skladování [2,4].

Funkce tepelného akumulátoru závisí na volbě akumulačního média. Dle [4] existují dále uvedené metody tepelné akumulace:

1. Akumulace pomocí tepelné kapacity.
2. Akumulace pomocí skupenského (latentního) tepla.
3. Akumulace pomocí termochemické reakce.

Porovnání metod akumulace tepelné energie je znázorněno v grafu závislostí skladovací kapacity na provozní teplotě na obrázku 1.



Obr. 1. Porovnání metod akumulace tepelné energie [2]. Překlad vysvětlivek v obrázku: Storage capacity – skladovací kapacita, Temperature – teplota, TCM – materiály pro termochemickou akumulaci, PCM – materiály pro akumulaci pomocí latentního tepla, Water – voda představuje omezené porovnání s materiály pro akumulaci pomocí tepelné kapacity.

3.1. Akumulace energie pomocí tepelné kapacity

V literatuře [2,4,5] je uvedeno, že metoda akumulace tepelné energie pomocí tepelné kapacity je aktuálně nejvíce využívanou metodou, a to převážně díky jednoduchosti. Při fázi nabíjení dochází k zahřívání úložného média. V akumulačním médiu nedochází během pracovního cyklu k fázovým přeměnám. Množství energie uložené v akumulačním médiu lze stanovit pomocí vztahu:

$$\boldsymbol{Q = m \cdot c_p \cdot (T_f - T_p)},$$

kde $\boldsymbol{Q}$ je množství uložené energie v Joulech; $\boldsymbol{m}$ je hmotnost úložného média v kilogramech; $\boldsymbol{c_p}$ je měrná tepelná kapacita úložného média; $\boldsymbol{T_f}$ je konečná teplota po tepelné výměně ve stupních Celsia; a $\boldsymbol{T_p}$ je počáteční teplota před tepelnou výměnou ve stupních Celsia.

Hlavními požadavky na akumulační média jsou:
- vysoká hustota a měrná tepelná kapacita, tedy hustota uložené energie,
- široká dostupnost,
- nízká cena,
- chemická stabilita i při zvýšených teplotách
- a tepelná vodivost.

Mezi materiály vhodné pro metodu akumulace pomocí tepelné kapacity se řadí přírodní materiály (písky, drcené nerosty např. žula, čedič atd.), beton, litinová či ocelová drť [5]. Mezi kapalné materiály užívané pro metodu akumulace pomocí tepelné kapacity patří voda, termální oleje, roztavené soli nebo tekuté kovy [6].

3.2. Akumulace pomocí skupenského (latentního) tepla

Metoda akumulace tepelné energie pomocí skupenského tepla závisí na fázových přeměnách v akumulačním médiu [2]. Dle informací uvedených v literatuře [2,4,7] při pracovním cyklu dochází ke skupenským či fázovým přeměnám, které se uskutečňují v úzkém teplotním intervalu. Mimo interval fázové přeměny je teplo ukládáno do tepelné kapacity. Tepelnou energii uloženou ve fázové přeměně je možné vyjádřit vztahem:

$$\Delta \boldsymbol{Q} = \Delta \boldsymbol{H} = \boldsymbol{m} \cdot \Delta \boldsymbol{h},$$

kde $\Delta \boldsymbol{Q}$ je energie uložená ve fázové přeměně v Joulech; $\Delta \boldsymbol{H}$ je rozdíl entalpie před fázovou přeměnou a po jejím průběhu v Joulech; $\boldsymbol{m}$ je hmotnost akumulačního média v kilogramech; a $\Delta \boldsymbol{h}$ je měrná entalpie fázové přeměny.

Hustota uložené energie dosahuje u sledované metody akumulace vyšších hodnot než u akumulace pomocí tepelné kapacity [2]. Nejčastěji užívaná akumulační média pracují na fázovém přechodu z pevného do kapalného skupenství, další možností jsou média s fázovou přeměnou v pevném skupenství nebo s přeměnou kapalina - plyn. Média s fázovou přeměnou na rozhraní kapalina – plyn ovšem doprovází riziko spojené s velkými objemovými změnami [6]. Mezi známá média vhodná pro tuto metodu akumulace patří vybrané parafíny, mastné kyseliny a alkoholy, určené pro nízkoteplotní aplikace [7]. Pro vysokoteplotní aplikace je možné využití vybraných solí, kovů a jejich a jejich slitin [6].

3.3. Akumulace pomocí termochemické reakce

Metoda akumulace tepelné energie pomocí termochemické reakce dle [2] spočívá v uložení energie do produktů vhodné vratné chemické reakce s vysokými energetickými nároky. Z poznatků v literatuře [2,4,7] vyplývá, že při fázi nabíjení dochází k endotermické chemické reakci. Během reakce dochází k zahřívání a rozkladu akumulačního média na samostatné složky, které jsou při fázi skladování uskladněny odděleně. Při spotřebě uložené energie dochází smícháním uložených složek k exotermické reakci, při které dochází k uvolnění uskladněné energie.

Obecný popis typu reakce, na které je tato metoda založena lze vyjádřit následovně:

$$\boldsymbol{AB} + \boldsymbol{teplo} \leftrightarrow \boldsymbol{A} + \boldsymbol{B},$$

který představuje vratnou reakci, při které dochází k rozkladu látky $\boldsymbol{AB}$ za současného dodání reakčního tepla na samostatné složky $\boldsymbol{A} + \boldsymbol{B}$.

Předmětná metoda akumulace tepelné energie umožňuje dosažení nejvyšších hodnot hustoty uložené energie. Praktické využití je ovšem vysoce technologicky náročné a aktuálně velmi nákladné [6], proto je akumulace pomocí termochemické reakce předmětem výzkumů. Největší potenciál vykazuje využití reakcí pevných látek s plyny (s využitím kovových uhličitanů, oxidů, hydridů, hydroxidů) nebo reakcí probíhajících v plynném skupenství (syntéza a rozklad amoniaku, reformace metanu) [5,6].

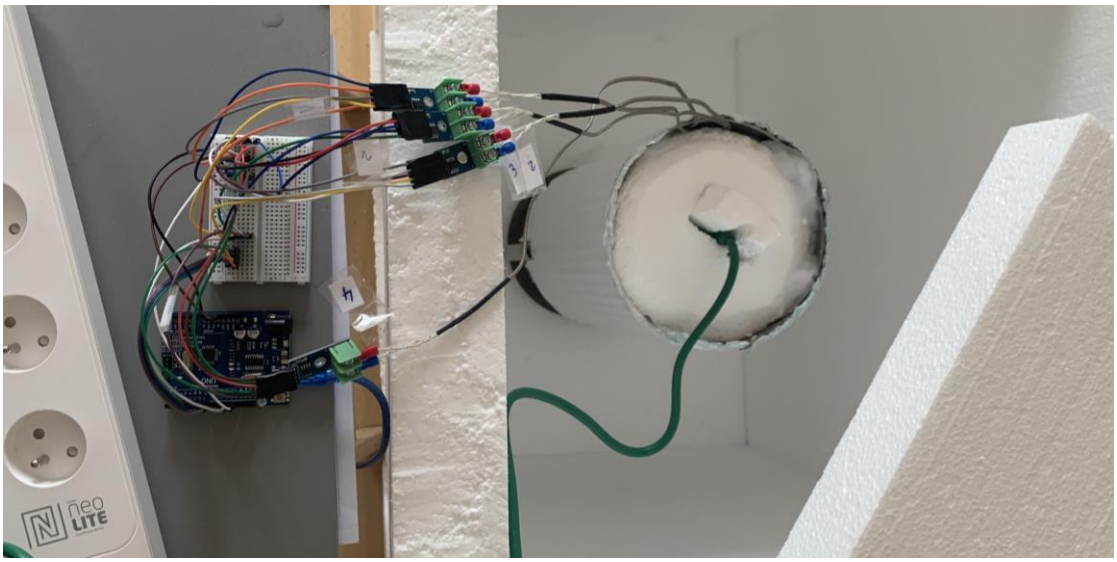
4. EXPERIMENT

Náplní experimentu bylo v první řadě sestavení zkušebního zařízení vhodného pro hodnocení sypkého akumulačního média pro metodu akumulace pomocí tepelné kapacity [8]. Následně byla funkce měřícího zařízení ověřena při měření simulovaného pracovního cyklu.

4.1. Zkušební zařízení

Bylo navrženo a sestaveno zkušební zařízení vhodné k hodnocení chování sypkého akumulačního média pro metodu akumulace pomocí tepelné energie [8]. Konstrukce zařízení je tvořena izolovanou nádobou na akumulační médium, která je uložena v polystyrenovém obložení. Nádoba na akumulační médium je konstrukce svařovaná z trubek z korozivzdorné oceli (1.4301). Izolace nádoby je zajištěna obalem z reflexní izolační folie. Maximální objem zkoušeného média činí 6 litrů a zkušební prostor tvaru válce má podstavou o průměru 168 milimetrů a výšku 300 milimetrů. Polystyrenové obložení slouží ke snížení vlivů kolísání teploty okolního prostředí. K ohřevu akumulačního média bylo použito topné těleso s výkonem 500 W.

Byl navržen a sestaven měřící systém zkušebního zařízení [8], který je složen z mikrokontrolerové desky Arduino Uno, čtyř termočlánků typu K a modulů pro převod analogového signálu na digitální. Fotografie zkompletované sestavy zkušebního zařízení je zachycena na obrázku 2.



Obr. 2. Sestava zkušebního zařízení pro hodnocení akumulačního média.

4.1. Výsledky měření

Zvoleným médiem pro měření byl křemičitý písek (SiO_2) ve frakci 0-0,4 milimetru. Celkem bylo použito 6 litrů média o hmotnosti 7,97 kg [8]. Umístění termočlánků bylo zvoleno následovně:

t1 – v kontaktu s topným tělesem ve výšce 150 mm ode dna nádoby,

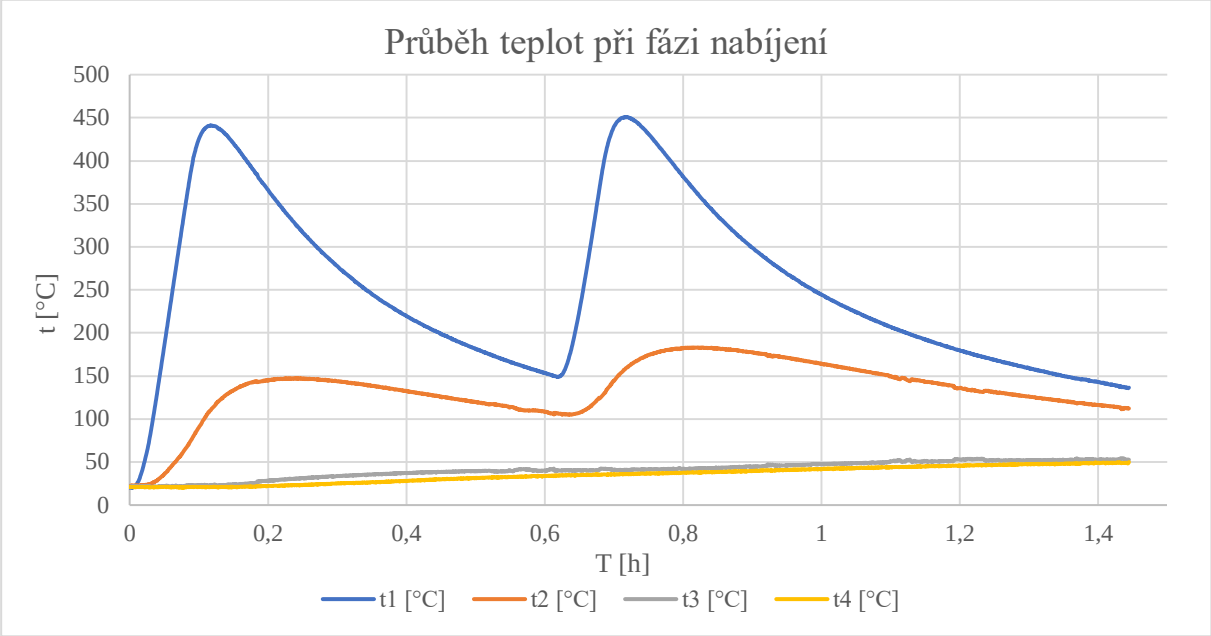
t2 – ve vzdálenosti 40 mm od termočlánku t1, ve výšce 150 mm ode dna nádoby,

t3 – v kontaktu se stěnou nádoby, ve výšce 150 mm ode dna nádoby,

t4 – referenční termočlánek, v kontaktu se stěnou nádoby ve výšce 300 mm.

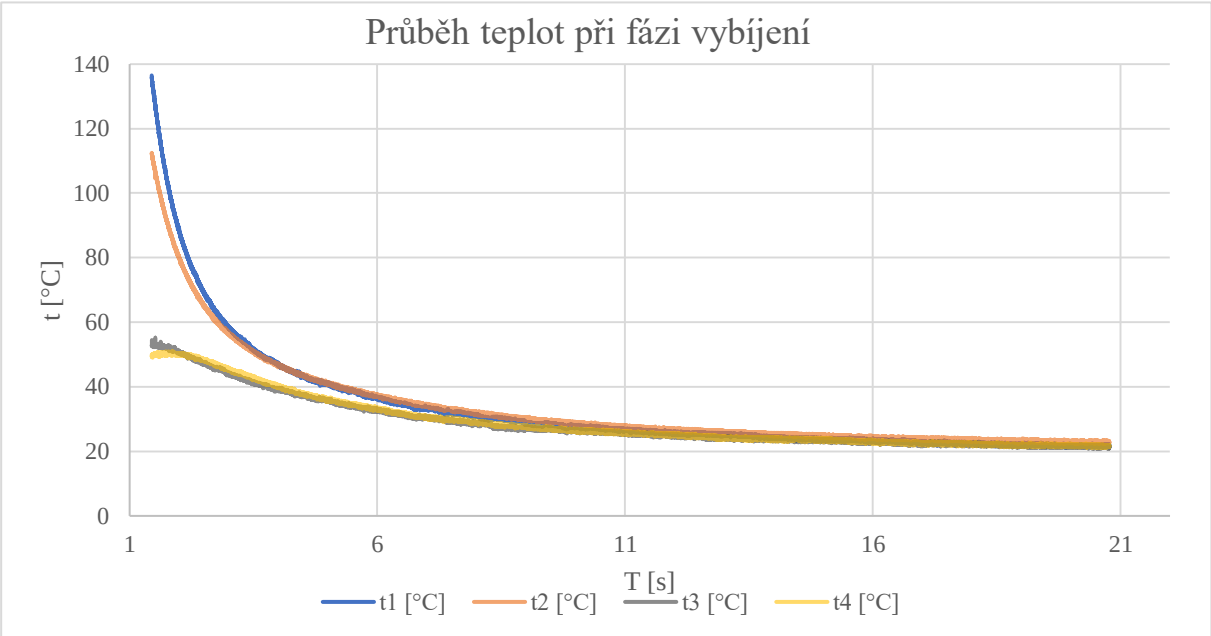
Fáze nabíjení akumulačního média byla řízena teplotou sledovanou na termočlánku t1. Při dosažení teploty 350 °C bylo vypnuto topné těleso a držena prodleva pro vyrovnání teplot. Po poklesu teploty na 150 °C na témže termočlánku bylo topné těleso znovu zapnuto. Ohřívací cyklus byl opakován, dokud nebylo dosaženo předem zvolené kontrolní teploty 50 °C na referenčním termočlánku t4. Po dosažení této teploty byla fáze nabíjení považována za ukončenou a dále probíhalo měření fáze vybíjení [8].

Při vyhodnocení byla naměřená data rozdělena na fázi nabíjení a vybíjení. Fáze nabíjení trvala celkem 86 minut, z čehož aktivní ohřev topným tělesem probíhal pouze 8, 5 minut (přibližně 10 % celkového trvání fáze nabíjení), zbylý čas docházelo k vyrovnávání teplot v médiu. Průběh teplot v závislosti na čase při fázi nabíjení je znázorněn na obrázku 3.



Obr. 3. Průběh naměřených teplot při fázi nabíjení.

Fáze vybíjení trvala celkem 19,3 hodin, dokud nedošlo k vyrovnání teploty média s teplotou okolí. Průběh teplot při fázi vybíjení je znázorněn na obrázku 4.



Obr. 4. Průběh naměřených teplot při fázi vybíjení.

5. ZÁVĚR

V rámci této studie bylo sestaveno a vyzkoušeno zkušební zařízení vhodné ke zjišťování stěžejních vlastností sypkých akumulačních médií. Byl naměřen simulovaný pracovní cyklus křemičitého písku jako akumulačního média. Kvůli časově náročnému procesu vyrovnávání teplot je křemičitý písek společně s metodou akumulace pomocí

tepelné kapacity vhodný převážně pro případy dlouhodobého skladování energie, při kterých není podstatná rychlost nabíjení a vybíjení akumulátoru. Z provedeného měření byl jako vhodný předmět dalšího zkoumání zvolen vliv rozměru částic akumulačního média na rychlost nabíjení akumulátoru a možnosti mísení akumulačních médií za účelem zlepšení akumulačních vlastností při snaze o udržení nízkých cen.

Abychom zajistili výstupy pro praxi, budeme aplikovat na další měření metodiku řízení bezpečnosti procesu (PSM – proces safety management), abychom zjistily interval podmínek, ve kterém budou výsledky opakovatelné [9].

Poděkování: Článek byl podpořen projektem SGS22/156/OHK2/3T/12 (Vliv povrchových úprav na kvalitu výrobních technologií).

LITERATURA

[1] IEA. *World Energy Outlook 2021*. Paris: IEA 2021. https://www.iea.org/reports/world-energy-outlook-2021

[2] CABEZA, L. F. *Advances in Thermal Energy Storage Systems: Methods and Applications*. ISBN 978-0-12-819888-9. město: Woodhead Publishing 2021, 796 p.

[3] ČEZ, A.S. *Přečerpávací vodní elektrárna Dlouhé stráně*. ČEZ, A.S. *SKUPINA ČEZ.* https://www.cez.cz/cs/o-cez/vyrobni-zdroje/obnovitelne-zdroje/voda/vodni-elektrarny/ceska-republika/dlouhe-strane-58155

[4] SADEGHI, G. Energy Storage on Demand: Thermal Energy Storage Development, Materials, Design, and Integration Challenges. *Energy Storage Materials* 46 (2022), pp. 192-222. Doi:10.1016/j.ensm.2022.01.017.

[5] SEYITINI, L., BELGASIM, B., ENWEREMADU, C. C. Solid State Sensible Heat Storage Technology for Industrial Applications – A Review. *Journal of Energy Storage,* 62 (2023). Doi:10.1016/j.est.2023.106919.

[6] ALVA, G., LIN, Y., FANG, G. An Overiew of Thermal Energy Storage Systems. *Energy.* 144 (2017), pp. 341-378. Doi:10.1016/j.energy.2017.12.037.

[7] JOUHARA, H., ŻABNIEŃSKA-GÓRA, A., KHORDEHGAH, AHMAD, D., LIPINSKI, T. Latent Thermal Energy Storage Technologies and Applications: A Review. *International Journal of Thermofluids* Doi:10.1016/j.ijft.2020.100039.

[8] ČERNÝ, D. Akumulace tepelné energie. *Diplomová práce*. Praha: České vysoké učení technické v Praze, Fakulta strojní, Ústav strojírenské technologie2023, 81 p.

[9] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessee: US DOE 1996, 180 p.

ZPĚTNÁ VAZBA Z PROVOZNÍCH UDÁLOSTÍ A ANALÝZA PŘÍČIN NEOBVYKLÝCH UDÁLOSTÍ METODOU IPICA

FEEDBACK FROM OPERATIONAL EVENTS AND ANALYSIS OF THE CAUSES OF UNCOMMON EVENTS BY THE IPICA METHOD

Lenka Frýbortová, Tomáš Bílý

ČVUT v Praze, Fakulta jaderná a fyzikálně inženýrská, V Holešovičkách 2, 180 00 Praha 8. Česká republika. lenka.frybortova@cvut.cz

Abstrakt: Systém řízení bezpečnosti průmyslových procesů se obvykle skládá ze čtyř pilířů: přijetí odpovědnosti za bezpečnost procesu, porozumění zdrojům rizika a riziku, řízení rizika a poučení ze zkušeností. Čtvrtý pilíř, někdy nazývaný také zpětná vazba, pomáhá odhalovat nedostatky v prvních třech pilířích, pomáhá je zlepšovat a přispívá k tomu, aby úroveň řízení bezpečnosti v čase neupadala. Při provozu jaderných elektráren mluvíme o tzv. zpětné vazbě z provozních událostí. Zpětná vazba obsahuje celý životní cyklus poučení ze zkušeností. Provozní události jsou evidovány a vyhodnocovány s cílem zabránit jejich opakování a případně odhalit bezpečnostní rizika spojené s výskytem podobných událostí. Provozní události v jaderných zařízeních ukazují na nedostatky nebo selhání jedné nebo více bariér ochrany do hloubky, nedostatek kontroly nebo nedostatky v řízení bezpečnosti. Identifikace příčin zaznamenaných provozních událostí tak slouží jako možnost poučení a následná opatření vedou k dalšímu zlepšování bezpečnosti. Zavedení systému zpětné vazby je povinností držitele povolení a umožňuje efektivní předávání informací nejen uvnitř organizace, ale také umožňuje sdílet a přebírat zkušenosti s ostatními provozovateli a organizacemi, a to jak na národní tak i mezinárodní úrovni.

Cílem zpětné vazby je zabránit opakování příčin bezpečnostně významných událostí, stanovit události a podmínky, které jsou možnými předchůdci události a potenciální příčinou havárií, stanovit bezpečnostně významné události, jejich kořenové příčiny a stanovit nápravná opatření, a odhalit existující negativní trendy významné z hlediska bezpečnosti.

Legislativa jasně definuje způsob kategorizace událostí, způsob interního hlášení a hlášení dozornému orgánu, požadavky na šetření a analýzu událostí a stanovení nápravných opatření. Za většinu činností je zodpovědný provozovatel jaderného zařízení, nicméně dozorný orgán si zpracovává vlastní posouzení šetření událostí, stanovení kořenových příčin a plnění nápravných opatření. Součástí tohoto procesu je i nezávislé hodnocení neobvyklých provozních událostí hodnotiteli nezávislými jak na provozovateli, tak na regulátorovi.

Při vyšetřování událostí se zpravidla využívá metoda analýzy kořenových příčin (RCA). Nicméně při aplikaci na vážnější nehody ve složitějších systémech tato metoda naráží na určitá omezení, kdy nemůže identifikovat některé typy příčin. Proto byl zaveden inovativní integrovaný přístup k analýze příčin nehod IPICA [1], který nabízí cesty, jak se s omezeními vypořádat. Integrovaný přístup je založen na integraci předpokladů o struktuře řízení bezpečnosti ve zkoumaném procesu do komplexního obrazu. Nabízí integrovaný pohled na různé typy příčin a v nezbytné míře integruje do RCA procedury nelineární model incidentu.

Dalším vývojem vznikl postup IPICA 2.0, [2] který pro analýzu kořenových příčin událostí kombinuje sekvenční metodu IPICA a systémovou metodu CAST. Postup zdokonaluje interní kontrolu úplnosti analýzy použitím třetí popisné alternativy – motýlkového diagramu, vedle sekvenčních a systémových modelů incidentů. Vývojový diagram IPICA 2.0 umožňuje vybrat si z kombinace přístupů ten, který umožňuje nejefektivnější hledání skrytých příčin událostí.

Klíčová slova: Zpětná vazba, analýza kořenových příčin, IPICA.

Abstract: An industrial process safety management system typically consists of four pillars: accepting responsibility for process safety, understanding sources of risk and risk, managing risk, and learning from experience. The fourth pillar, sometimes called feedback, helps identify deficiencies in the first three pillars, helps to improve them, and helps ensure that the level of safety management does not decline over time. When operating nuclear power plants, we talk about so-called feedback from operational events. Feedback includes the entire life cycle of learning from experience. Operational events are recorded and evaluated with the aim of preventing their recurrence and

possibly uncovering security risks associated with the occurrence of similar events. Operational events at nuclear facilities indicate deficiencies or failures of one or more defence-in-depth barriers, lack of control, or deficiencies in safety management. Identification of the causes of recorded operational events thus serves as a learning opportunity and subsequent measures lead to further safety improvements. The establishment of a feedback system is the responsibility of the permit holder and enables the effective transfer of information not only within the organization, but also enables sharing and taking over experience with other operators and organizations, both nationally and internationally.

The aim of the feedback is to prevent the recurrence of the causes of safety-significant events, to determine events and conditions that are possible precursors of the event and the potential cause of accidents, to determine safety-significant events, their root causes and to determine corrective measures, and to reveal existing negative trends significant from the point of view of safety.

The legislation clearly defines the method of categorizing events, the method of internal reporting and reporting to the supervisory authority, the requirements for the investigation and analysis of events and the determination of corrective measures. The operator of the nuclear facility is responsible for most of the activities, however, the supervisory authority processes its own assessment of the investigation of events, the determination of root causes and the implementation of corrective measures. This process also includes an independent evaluation of unusual operational events by evaluators independent of both the operator and the regulator.

When investigating incidents, the root cause analysis (RCA) method is usually used. However, when applied to more serious accidents in more complex systems, this method encounters certain limitations where it cannot identify some types of causes. Therefore, the innovative integrated approach to the analysis of the causes of accidents IPICA [1] was introduced, which offers ways to deal with the limitations. The integrated approach is based on the integration of assumptions about the structure of safety management in the investigated process into a comprehensive picture. It offers an integrated view of different types of causes and integrates a non-linear incident model into the RCA procedure to the extent necessary.

Further development resulted in the IPICA 2.0 procedure, [2] which combines the IPICA sequence method and the CAST system method for the analysis of the root causes of events. The procedure improves the internal control of the completeness of the analysis by using a third descriptive alternative – the butterfly diagram, in addition to sequential and systemic incident models. The IPICA 2.0 flowchart allows you to choose from a combination of approaches the one that allows the most effective search for the hidden causes of events.

Key words: Feedback, root cause analysis, IPICA.

LITERATURA

[1] FERJENCIK, M., BILY, T., FRYBORTOVA, L. A Combined Approach to Incident Cause Analysis: Sque-eze Every Drop of Info from Undesirable Events. *Safety Science.* ISSN 0925-7535. 158 (2023). Doi: 10.1016/j.ssci.2022.105997.

[2] FERJENCIK, M. An Integrated Approach to The Analysis of Incident Causes. *Safety Science*. ISSN 0925-753. 49 (2011), 6, pp. 886-905. Doi:10.1016/j.ssci.2011.02.005.

ŘÍZENÍ RIZIK V RADIAČNÍ OCHRANĚ

RISK MANAGEMENT IN RADIATION PROTECTION

Jiří Havránek

Státní úřad pro jadernou bezpečnost, Senovážné náměstí 9, 110 00 Praha 1, jiri.havranek@sujb.cz

Abstrakt: Článek popisuje vývoj radiační ochrany a způsoby její optimalizace.

Klíčová slova: Radioaktivita, ozáření, dopady, dávka, optimalizace.

Abstract: The article describes the development of radiation protection and ways of its optimization

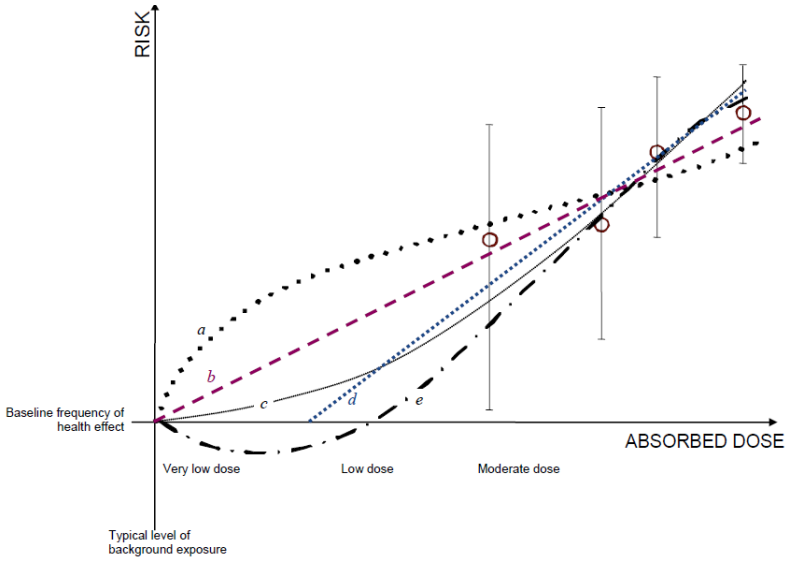
Key words: Radioactivity, irradiation, impacts, dose, optimization.

1. ÚVOD

Rozvoj radiační ochrany začal krátce po objevu X záření W. K. Roentgenem v roce 1895 a radioaktivity H. Becquerelem v roce 1896. Velmi brzo došlo k rozšíření zdrojů ionizujícího záření zejména v lékařství, dále ve výzkumu a průmyslu. Spolu s využíváním ionizujícího záření se záhy začalo objevovat poškození zdraví uživatelů a pacientů. Jako reakce na tyto poznatky o negativních účincích byla navržena první ochranná opatření a posléze byly navrženy i první limity ozáření.

2. SOUHRN POZNATKŮ

Současně s poznatky o biologických účincích ionizujícího záření se vyvíjí i radiační ochrana, kdy první představy o existenci dávkového prahu pro poškození zdraví člověka (tj. existence tzv. bezpečné dávky) jsou nahrazeny lineárním bezprahovým modelem, který je platný dodnes. Základem koncepce radiační ochrany je zamezit vzniku nepříznivých tkáňových reakcí (deterministických účinků) a omezit pravděpodobnost vzniku účinků stochastických na míru pokládanou za přijatelnou pro jednotlivce a společnost. Tkáňové (deterministické) účinky jsou takové účinky ionizujícího záření, k nimž dochází v důsledku smrti části ozářené buněčné populace, jejich závažnost vzrůstá s dávkou od určitého dávkového prahu (pod touto prahovou dávkou se účinek neprojeví) a mají charakteristický klinický obraz. Vztah dávky a účinku pro stochastické účinky je uveden na obrázku 1.



Obr. 1. Vztah dávky a účinku pro stochastické účinky, převzato z [1].

3. RADIAČNÍ OCHRANA V ČESKÉ REPUBLICE

Radiační ochrana je v České republice upravována zákonem č. 263/2016 Sb., atomový zákon a vyhláškou č. 422/2016 Sb., o radiační ochraně a zabezpečení radionuklidového zdroje. Radiační ochrana je v atomovém zákoně definována jako systém technických a organizačních opatření k omezení ozáření fyzické osoby a k ochraně životního prostředí před účinky ionizujícího záření. Samotná koncepce radiační ochrany musí být v souladu se soudobými poznatky o biologických účincích ionizujícího záření, s obecnými přístupy společnosti k ochraně zdraví obyvatelstva před faktory technického rozvoje a životního prostředí a s rozmanitými potřebami soudobé a očekávané praxe, tj. musí brát v úvahu všechny situace v ozáření lidí, jež se vyskytují nebo mohou vyskytnout, a skýtat pro ně principiální řešení. Radiační ochrana stojí na čtyřech základních pilířích – principech radiační ochrany, kterými jsou principy zdůvodnění, optimalizace, dodržení dávkových limitů a bezpečnost zdrojů ionizujícího záření. A právě princip optimalizace řídí rizika v radiační ochraně.

Optimalizace ochrany je definována jako iterativní proces k dosažení a udržení takové úrovně radiační ochrany, aby ozáření fyzické osoby a životního prostředí bylo tak nízké, jakého lze rozumně dosáhnout při uvážení všech hospodářských a společenských hledisek. Princip optimalizace radiační ochrany se aplikuje ve všech třech expozičních situacích, tj. plánovaných expozičních situacích, nehodových expozičních situacích a existujících expozičních situacích. Je to metoda, která je orientovaná do budoucna a směřující k vyloučení nebo snížení budoucích expozic. Zohledňuje jak technický, tak i socioekonomický rozvoj a vyžaduje jak kvalitativní, tak i kvantitativní uvažování. Nejlepší volba je vždy specifická pro danou expoziční situaci a představuje nejlepší úroveň ochrany, kterou lze dosáhnout v daných podmínkách. Nelze tedy určit takovou dávkovou úroveň, po níž by se měl proces optimalizace zastavit.

Optimalizovaná radiační ochrana je výsledkem hodnocení, které pečlivě váží újmu z obdržené dávky na jedné straně a prostředky, které jsou k dispozici pro ochranu jednotlivců na straně druhé. Vedle snížení velikosti individuálních dávek je třeba zvažovat i snížení počtu ozářených jednotlivců. V této souvislosti byla zavedena veličina kolektivní dávka – což je součet efektivních dávek všech jednotlivců v určité skupině (jednotkou je tzv. mansievert). Kolektivní efektivní dávka je a zůstává klíčovým ukazatelem optimalizace ochrany pracovníků. Porovnávání alternativ radiační ochrany pro účely optimalizace musí znamenat i pečlivé zvažování charakteristik distribuce individuálních expozic v ozářené populaci. V souvislosti s optimalizací radiační ochrany se používají tzv. dávkové optimalizační meze a referenční úrovně. Dávkovou optimalizační mezí se rozumí horní mez předpokládaných osobních dávek stanovená pro účely optimalizace radiační ochrany pro příslušný zdroj ionizujícího záření v plánované expoziční situaci. Referenční úroveň je taková úroveň ozáření nebo rizika ozáření v nehodové expoziční situaci nebo v existující expoziční situaci, kterou je nežádoucí překročit. Snížením úrovně ozáření nebo rizika ozáření na referenční úroveň nelze mít optimalizaci radiační ochrany za docílenou. Počátečním záměrem bývá nepřekročit tyto úrovně nebo se na nich udržovat, ale další snahou je snížit dávky na úrovně tak nízké jak je rozumně dosažitelné s přihlédnutím k ekonomickým a společenským hlediskům. Dávková optimalizační mez je taková úroveň dávky, při jejímž překročení je nepravděpodobné, že radiační ochrana pro daný zdroj ozáření je optimalizována, a proto téměř vždy musí být provedeno opatření. Dávkové optimalizační meze pro plánované expoziční situace představují základní úroveň radiační ochrany a budou vždy nižší než příslušný dávkový limit. Koncept dávkových optimalizačních mezí byl uveden v Publikaci ICRP 60 [2] jako nástroj zajišťující, že optimalizační metoda nebude způsobovat nerovnost, tedy možnost, že někteří jednotlivci budou vystaveni podstatně vyššímu ozáření než průměr.

Pro profesní ozáření představuje dávková optimalizační mez hodnotu individuální dávky užívanou k omezení rozpětí uvažovaných možností ozáření. Rozumí se tím, že v procesu optimalizace se uvažuje pouze o možnostech, že očekávané dávky se budou pohybovat pod dávkovými optimalizačními mezemi. Pro ozáření obyvatel je dávková optimalizační mez horní hranicí roční dávky, kterou by mohl jednotlivý obyvatel obdržet z plánovaného provozu konkrétního kontrolovaného zdroje. Dávkové optimalizační meze se nemají užívat jako závazné limity stanovené předpisem, ani nemají být takto chápány [3].

Postup k výběru alternativ radiační ochrany a k posouzení, že další snížení dávky není rozumné, má zahrnovat porovnání určitého množství možných alternativ ke snížení plánovaných a potenciálních dávek jedincům i skupinám. Opatření přijímaná k ochraně jedinců nebo skupin proti vlivu zdroje ionizujícího záření mohou být uplatněna jednak u tohoto zdroje, v prostředí mezi tímto zdrojem a jedincem nebo u jedince. Kde je to možné, dává se přednost omezení vlivu na úrovni zdroje. Taková opatření jsou méně rušivá a vztahují se ke všem cestám ozáření všech lidí z nějakého zdroje. Na rozdíl od toho omezení na úrovni prostředí nebo jedinců nemusí zahrnout všechny možnosti působení zdroje ionizujícího záření. Vedle toho při opatřeních na úrovni zdroje je menší pravděpodobnost neočekávaných socioekonomických problémů, alespoň ve vztahu k ozáření obyvatel. Optimalizace radiační ochrany neznamená minimalizaci. Optimalizace je výsledkem hodnocení, které pečlivě vyvažuje újmu z ozáření

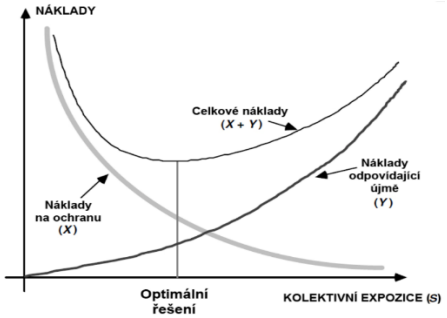
(hospodářskou, humánní, sociální, politickou aj.) a zdroje, které jsou k dispozici pro ochranu jedinců. Proto nejlepší volba není tedy nutně volba s nejnižší dávkou.

Porovnávání alternativ radiační ochrany je klíčovým rysem optimalizačního procesu, který znamená pečlivé zvažování charakteristik rozdělení ozáření jedinců uvnitř skupiny ozářených osob. Každá skupina populace zasažená zdrojem ionizujícího záření může být popsána různými znaky, jako je věk, pohlaví a životní návyky, a také různými parametry ozáření, jako jsou střední, nejmenší a nejvyšší individuální dávka, počet ozářených osob, kolektivní dávka a pravděpodobnost potenciálního ozáření. Další hlediska, která je třeba posoudit při porovnávání alternativ radiační ochrany, jsou společenské hodnoty, zejména míra rovnosti v rozdělení ozáření mezi dotčenými skupinami jedinců. Pro případy expozičních situací při práci jsou většinou informace o dávkách jednotlivým pracovníkům přístupné a v mnoha případech je posouzení rozdělení individuálních dávek relativně snadné. Pro expoziční situace obyvatel informace o jejich individuálních dávkách přímo dostupné zpravidla nejsou a mohou být oceněny pouze použitím zástupných dat. Např. průměrné individuální dávky mohou být odhadnuty s použitím modelu pro různé podskupiny exponované danému zdroji. Při takovém přístupu je nutné pro každou skupinu ozářených obyvatel definovat místo pobývání (vzdálenost od zdroje), rozdělení věku a pohlaví osob a životní návyky (stravování, typy rekreace). Je-li to nutné, je také možné odhadnout vývoj ozáření v čase pro každou skupinu v současné a v budoucích generacích. Jedním ze způsobů, jak charakterizovat rozdělení dávek jedincům uvnitř skupin pro účely porovnávání alternativ radiační ochrany v procesu optimalizace, je používání kolektivní dávky. V případě profesního ozáření se kolektivní dávka obvykle užívá jako „indikátor vykonávání práce“ k charakterizaci celkové dávky spojené s provozem zařízení za určitou dobu nebo při konkrétním typu práce. Pro účely porovnání variant radiační ochrany v procesu optimalizace radiační ochrany není kolektivní dávka vždy postačující k charakterizaci rozložení dávek jedincům, zejména když existují významné rozdíly ve velikosti ozáření jedinců uvnitř exponované skupiny. Za takových okolností musí posuzování rovnosti vzít na zřetel jak individuální, tak i kolektivní dávky spolu s rozdělením expozice.

4. APLIKACE OPTIMALIZACE V PROVOZU A ŘÍZENÍ RADIAČNÍ OCHRANY

Používání technik k podpoře rozhodování určených ke kvantifikaci a porovnávání variantních řešení radiační ochrany v procesu optimalizace umožňuje těm, kteří mají rozhodovat o úrovni radiační ochrany, vybrat nejlepší kompromis mezi různými atributy charakteristickými pro tento proces, s přihlédnutím k neodstranitelným neurčitostem a k zvažování hodnot. Podle míry složitosti situace, jíž se volba může týkat, se mohou používat různé techniky. Historicky byla první technikou propagovanou ICRP [4] na začátku sedmdesátých let minulého století analýza náklady-přínos (cost-benefit) určená k vyvažování nákladů spojených s újmou z ozáření a nákladů na ochranná opatření [5]. Je to jednoduchá metoda, kterou lze použít v řadě oblastí radiační ochrany obyvatel a pracovníků v plánovaných, nehodových a existujících expozičních situacích. Později byly ICRP [6] doporučovány také jiné techniky k podpoře rozhodování, jako je analýza náklady-účinnost (cost-effectiveness) nebo analýza vícefaktorová (multi-attribute) [5].

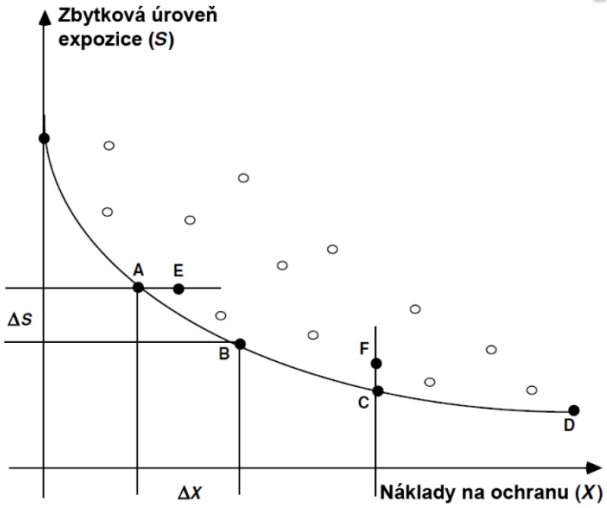
Existují různé způsoby, jak provést analýzu náklady-přínos (cost-benefit) [7]. Nejjednodušší cesta je vyjadřovat peněžním ekvivalentem náklady na radiační ochranu na jedné straně a přínosy na straně druhé a seskupovat je s cílem vybrat variantu s nejnižší peněžní hodnotou tohoto seskupení. Klíčovým momentem tohoto postupu při jeho aplikaci na výběr variant radiační ochrany je používání peněžní hodnoty mansievertu, která umožňuje vyjádřit přínos opatření radiační ochrany (tj. snížení dávky způsobené zavedením určité alternativy ochrany) ve stejné jednotce, jako jsou vyjádřeny náklady ochrany. Celkové náklady každé zvolené alternativy se vypočítávají jako součet s ní spojených nákladů ochrany (X) a příslušných nákladů kolektivní expozice (Y). Optimální varianta radiační ochrany je určována minimální hodnotou celkových nákladů [8]. Schéma je uvedeno na obrázku 2.



Obr. 2. Porovnání nákladů a přínosů; převzato z [8].

Velkým krokem k vypracování konceptu bylo zavedení pojmu odvrácení rizika v práci [7]. S pojmem odvrácení rizika se začal brát ohled na úvahy týkající se rizika jedinců, tj. na individuální dávky v ozářené populaci. Tak kolektivní dávka jednoho mansievertu vyplývající z deseti individuálních dávek 100 mSv a tatáž kolektivní dávka vyplývající z 1000 dávek po 1 mSv nebude hodnocena peněžním ekvivalentem stejně, i když z hlediska kolektivní dávky bude potenciální riziko stejné, pokud se vyjde z hypotézy o bezprahovém lineárním vztahu mezi dávkou a účinkem. Když riziko pro jedince stoupá, působí všeobecná tendence zajišťovat větší ochranu a důsledkem je ochota přidělit více zdrojů a snížit riziko. Je to tedy systém, pomocí něhož peněžní ekvivalent mansievertu vzrůstá se stoupající úrovní expozice jedinců [8].

Přísně vzato analýza náklady-účinnost (cost-effectiveness) není technika optimalizace, ale metoda umožňující vyloučit z řady variant ty alternativy, které nesplňují požadavek efektivity vynaložených nákladů. Pro zbývající alternativy, které vyhovují podmínce „cost-effectiveness“ se potom stanoví pořadí a alternativy se navzájem porovnají [6]. Základním principem metody je nejprve charakterizovat každou alternativu radiační ochrany jejími náklady a odpovídající zbytkovou dávkou. Následujícím krokem je výběr alternativ splňujících požadavek efektivity vynaložených nákladů, tj. těch alternativ, pro něž neexistuje variantní řešení vedoucí ke stejné zbytkové kolektivní dávce při nižších nákladech na ochranu nebo ke stejné úrovni nákladů na ochranu vedoucí k nižší zbytkové kolektivní dávce. Formálně je analýza náklady-účinnost založena na analýze „mezních nákladů“ každé varianty ochrany, která se musí porovnávat s nejblíže levnější nebo dražší variantou. Jestliže nějaký malý přídatný náklad vede k mnohem vyšší efektivitě ve smyslu snížení dávky, splňuje tato nová varianta požadavek efektivity nákladů lépe. Nakonec každá varianta splňující podmínku efektivity nákladů může být charakterizována vzestupem nákladů při přechodu od jedné varianty k nejblíže vyšší [X] a odpovídajícím poklesem kolektivní dávky [S]. Kvocient [X/S] se nazývá podíl náklady-účinnost (cost-effectiveness ratio) a představuje základ pro určování pořadí různých variant ochrany. Nejlepší variantou je ta, jejíž podíl je rovný peněžnímu ekvivalentu mansievertu, vybranému jako referenční kritérium pro konkrétní expoziční situaci nebo je právě pod ním [8]. Schéma je vedeno na obrázku 3.



Obr. 3. Korelace zbytkové úrovně expozice a nákladů na ochranu; převzato z [8].

Když příslušné znaky (attributes) k charakterizaci expoziční situace, mimo újmy z ozáření a nákladů na radiační ochranu, jsou početné nebo v peněžních ukazatelích obtížně kvantifikovatelné, a přitom jsou kvantifikovatelné podle jiných kritérií nebo připouštějí stanovit kvantitativním způsobem své pořadí, může být vhodnější použít vícefaktorovou analýzu přínosnosti (multi-attribute utility analysis – MAUA) [6]. Základním principem této techniky je vytvoření skórovacího schématu (nebo-li funkce vícefaktorové přínosnosti – multiple utility function) pro každou alternativu ochrany na základě všech významných kritérií charakterizujících situaci (tj. nákladů zvoleného ochranného opatření, kolektivní dávky, dávky jedincům, rozložení expozice v čase a prostoru, vnímání úrovně rizika aj.). Identifikace různých alternativ ochrany, což bývá prvním krokem v metodě MAUA, je spojena s definováním příslušných kritérií pro konkrétní rozhodovací proces. Potom podle těchto jednotlivých kritérií opatření musí být vyhodnoceno (buď kvantitativně, nebo kvalitativně) každé ochranné opatření. Vzhledem k různorodosti kritérií je variantám ochrany přiřazeno v rámci každého kritéria rozdílné pořadí. Další krok spočívá v přiřazení váhových faktorů každému kritériu, aby se vyjádřila relativní důležitost náležející každému z těchto kritérií. Je třeba poznamenat, že toto je nejdůležitější a často obtížný krok v MAUA. Přitom však existuje několik metod k

odvození souboru hodnot váhových faktorů a ať už je použito kterékoliv z nich, volba těchto faktorů musí být vždy zdůvodněna. Nakonec se vybere alternativa radiační ochrany, která vede k nejvyšší celkové přínosnosti. Vzhledem k tomu, že váhové faktory se většinou opírají o hodnotový žebříček nositele rozhodování, doporučuje se naléhavě provést analýzu citlivosti pro rozdílné soubory váhových faktorů, aby se testovala „odolnost“ výsledků [8].

5. ZÁVĚR

Pro mnoho expozičních situací je použití technik k podpoře rozhodování účinným nástrojem k formalizaci a kvantifikaci výběru nejlepší alternativy v procesu optimalizace. Výběr konkrétní techniky je určován zejména typem dostupných vstupních dat a ochotou zohlednit v konečných výsledcích různé příznačné znaky/atributy charakterizující situaci. Z toho hlediska je zřejmé, že vícefaktorová analýza přínosnosti (MAUA) se spíše hodí pro situace s protikladnými atributy a hledisky nositelů rozhodování. Je ovšem důležité mít na paměti, že s mnoha atributy je možné se vypořádat také v rámci metody „cost-benefit“ za předpokladu, že proces vážení vztažený k zařazeným atributům je jasně vymezen a že se k potvrzení výsledků provede široká analýza citlivosti [8].

LITERATURA

[1] UN. *Sources, Effects and Risks of Ionizing Radiation.* ISBN 978-92-1-142307-5. New York: UN 2015, 232 p.

[2] ICPR. Recommendations of the ICPR. ICPR 60. *Annals of the ICPR.* ISSN 0146-6453. 21 (1991), 1-3, pp. 1-211.

[3] ICPR. Recommendations of the ICPR. ICPR 103. *Annals of the ICPR.* ISSN 0146-6453. 20 (2007), 2-4, pp. 81-136.

[4]] ICPR. Recommendations of the ICPR. ICPR 21. *Annals of the ICPR.* ISSN 0146-6453. 20 (1973), 1, pp. 1-73.

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

[6] ICPR. Recommendations of the ICPR. ICPR 55. *Annals of the ICPR.* ISBN 0-08-016872-8 Pergamon Press 1973, 47 p.

[7] ICPR. Recommendations of the ICPR. ICPR 37. *Annals of the ICPR.* ISSN 0146-6453. 10 (1983), 2-3, pp. 6-45.

[8] ICPR. Recommendations of the ICPR. ICPR 101. *Annals of the ICPR.* ISSN 0146-6453. 36 (2006) 3, pp. 23-34.

DOPADY ENERGETICKÉ KRIZE NA ČESKÉ SLÉVÁRENSTVÍ

IMPACTS OF THE ENERGY CRISIS ON CZECH FOUNDRY

Aleš Herman[1], Jindřich Zeman[1], Josef Hlavinka[2]

[1] *ČVUT v Praze, Fakulta strojní, Technická 4, 166 04 Praha 6, ales.herman@fs.cvut.cz*
[2] *Svaz sléváren České republiky, Technická 2896/2, 616 00 Brno, dir@svazslevaren.cz*

Abstrakt: Příspěvek pojednává o energetické krizi v letech 2021 – 2022 a jejím vlivu na dopady na české slévárny. Je to ukázáno na jedné anonymizované slévárně, která tuto krizi zatím přežila. Jsou zde zmíněny klíčové momenty, jak krize na slévárny dopadaly a s čím se musí potýkat.

Klíčová slova: Elektřina, zemní plyn, náklady, energetická krize.

Abstract: The paper discusses the energy crisis in 2021-2022 and its effect on the impact on Czech foundries. It is shown at one anonymized foundry that has survived this crisis so far. The key moments of how the crisis affected foundries and what they have to deal with are mentioned here.

Keywords: Electricity, natural gas, costs, energy crisis.

1. ÚVOD

V roce 2020 a 2021 se nejen v ČR začaly odehrávat poměrně závažné změny v distribuci energií [1]. V tomto období došlo k několika závažným událostem:

1. Německo začalo s útlumem jaderných elektráren – omezení výroby a nutnost náhrady nákupem z ostatních zemí
2. Začala válka na Ukrajině a Rusko začalo omezovat tok plynu do Evropy – růst ceny zemního plynu
3. Nedostatek vody v řekách – malá možnost výroby elektřiny z vodních děl v Německu

Kvůli útlumu jaderných elektráren se v Německu se zvedla poptávka po nákupu energií zvenčí. Sami Němci kvůli rušení jaderných elektráren a změny uhelných elektráren na plynové si vytvořili velmi špatný energetický mix, kde se na výrobě energií podílí 50% plynových elektráren. Toto mělo v souvislosti se zvedáním ceny zemního plynu k růstu mezních cen elektřiny na burze (princip stanovení mezních cen (obrázek 1).

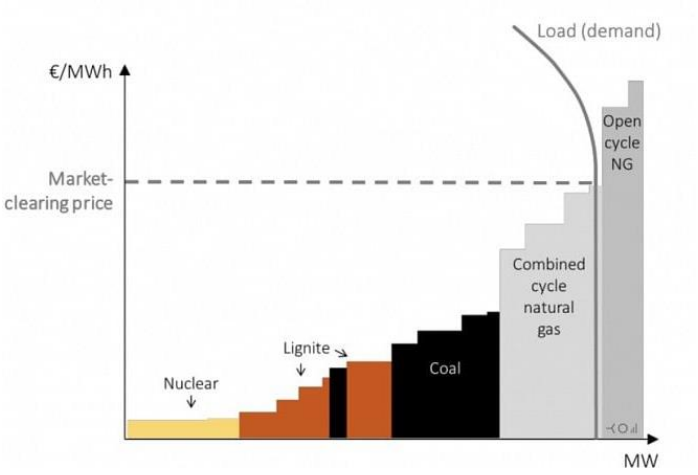
Mezní ceny znamenají, že ceny elektřiny se stanovují podle variabilních nákladů mezního zařízení, tj. nejdražší elektrárny, která je potřeba k uspokojení poptávky (tzv. závěrná elektrárna). To se často znázorňuje pomocí "merit order" křivky – grafu, který znázorňuje náklady na výrobu elektřiny ze stávajících elektráren, které jsou na burze. Aby se uspokojila poptávka po elektřině, postupně se do systému zapojují další zdroje podle výše svých mezních nákladů. S rostoucí poptávkou je vždy nutné zapojit další dražší zdroj, přičemž ceny se vždy odvíjí právě od nejdražšího zdroje. Pořadí, ve kterém jsou zapínány jednotlivé elektrárny podle jejich finanční náročnosti, se označuje právě "merit order". Všichni výrobci dostávají a všichni spotřebitelé platí stejnou cenu [2].

Spolu v kombinaci výše uvedených vnějších faktorů a s růstem cen za zemní plyn toto doslova vyvolalo řetězovou reakci, která vedla zdražování elektřiny a obecně všech energií (obrázky 2 a 3) [3].

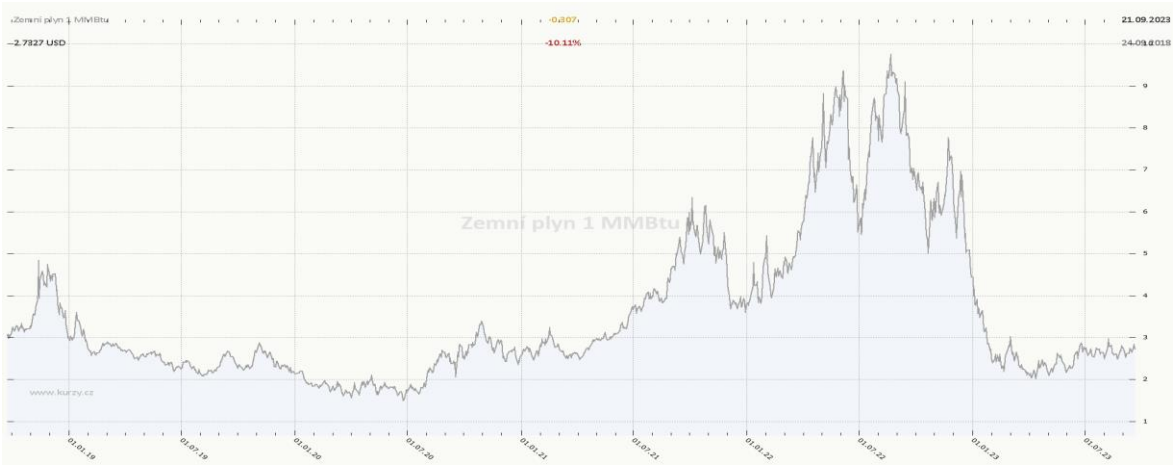
Toto mělo za následek zhoršování ekonomické situace dodavatelů energií (elektřina a plyn) s ohledem na poměrně nízko fixované ceny, které se začaly od těch aktuálních tržních cen na burze několikanásobně lišit. Předzvěstí událostí na trhu s energetickými komoditami v Česku se stalo ukončení činnosti společnosti Slovakia Energy na slovenském trhu, které tato firma patřící do skupiny Bohemia Energy oznámila 30. září 2021[4].

Sérii úpadků dodavatelů energií zahájila energetická skupina Bohemia Energy, která se 13. října 2021 rozhodla ukončit podnikatelskou činnost (600 000 odběrných míst el. energie a 300000 odběrných míst plynu) [5]. V návaznosti na tyto události Energetický regulační úřad zahájil prověřování všech dodavatelů energie, zda mají zajištěný dostatek energie odpovídající závazkům, které mají vůči domácnostem i podnikům [6]. A do března 2022 ukončilo činnost dalších 12 dodavatelů energie. Tzn. že po ukončení dodávek energií spadlo do režimu DPI (dodavatel poslední instance) přes milion odběrných míst (neodlišujeme plyn a elektřinu). Tato situace se bohužel

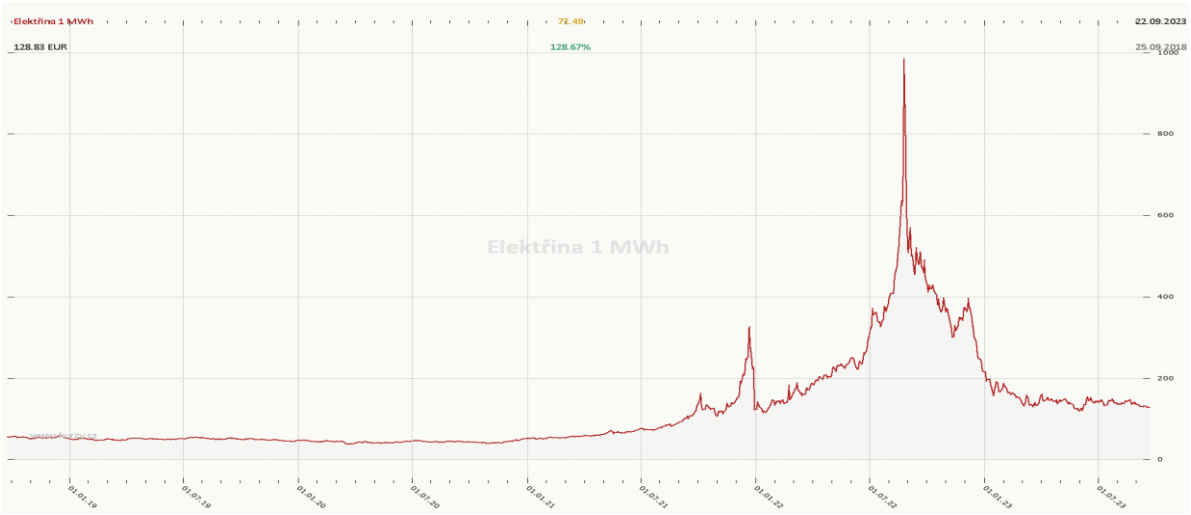
nevyhnula ani slévárnám, které již z principu výroby mají velmi vysoké energetické náklady (tavení, předehřevy, regenerace formovacích směsí a tepelné zpracování).



Obr. 1. Stanovení mezních cen (tzv. závěrné – výrobně nejdražší elektrárny) [2].



Obr. 2 .Vývoj cen zemního plynu v období 01/2019 – 07/2023 [7].



Obr. 3. Vývoj cen zemního plynu v období 01/2019 – 07/2023 [8].

2. ANALÝZA POHYBU ENERGETICKÝCH KOMODIT

Pokud se podrobně podíváme na růst energií v průběhu let 2021 – 2022, tak z obrázků 2 a 3 lze vyčíst následující. První změny v cenách jsou zaznamenány u plynu, kdy v létě 2021 vlivem omezených dodávek plynu z Ruska (opravy NORD STREAM1) a nedostatku vody v Německých řekách je zvýšená poptávka po elektřině a musí běžet v Německu i plynové elektrárny. Maximální ceny plynu se na první maximum vyšplhaly v září 2021 a pomalu klesají do konce roku 2021 (ale už ne na hodnoty z let 2019 a 2020). Tato změna způsobí nárůst cen elektřiny, který je pozvolný od počátku roku 2021 (vlivem omezení jaderných elektráren v Německu) a k lomu křivky /tedy rychlejšímu nárůstu dochází v ca 7/2021, kde se začne projevovat narůstající cena zemního plynu. K prvnímu výraznému skoku v cenách el. energie dochází v 09/2021, kdy cena elektřiny vyskočí zhruba o 600% - toto má za následek úpadek dodavatelů energie.

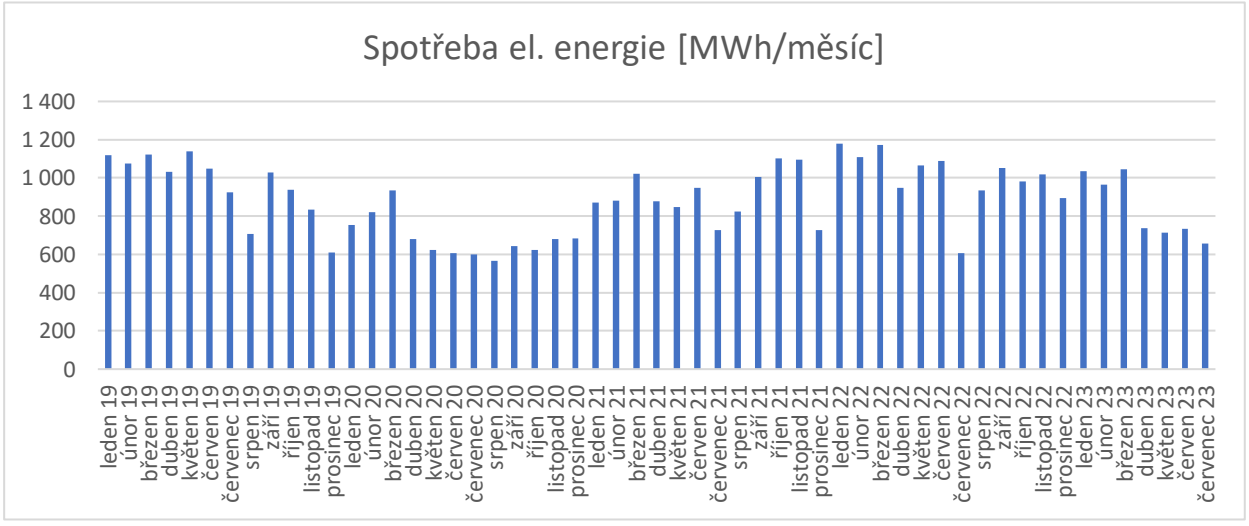
Od 09/2021 dochází na mezinárodním poli jednak k omezování dodávek plynu z Ruska (výmluvy na sankce a nemožnost opravy Nord stream 1) a okamžité hledání náhrady pomocí zkapalněného zemního plynu. Tudíž cena zemního plynu stále stoupá a zničením NORD STREAM 2 (03/2022) [6] dosahuje v 04/2022 prvního maxima. Toto zdražování plynu má za důsledek poměrně prudké zdražování elektrické energie, kde opět v 05/2022 dojde k výraznému zlomu a poměrně strmému stoupání cen elektřiny. Hlavním viníkem je zde opět německý vliv, kdy kvůli nedostatku vody nemohou pouštět vodní elektrárny a jsou nutné chybějící elektřinu nakupovat a vyrábět na plynových elektrárnách. Toto trvá celé léto a prakticky po celý rok měli v Německu vyprázdněné zásobníky, takže zvyšovali poptávku po zemním a zkapalněném plynu, kde cena rostla na maximum, kterého dosáhla 08/2022, kdy se cena zemního plynu zvedla zhruba o 500%. Toto mělo dopad i na elektřinu, kdy pík cen elektřiny také nastal v 08/2022 – zde nastal nárůst oproti rokům 2019 – 2020 zhruba o 1350%.

3. SITUACE – STŘEDNĚ VELKÁ SLÉVÁRNA LITIN

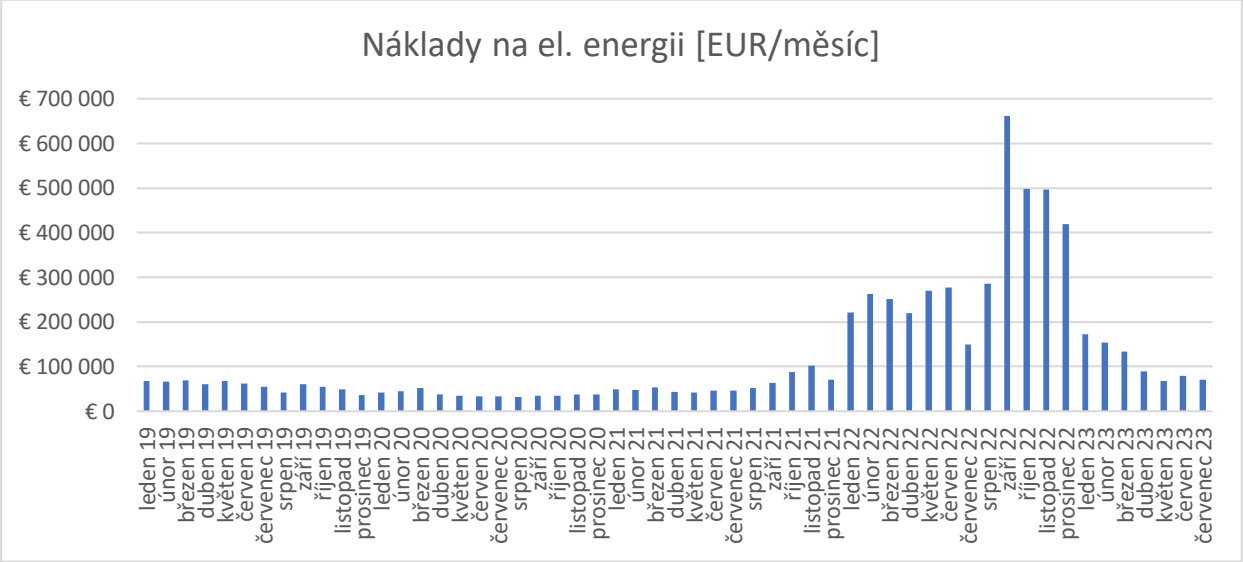
Představíme si vše na typické slévárně litin, kde se zemní plyn využívá k vysoušení formovací směsi po mokré regeneraci a k předehřevu licích pánví. Elektřina se kromě osvětlení používá pro tavení materiálu. A ukážeme si, jak se výše zmíněné zlomy projevili v nákladech slévárny – vždy ve srovnání s předchozími roky 2019 a 2020. Daná slévárna má zhruba roční spotřebu elektrické energie 11 GWh a zemního plynu 5 GWh. Na obrázcích 4 a 5 je ukázána spotřeba elektrické energie, včetně nákladů na ní. Na obrázcích 6 a 7 je ukázána spotřeba zemního plynu a nákladů na zemní plyn ve výše uvedeném období.

Spotřeba elektrické energie i plynu kopíruje snížené výkony v období Covidu, u zemního plynu došlo v roce 2020 k úpravě vysoušení formovací směsi po mokré regeneraci a ke změně předehřevu pánví, proto spotřeba pro rok 2021 vykazuje pokles oproti roku 2019. Na obrázcích 4 a 6 je rovněž vidět vliv celozávodní dovolené (2 týdny – přelom července, srpna, týden na konci roku).

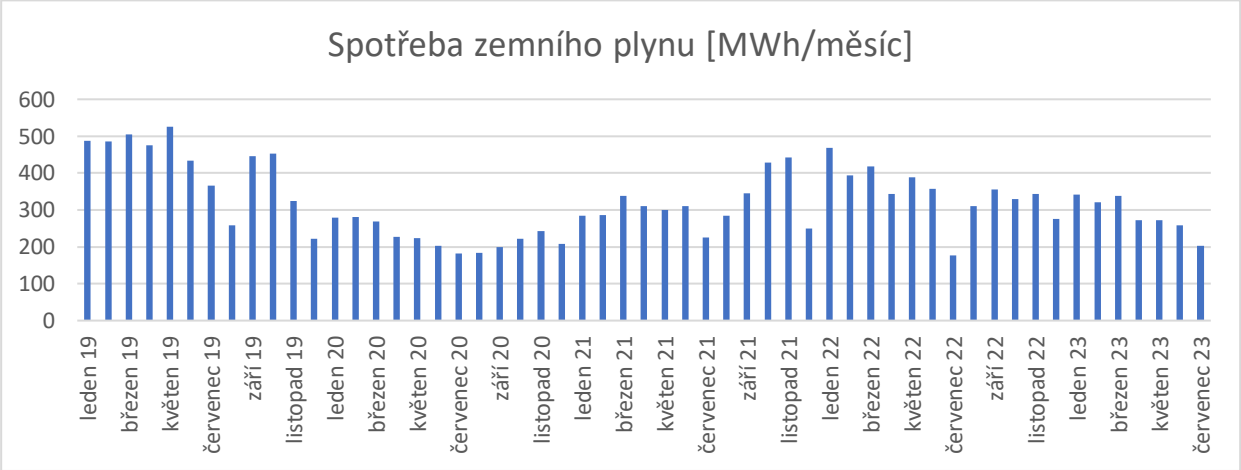
Pokud se týká nákladu na elektrickou energii tak měsíční náklady v r. 2020 a první pol. 2021 se pohybovaly v rozmezí 35 – 45 tisíc EUR. Cena za tyto energie začala pozvolně narůstat od září 2021 ca o 10 tisíc EUR/měsíc.



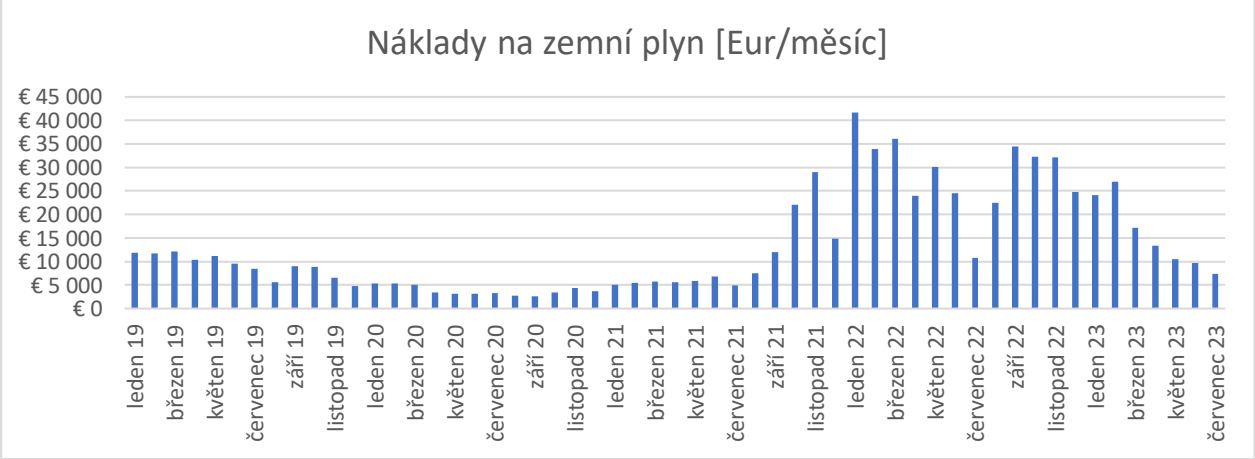
Obr. 4. Spotřeba elektrické energie ve slévárně v letech 2019 - 07/ 2023.



Obr. 5. Náklady na elektrickou energii ve slévárně v letech 2019 - 07/ 2023.



Obr. 6. Spotřeba zemního plynu ve slévárně v letech 2019 - 07/ 2023.



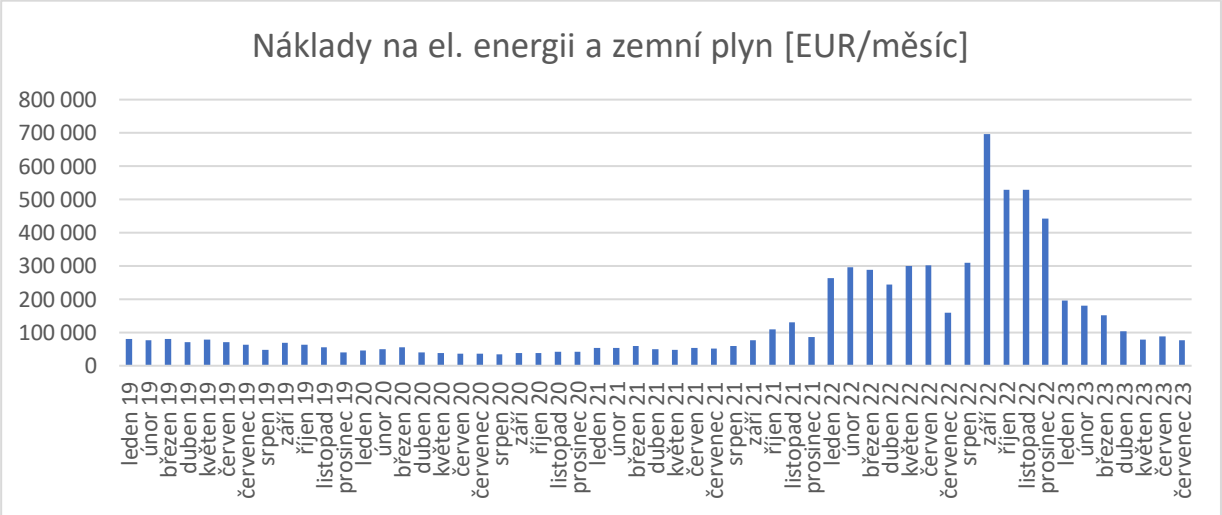
Obr. 7. Náklady na zemní plyn ve slévárně v letech 2019 - 07/ 2023.

Jak je uvedeno výše, ukončení dodávek energií a přechod do režimu DPI se bohužel nevyhnul ani slévárnám. K těmto situacím docházelo v období 09/2021 až 4/22. Pro slévárnu v tomto příspěvku došlo ke změně režimu DPI v 12/2021 V tomto období dodavatel energií (elektřina i zemní plyn) ukončil činnost a slévárna byla převedena do režimu DPI a od 1/2022 přešel k novému dodavateli energie s tím, že fixace nebyla možná a vše přešlo na spotové ceny. Období 01 – 06/2022 byly průměrné měsíční náklady na ca 280 tisíc EUR. Tj. oproti roku 2020 a 1. polovině r. 2021 se jedná o nárůst ca o 700 %. Vlivem celkového nárůstu energie (obrázek 4) v 08/2022 – se toto projevilo i na spotových cenách, kdy v září náklady na elektrickou energii vzrostly až na 660 tis. EUR/měsíc – ***tj. nárůst oproti 2020 o zhruba 1650 % !!!.***

Podobná situace byla u zemního plynu, kde se spotřeba pohybuje relativně po sinusoidě v závislosti na ročním období. V rozmezí 200 – 400 MWh/měsíc. Za období 2020 a 1.pol. roku 2021 byly náklady zhruba v rozmezí 3,5 – 5,0 tisíc EUR/ měsíc. Od září 2021 začaly tyto náklady stoupat měsíčně až na částku 42 tisíc EUR/měsíc (01/2022)– ***zde se jedná o zdražení zhruba 800 - 900 %.*** V roce 2022 již pak tyto náklady nedosahovaly takto vysokých hodnot, ale došlo k poklesu průměrně na 33 tis. EUR/měsíc – což je opět oproti roku 2020 a 2021 cena vyšší ca o 700 %.

Pokud se na tyto energetické náklady podíváme součtově – obrázek 8, kde průměrné měsíční náklady na energie (elektřina + zemní plyn) byly v roce 2020 a 1. polovině roku 2021 průměrně 54 tisíc EUR, tak tyto náklady se zvedly v 09/2022 až na 696 tisíc EUR/měsíc – ***tzn. hlavní energetické náklady se v tomto měsíci zvedly o 1290%.*** A v dalších měsících roku 2022 byly na úrovni ca 500 tisíc EUR/ měsíc – zde jsou náklady vyšší o ca 1000%.

V r. 2023 došlo už k částečné fixaci cen – jak elektřiny, tak i zemního plynu, takže celkové náklady se pohybují na úrovni 80 – 90 tisíc EUR/měsíc – zde se jedná o zdražení o ca 60 %, které vypadá, že už bude trvalé, pokud nedojde opět k nějakým výrazným výkyvům na burzách.



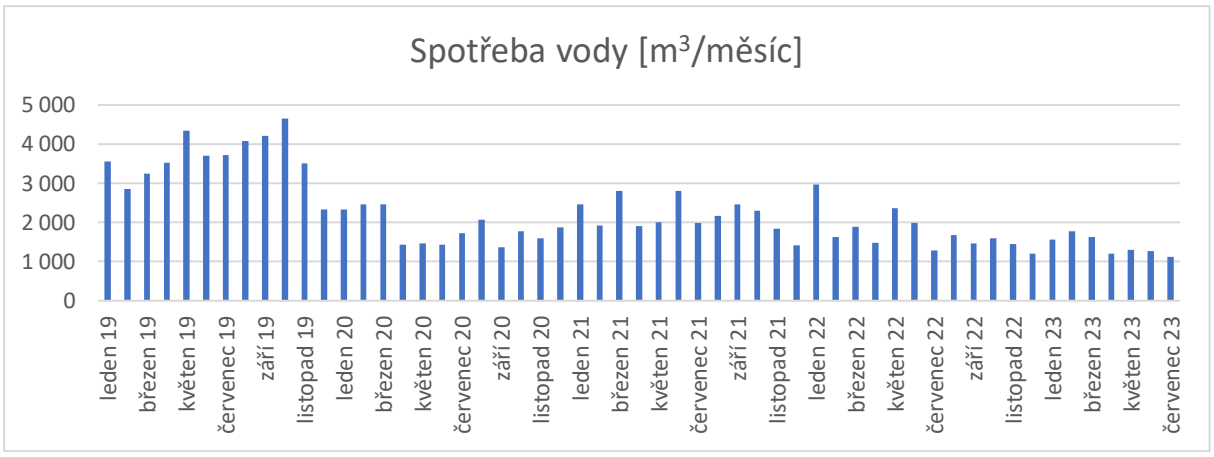
Obr. 8. Kumulativní náklady na zemní plyn a elektřinu ve slévárně v letech 2019 - 07/ 2023.

Do nákladů vstupují i další položky závislé na energiích a inflaci jako je spotřeba tepla, vody (pitná, užitková a stočné) a spotřeba stlačeného vzduchu, které jsou ve srovnání s předchozími položkami na úrovni jednotek procent, ale do celkové sumace se pak také promítnou. Náklady na vodu a její spotřeba, jak pitnou, užitnou včetně stočného jsou uvedeny na obrázcích 9 a obr.10. Díky úpravám v technologickém procesu se vede snižovat celkové množství vody za posledních 5 let tato spotřeba klesla na 1/3. Ovšem z důvodu rostoucích cen vodného a stočného jsou náklady prakticky konstantní.

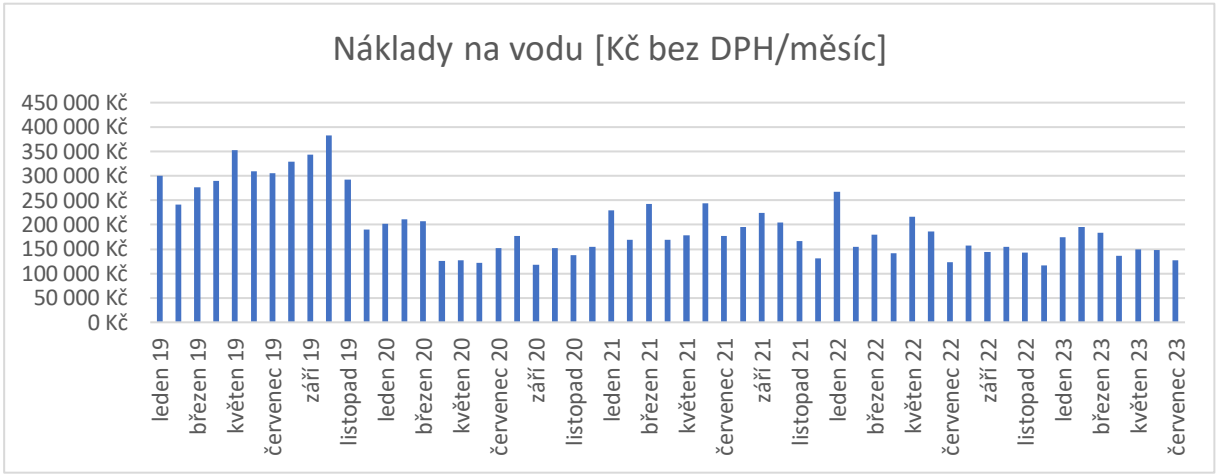
Jedním z nezanedbatelných energetických nákladů je i spotřeba stlačeného vzduchu, který je nutný k různým operacím na slévárně (tryskání, pneudoprava, ofuk forem, jader atd. Na obrázku 11 je vidět průběh spotřeby stlačeného vzduchu pozvolně rostou – za toto pětileté období narostly o 12% (obrázek 12).

Poslední z nezanedbatelných energetických nákladů je i spotřeba tepla - jednak vytápění slévárny, kancelářských prostor. Průběh spotřeby nakupovaného tepla kopíruje tvar sinusoidy (obrázek 13) a náklady na teplo se měnili z ca 340 Kč/GJ na částku 740 Kč/GJ – to znamená za období 5 let vzrostly celkově o 120%, při téměř stejných

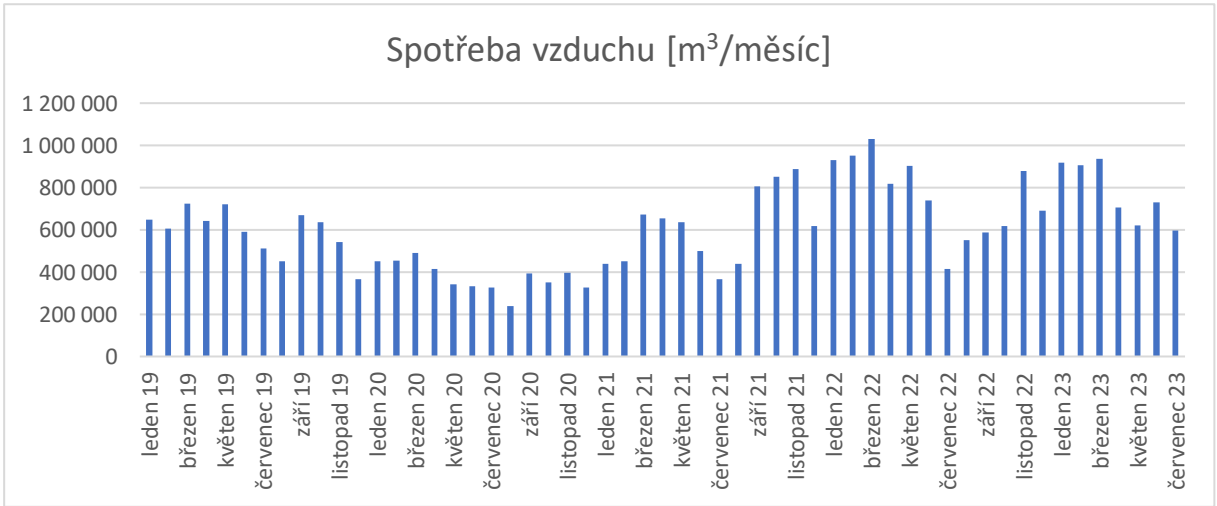
nákladech (obrázek 14). Tzn. že slévárna udělala řadu opatření ke snížení topných ztrát a snížení spotřeby tepla ca o 1/3, ale ve výsledku se tyto náklady neustále zvyšují.



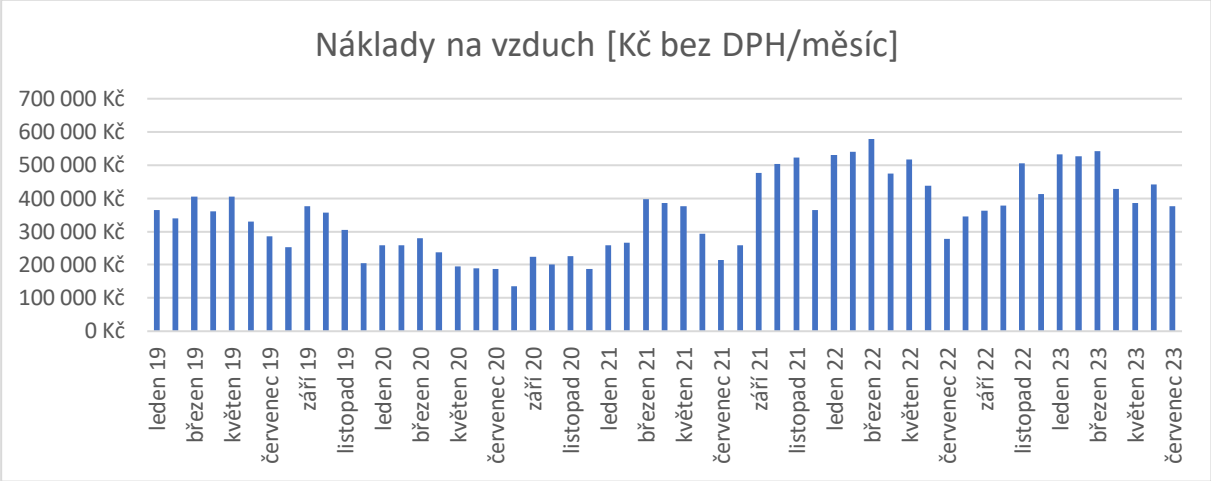
Obr. 9. Spotřeba vody ve slévárně v letech 2019 - 07/ 2023.



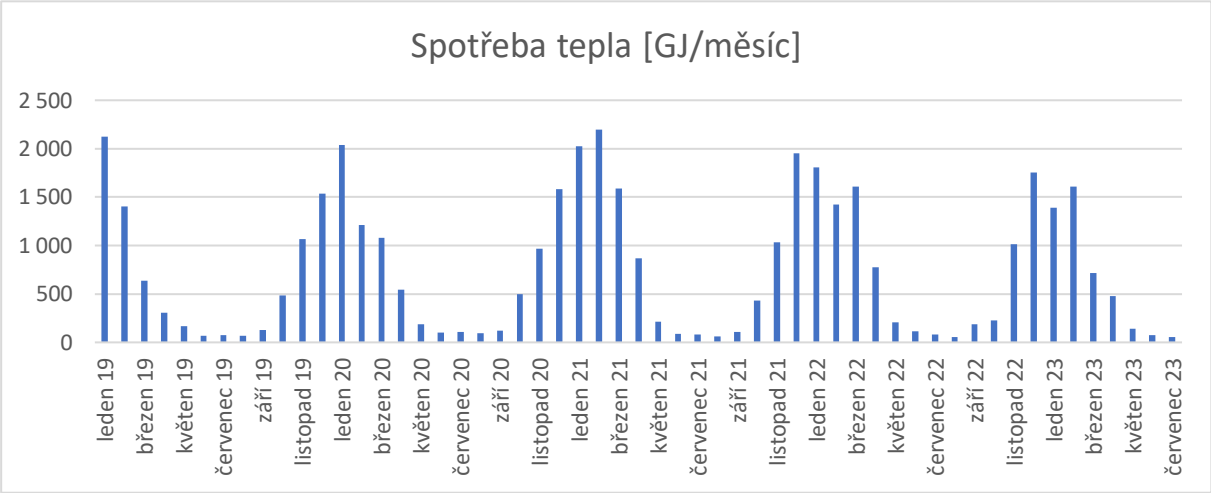
Obr. 10. Náklady na vodu ve slévárně v letech 2019 - 07/ 2023.



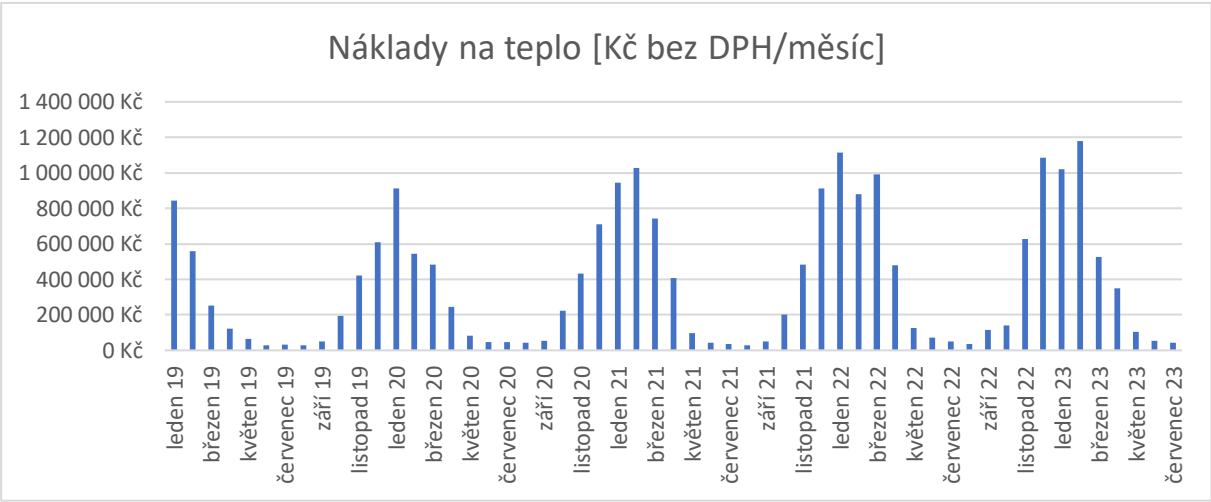
Obr. 11. Spotřeba stlačeného vzduchu ve slévárně v letech 2019 - 07/ 2023.



Obr. 12. Náklady na stlačený vzduch ve slévárně v letech 2019 - 07/ 2023.



Obr. 13. Spotřeba nakupovaného tepla ve slévárně v letech 2019 - 07/ 2023.



Obr. 14. Náklady na nakupované teplo ve slévárně v letech 2019 - 07/ 2023.

4. ZÁVĚR

Tento příspěvek ukazuje žalostný stav nejen českého slévárenství, ale i českého průmyslu, který víceméně likviduje energetická krize v souvislosti s politikou EU a ČR. Pokud vezmeme v potaz, že slévárny měli na odlitcích zisk řádově v desetinách procent z důvodu velké konkurence v Turecku, Indii a Číně a de facto konkurovali pouze kvalitou odlitků a snazší logistikou (rychlejší dobou dodání). Tak tyto růsty nákladů o stovky procent již nepřežila řada sléváren. Slévárny jsou zde tlačeny do situace, kdy se musí rozhodnout, zda zakázku splní a pokouší se jednat o ceně, která bude odlišná např. od smluvně sjednané z roku 2021 – to lze dělat tím, že se stanovuje tzv. energetická přirážka – kterou však zákazník nemusí akceptovat.

Nebo budou realizovat druhou cestu, že přestanou vyrábět a počkají na stabilizované prostředí, kdy ceny energií ještě trochu klesnou, a to i za cenu, že zaměstnancům bude vyplácena náhrada za překážku v práci ze strany slévárny. Těmito cenami energií jsou konkurenceschopnější slévárny v Rakousku, Německu, Švýcarsku, kde je výrazně dražší pracovní síla, ale jsou tam levnější energie či existuje alespoň nějaká podpora průmyslu ze strany státu.

Zde uvedeme příklad uvedený v tisku - Otto Daněk, místopředseda Asociace exportérů ČR uvedl i jeden konkrétní příklad, přímo z firmy, kterou řídí (ATAS Elektromotory, Náchod). „Vyrábíme motory k přepravním kontejnerům. A tam je jeden speciální litinový štít, který váží zhruba jeden kilogram. Slévárenství je poměrně náročná disciplína, kde mají veliký podíl na nákladech energie.“ „Na výrobu tohoto štítu jsme oslovili šest dodavatelů: několik z Německa, ze Švýcarska a také z Česka. A světe div se – nejlevnější byly nabídky z Německa. Pak ze Švýcarska a až jako šestý, nejdražší, se umístil český výrobce. Když jsme s ním tuto situaci konzultovali, řekl nám, že musí do ceny promítnout obrovský podíl energetických nákladů. Pokud by nezdražil, skončil by. A nám nezbylo nic jiného, než kvůli ceně vybrat dodavatele z Německa,“ popisuje Otto Daněk [9].

V současné době tedy musím konstatovat na základě výše uvedeného, že české slévárenství je z důvodů vysokých energetických nákladů zcela nekonkurenceschopně, nejen v Asii, ale už i v EU a bohužel to směřuje k velmi smutnému konci, že místo několika desítek sléváren, které v ČR byly, tu zůstane pouze pár nejsilnějších sléváren (kterých budou maximálně jednotky). Toto je však zdrojem velkého rizika jak pro ekonomiku, tak i pro bezpečnost státu. Pokud by došlo k úpadkům sléváren, je velká pravděpodobnost, že provozy již nebudou obnoveny a nemohly by se podílet na řadě zakázek např. pro armádu (z toho důvodu je to i velké bezpečnostní riziko).

K dalšímu snižování konkurenceschopnosti a de facto „postupné likvidaci“ sléváren přispívají „úniky z informací z připravovaného „ozdravného konsolidačního balíčku“, kdy se uvažuje o zrušení osvobození od ekologické daně, které je zavedeno pro energeticky náročné provozy a obnoveným platbám za OZE, které povedou k dalšímu zvýšení nákladů na energie v řádech miliónů Kč. [10].

Poděkování: Tento příspěvek vznikl za podpory SGS22/155/OHK2/3T/12 Aditive technology and simulation processes in sphere of manufacturing technology.

LITERATURA

[1] EON. Cena elektřiny za kWh opět zdražila. V roce 2020 stojí 4,76 Kč. Online. In: *Elektřina.cz.* https://www.elektrina.cz/cena-elektriny-za-kwh-2020-cez-eon-pre-bohemia-centropol-a-dalsi.

[2] HIRTH, L. Trh s elektřinou neselhal, funguje správně. Jak tedy vzniká cena elektřiny? In: *Podnikatel.cz - největší server pro podnikatele v ČR*. https://www.podnikatel.cz/clanky/trh-s-elektrinou-neselhal-funguje-spravne-jak-tedy-vznika-cena-elektriny/#h20.

[3] NOVINKY. Slovakia Energy na Slovensku končí. In: *Novinky.cz* - nejčtenější zprávy na českém internetu. https://www.novinky.cz/clanek/ekonomika-slovakia-energy-na-slovensku-konci-40373533.

[4] BOHEMIA ENERGY. Skupina Bohemia Energy ukončuje dodávky elektřiny a plynu: *Tisková zpráva*. https://bohemiaenergy.cz/data/TZ_Bohemia_Energy.pdf.

[5] ERU. ERÚ prověřuje dodavatele energií a jejich schopnost dostát závazkům vůči spotřebitelům. In: *Energetický regulační úřad | eru.cz*. https://www.eru.cz/eru-proveruje-dodavatele-energii-a-jejich-schopnost-dostat-zavazkum-vuci-spotrebitelum.

[6] E15. Záhadné zničení plynovodu Nord Stream: motiv měli Američané, Rusové i Ukrajinci. In: *e15.cz - Byznys, politika, ekonomika, finance, události*. https://www.e15.cz/byznys/prumysl-a-energetika/zahadne-zniceni-plynovodu-nord-stream-motiv-meli-americane-rusove-i-ukrajinci-1397121.

[7] ČR. PXE - Zemní plyn denní graf komodita, ke stažení SVG, PNG. In: *Kurzy měn, akcie, komodity, zákony, zaměstnání - Kurzy.cz* | Kurzy.cz. https://www.kurzy.cz/graf-komodita/pxe-zemni-plyn-eur-png-svg-5let.

[8] ČR. Elektřina denní graf komodita, ke stažení SVG, PNG. In: *Kurzy měn, akcie, komodity, zákony, zaměstnání - Kurzy.cz* | Kurzy.cz. https://www.kurzy.cz/graf-komodita/cena-elektriny-eur-png-svg-5let.
[9] IDNES. Exportér: Proč s námi nejednáte, pane premiére? Hrozí ekonomická katastrofa: Rozstřel. In: *iDNES.cz – s námi víte víc*. https://www.idnes.cz/ekonomika/domaci/otto-danek-exporteri-premier-fiala-dopis-ekonomicka-katastrofa.A230924_103604_ekonomika_vov.
[10] SEZNAM. České kovy podraží. Železárny a slévárny přišly o výjimku z ekologické daně. In: *Seznam Zprávy*. https://www.seznamzpravy.cz/clanek/ekonomika-firmy-konsolidacni-balicek-vyjimka-metalurgie-231126.

BEZPEČNOST VÝROBY, SKLADOVÁNÍ A APLIKACÍ VODÍKU

SAFETY OF PRODUCTION, STORAGE AND APLICATIONS OF HYDROGEN

Dalibor Jeřábek, Viktor Kreibich

ČVUT v Praze, Fakulta strojní, Technická 4, 166 07 Praha 6; dalibor.jerabek@fs.cvut.cz

Abstrakt: S rostoucí světovou populací, která je každým rokem bohatší, rostou také požadavky na její energetickou spotřebu. Vzniká tak silná motivace najít čisté alternativní palivo, či nositele energie, který by zastoupil roli fosilních paliv, ve světovém energetickém mixu. Vodík se jeví jako slibný kandidát, neboť jeho produkce i zpětná přeměna nemají žádné lokální emise skleníkových plynů. Potenciální problém však nastává při zmírňování rizik vodíku a jeho nešťastné reputaci ve veřejné sféře, z důvodu historických neštěstí. V tomto příspěvku budou rozebrána rizika při produkci, skladování, transportu a koncové spotřebě vodíku. Rizika vyvolávají dopady spojené se zapálením a hořením, které jsou způsobeny vlastnostmi jako: široké pásmo výbušnosti, nízká zápalná teplota, vysoká rychlost spalin, rychlé rozptýlení a vzlínání v kapalné fázi.

Klíčová slova: Vodík, riziko, zdroje rizik, vodíková ekonomika, bezpečnost vodíkových systémů.

Abstract: As the world's population grows, and gets richer every year, so do the demands on its energy consumption. This creates a strong motivation to find a clean alternative fuel, or an energy carrier that would replace the role of fossil fuels, in the world's energy mix. Hydrogen appears to be a promising candidate, as both its production and conversion have no local greenhouse gas emissions. However, a potential problem arises in mitigating the risks of hydrogen and its unfortunate reputation in the public sphere, due to historical mishaps. In this paper, the risks in the production, storage, transport and final consumption of hydrogen will be discussed. Risks are caused by the impacts associated with ignition and combustion, which are caused by properties such as: wide explosion band, low ignition temperature, high flue gas velocity, rapid dispersion and capillary action in the liquid phase.

Keywords: Hydrogen, risk, risk sources, hydrogen economy, safety of hydrogen systems.

1. ÚVOD

Poptávka po energii nadále eskaluje. Fosilní paliva, která jsou převážným zdrojem uspokojujícím tuto potřebu, jsou neobnovitelná a při spalování vylučují skleníkové plyny a další polutanty. Tato nesnáze proto podnítila neúnavné hledání ekologických a energeticky účinných alternativních paliv. Každý zdroj energie má svoje vrozené nedostatky. Obnovitelné zdroje, jako větrná, sluneční a přílivová energie, narážejí na skutečnost, že závisí na chování přírodních zdrojů, které jsou proměnné, což zapříčiňuje období energetického nedostatku, a naopak energetického přebytku. Na druhou stranu, neobnovitelné zdroje jsou konečné, a mají velký dopad na životní prostředí.

Celosvětová iniciativa nahradit fosilní paliva alternativními zdroji energie nabírá na hybnosti. Tento fakt je silně podpořen rychlým technologickým posunem v tomto odvětví. Hlavními tahouny alternativních systémů produkujících čistou energii jsou geotermální, nukleární, solární, vodní a větrné zdroje energie. Prvořadá kritéria podmiňující ideální palivo zahrnují udržitelnost, minimální dopad na životní prostředí, spolehlivost a nezávislost na externích činitelích, např. geopolitice nebo ročnímu období [1]. Vodík v rámci těchto kritérií představuje velice slibné řešení [2,3]. Vhodnost vodíku je hodnocena na globální úrovni a jeho implementací je slibována zelená substituce látek jako benzin, nafta, topný olej, zemní plyn a mnoho dalších paliv jak v dopravním odvětví, tak v průmyslu [1,2]. Vodík představuje zdroj, který ho předurčuje pro budoucí širokosáhle využívání. Těmito vlastnostmi univerzálnost, energetická účinnost, celkově nízký emisní profil a jeho obnovitelná nátura. Má tak potenciál fungovat jakožto nositel energie, který v případě správného technologického řešení dosahuje vysoké efektivity a zároveň prakticky nulové lokální emisní zátěži [3].

Čistý vodík se však v přírodě prakticky nevyskytuje. Je tak nutné ho vyrábět energeticky velmi náročnými procesy [4]. Jakmile je vodík vyroben, funguje jakožto nositel energie, která je později přeměňována na užitečnou energii v místě a času potřeby, například v cyklu spalovací plynové turbíny. Nicméně bezpečnost vodíkové ekonomiky není ještě plně zaručena [5,6]. Primární překážka rozšíření vodíku do širokého využívání se týká bezpečnostních aspektů, které zahrnují výrobní a skladovací zařízení [7,8], jakožto i různé další aplikace, včetně paliva pro osobní

vozidla a použití v domácnostech. Dopady rizik spojených s využitím vodíku lze kategorizovat následovně [11,12]:

1. Fyziologické (omrzliny a udušení).
2. Fyzikální (křehkost a selhání součástí).
3. Chemické (hoření, výbuch), přičemž primárním nebezpečím je neúmyslné vytvoření hořlavé nebo výbušné směsi se vzduchem [9].

Zatímco vodík se používá pro komerční a průmyslové účely již více než století, jako jsou rafinérie, chemické procesy a raketové pohony, jeho historie zahrnuje i nehody s významnými ekonomickými a společenskými důsledky. Mezi tyto incidenty patří např.: katastrofa Hindenburgu v New Jersey v roce 1937, únik vodíku při údržbě v Houstonu v roce 1989, prasknutí tlakové nádrže na vodík ve Frankfurtu v roce 1991 a výbuch nakumulovaného vodíku v Hirošimě 2011 [6,10,11]. Katastrofické události jsou obvykle připisovány dále uvedeným příčinám:

1. Mechanické selhání technického zařízení.
2. Korozní selhání technického zařízení.
3. Přetlakování technického zařízení.
4. Zvýšená křehkost tlakových nádob za nízkých teplot.
5. Exploze výparů expandující vroucí kapaliny (BLEVE).
6. Porušení technického zařízení v důsledku tlakových vln a rychle se pohybujících objektů z blízkých explozí.
7. Lidský faktor.

Bezpečné zacházení s vodíkem musí zvažovat jeho specifické vlastnosti [12]:

1. Samovolný únik molekul vodíku v důsledku jejich velikosti.
2. Nízká zápalná energie vodíku a široký rozsah explozivnosti směsi vodíku s kyslíkem.
3. Nižší hustota než vzduch.
4. Schopnost působit křehkost kovů.

Vodík má nejširší výbušné/zápalné pásmo ze všech plynů, až na acetylen, při smíchání se vzduchem [13]. Tento nebezpečný faktor je však minimalizován vysokou těkavostí vodíku, v důsledku které se velice rychle rozptýlí do okolního prostředí, a tím se sníží riziko zažehnutí. Pokud tedy nedojde k úniku vodíku v uzavřeném a neventilovaném prostředí, je jeho dopad zpravidla neškodný. Při porušení nádoby skladující vodík tak dochází k rychlému rozptýlení vodíku do okolního prostředí a rapidnímu snížení jeho koncentrace pod výbušnou hranici. V případě zahoření vodíku, jsou jeho plameny na denním světle velice těžko viditelné [14]. Závěrem zmíněných informací tak je:

1. Vodík je potenciálním řešením energetické krize, která je na horizontu v důsledku upozaďování fosilních paliv, a naší současné neschopnosti efektivně skladovat přebytečnou energii z obnovitelných zdrojů.
2. Vodík je ekonomicky výhodnou a environmentálně čistou alternativou, přes jeho nebezpečnou historii.
3. Při správném pochopení rizik spojených s používáním vodíku a jejich důslednému respektování, lze provozovat funkční a bezpečné systémy.

V posledních letech jsme svědky intenzivního výzkumu zaměřeného na vytvoření bezpečnostních předpisů a databází [15], bezpečnostních programů [16], výroby na bázi elektrolýzy [17] a demonstračních zařízení [18]. Tyto iniciativy podnítily vznik celé řady modelových a simulačních studií zaměřených na bezpečnost vodíku [19]. V důsledku toho se aplikace rozšířily tak, že obsahují požadavky důležité pro bezpečnost při výrobě [20], skladování [21], a úniku [20,22-24]. Posuzování bezpečnosti se provádí s ohledem na dopady havárií [11,14] na:

- životní prostředí [25],
- budovy [26],
- čerpací stanice [27]
- a především na vozidla a pozemní dopravu [28].

Budoucnost energetiky slibuje využití vodíku ve spojení s palivovými články pro výrobu energie a dopravní sektor. Výzkum bezpečnosti v těchto aplikacích proto nabývá mimořádného významu [29]. Senzorika hraje klíčovou roli

při zajištění bezpečnosti systémů závislých na vodíku [30], a je tak zásadní pro nastolení bezpečné vodíkové ekonomiky [31].

2. DOPADY RIZIK SPOJENÝCH S UŽÍVÁNÍM VODÍKU

Dopady rizik vodíku na živé organizmy jsou: udušení; zranění tlakem a popáleniny. Udušení nastává při přítomnosti molekul H_2 nebo jiného netoxického plynu rozptýleného v takové koncentraci, kdy vytlačuje, a tak redukuje, objemovou koncentraci kyslíku v atmosféře pod hranici 19,5 % [32]. Zranění tlakem nastává nejčastěji v důsledku tlakové vlny způsobené explozí. Vůči tlakové vlně jsou nejnáchylnější jemné tkáně, nevíce plíce a střední ucho. Rázová změna tlaku nad hranicí 0,7 atm po dobu 50 ms, nebo 1,4-2 atm po dobu 3 ms je dostatečná pro potrhání plic [32]. Tepelné poškození tkáně v důsledku sálavého tepla emitovaného hořením H_2, je přímo úměrné době vystavení tkáně, intenzitě hoření, teplotě hoření, ploše hoření, intenzitě větru a atmosférické vlhkosti. Již při nízké energii záření 0.95 $W*cm^{-2}$ dojde za přibližně 30 s k popálení kůže. Kryogenické omrzliny mohou nastat při kontaktu s unikajícím kapalným vodíkem, který je zkapalňován za teploty -253 °C [32].

Dopady rizik vodíku na materiály jsou v tom, že působí křehkost kovových nádob v případě stlačeného vodíku nebo kombinace křehkosti kovových nádob, kterou způsobuje vodík a velmi nízké teploty v případě kapalného vodíku, které je častou příčinou selhání vodíkové infrastruktury. Intenzita zkřehnutí materiálu je závislá na teplotě, tlaku, vnitřní čistotě a množství vad kovu, délce vystavení vodíku a povrchovým vlastnostem [33]. Atmosférická vodíková křehkost je nejintenzivnější v rozsahu teploty 200–300 K. Její intenzita je však kontrolovatelná pomocí oxidických povlaků, aditiv přidávaných do vodíku, správnou selekcí konstrukční slitiny a minimalizací napěťových koncentrátorů [33]. Tepelná roztažnost použitých materiálů musí být taktéž zohledněna pro účinné zabránění únikům vodíku při kryogenických teplotách. Smrštění kovů při 20 K (teplota tekutého vodíku) je méně jak 1 %. Pro srovnání plasty podléhají smrštění v rozmezí 1-2,5 % [33].

Další dopady rizik vodíku jsou spojené s jeho chemickými vlastnostmi – hořlavost a výbušnost. Hranice hořlavosti je závislá na zápalné energii látky, teplotě, tlaku a obecném charakteru okolního prostředí. Kapalný vodík, společně s tekutým nebo pevným kyslíkem, mohou explodovat v důsledku tlakové vlny [32]. Zápalná energie vodíku na atmosféře je velice malá (0,02 mJ) [32]. Z toho důvodu je stěžejní perfektně izolovat otevřený oheň a elektrická či topná zařízení v budovách, oplývajících vodíkovými systémy. Exploze se vyznačují rychlým uvolněním energie, které je doprovázeno vznikem tlakových vln. Naproti tomu deflagrace je definována přítomností fronty plamene, která postupuje hořlavou směsí jako podzvuková vlna. Exploze oproti deflagraci zahrnuje frontu plamene spojenou s rázovou vlnou, která se šíří výbušnou směsí v podobě nadzvukové vlny. Tlaková vlna se šíří rychlostí tisíckrát vyšší než počáteční reakce, takže je ve srovnání s deflagrací nebezpečnější a potentnější způsobovat zranění a škody [34].

Energeticky nejvýbušnější směs vodíku a kyslíku se nachází okolo stochiometrického poměru (při daném poměru H_2 a vzduchu má směs energii ekvivalentní výbuchu 2/3 stejného množství TNT [35]), nicméně přirozeně tento výskyt není častý. V případě vodíku (H_2) je však rozsah koncentrace vodíku a kyslíku široký. Výbuch je tak reálným rizikem, čímž se zvyšuje pravděpodobnost závažnější nehody [36]. Hranice explozivnosti však závisí na různých faktorech, včetně povahy uzavřenosti prostoru a rozsahu úniku v daném prostoru.

Po zhodnocení jednotlivých faktorů je zřejmé, že:

1. Hořlavé vlastnosti vodíku poukazují na jeho obtížnou manipulaci, nicméně ruku v ruce s tím na jeho slibný energetický potenciál.
2. Vodík je nejmenší prvek, což vede k problematice vysoké difuzivity, rizikům úniků a s tím spojeným rizikem zahoření či exploze.
3. Vznětlivost vodíku je funkcí koncentrace v atmosféře, jejíž nebezpečná hranice je nižší než ostatních běžných paliv. Hoření vodíku je také rychlejší, má vyšší teplotu a na denním světle je zároveň obtížně detekovatelné.

3. BEZPEČNOST PRODUKCE VODÍKU

Čistý vodík se běžně nevyskytuje, je proto nutné ho vyrábět. Vodík lze produkovat řadou procesů. Cena za 1 kg vodíku je silně závislá na typu výrobního procesu a způsobu distribuce [37]. Nejlevnější, ale také méně kvalitní vodík, pochází z fosilních paliv. Téměř polovina světového vodíku je vyráběna parním reformováním zemního plynu. Pouze přibližně 4 % světové produkce vodíku pochází z elektrolýzy vodných roztoků. Zanedbatelné množství pak z biologických procesů [38]. Procesy výroby vodíku se dělí na produkci z fosilních paliv a na produkci

z obnovitelných zdrojů. Dále na termální procesy, elektrolytické procesy a biologické procesy. Pro potřebu vodíkových palivových článků je nutné vodík dodatečně čistit, jinak by postupně došlo k otrávení katalyzátoru [1]. Výsledný čistý vodík může sloužit k různým účelům, včetně spalování v plynových turbínách pro výrobu elektřiny, přeměny na elektřinu pomocí palivových článků, využití jako palivo pro spalovací motory, nebo jako důležitá chemická složka při výrobě hnojiv a řady dalších produktů [1]. Elektrolýza vody je rozklad vody (H_2O) na plynný kyslík (O_2) a vodík (H_2) v důsledku průchodu stejnosměrného elektrického proudu vodou. Vodu lze rozkládat i bez použití elektrického proudu. Samovolně se rozkládá při teplotě přibližně 2 500 °C, ale tato teplota je příliš vysoká pro praktické využití v průmyslu [38]. Ke snížení teploty disociace na 800 °C jsou zapotřebí katalyzátory (nejúčinnější ze skupiny platinových kovů) [38].

Bezpečnost uvedených procesů výroby vodíku je v současné době upravena řadou národních i nadnárodních norem [39-46].

4. BEZPEČNOST SKLADOVÁNÍ VODÍKU

Účinné skladování vodíku hraje klíčovou roli při implementaci vodíkové ekonomiky. Pro dosažení optimální energetické účinnosti je nezbytné minimalizovat spotřebu energie v každé fázi procesu, včetně výroby, skladování a přepravy.

Po přemístění plynného vodíku potrubím z míst s pravidelným nadbytkem elektrické energie, vzniknou požadavky na jeho hromadné skladování, v různých distribučních centrech. V současné době je pro velkoobjemové skladování vodíku využíváno nejčastěji skladování v kapalné formě (LH_2) v izolovaných nádobách [47]. Skladování v kapalném stavu je energeticky náročný proces. Při zkapalňování se spotřebuje přibližně 1/3 celkové energie uložené ve vodíku [5]. Obecně vzato lze říci, že skladování vodíku pod tlakem je ekonomicky výhodnější (cca 9 % energie vodíku pro stlačení na 200 bar [5]) ale nebezpečnější jak v kapalné podobě. Zároveň dochází k jevu zvanému „boil-off“ při kterém je vlivem nedokonalé izolace nádoby vodík ohříván, a tak dochází k nárůstu tlaku v nádobě. Vzhledem k tomu, že kryogenní nádoby nejsou dimenzovány pro odolávání vnitřnímu tlaku, je nutné vodíkové výpary ventilovat, aby nedošlo k poškození nádoby. Takto skladovaný vodík o vysoké čistotě se nejčastěji používá pro potřeby chemického průmyslu, nebo jako palivo vesmírných raket [12].

Jeden kilogram stlačeného vodíku má při atmosférickém tlaku a teplotě objem 11 000 l [31]. Proto je nutné vysoké komprese za účelem efektivní skladování pro potřeby automotive. Z pevnostního hlediska přichází v úvahu vysokopevnostní ocel, austenitická ocel nebo jiné kovy. Ty však, pro potřeby automotive, mají nepříznivý poměr mezi váhou a pevností a zároveň podléhají vodíkové křehkosti, vlivem difuzivity vodíku. V praxi se tak používají speciální kompozitní nádoby, skládající se z polymerního, nebo hliníkového výstelu, který zamezuje úniku vodíku, a kompozitního uhlíkového obalu, který je schopný odolat tlaku vodíku až o hodnotě 1000 bar [48].

Skladovat 5 kg CH_2 při tlaku 700 bar vyžaduje objem 125 l [48], což je více než nádrž běžných vozidel, nehledě na váhu celého systému, který musí odolat vysokému tlaku a dekompresi před přivedením vodíku do vodíkového článku. Současnou výzvou v oblasti CH_2 je vyvinout konformní tlakové nádoby, které mohou optimalizovat prostor ve vozidlech FCV. Kromě toho bude v budoucím vývoji kladen důraz na další snižování nákladů a nižší hmotnost. Celková energie využitá při skladování CH_2 je nejnižší ve srovnání s LH_2, kovovými hydridy a všemi ostatními metodami skladování [9]. Srovnání metod skladování vodíku pro palubní účely je patrné v tabulce 1.

Tabulka 6. Srovnání palubních metod skladování vodíku [49].

Palivo	Celková energie (MJ)	Objem (l)	Hmotnost paliva (kg)	Hmotnost nádoby (kg)	Celková hmotnost systému (kg)
Benzín	662	19	14	6,4	20,4
Tekutý H_2	662	178	4,7	18,6	22,3
H_2 v FeTi kovovém hydridu	662	189	4,7	549,3	554
Stlačený H_2 (207-690 bar)	662	409-227	4,7	63,6-86,3	68,3-91

Za normálních podmínek je vodík bezbarvý plyn bez zápachu, čtrnáctinásobně lehčí než vzduch. Nízká hustota ve spojení s malou velikostí částic umožňuje rychlejší difuzi molekul vodíku do některých kovů a slitin, jako je litina a ocel s vysokým obsahem uhlíku [19]. Průnik může skončit malými úniky vodíku nebo v případě přítomnosti

mikrotrhlin, nebo jiných defektů ve struktuře, ve kterých se vodík koncentruje, snížením pevnosti materiálu a následným lomem. Vodík prudce reaguje s oxidačními činidly, jako je oxid dusný, halogeny (zejména s fluorem a chlorem) a nenasycenými uhlovodíky (např. acetylenem), přičemž dochází k intenzivním exotermickým reakcím. Vodík není toxický, avšak kromě nebezpečí bleskového požáru, či výbuchu, může vodík při dostatečně vysokých koncentracích působit jako dusivý prostředek tím, že vytlačí kyslík dostupný v atmosférickém vzduchu [50]. Proto:

1. Skladování je po technické stránce jedním z největších problémů spojeným s vodíkem.
2. Nebezpečí při skladování se týkají především úniku a větrání, které mohou vést k mísení vodíku se vzduchem.

5. BEZPEČNOST PŘEPRAVY VODÍKU

Pro přepravu vodíku je nezbytné zohlednit jak bezpečnostní, tak ekonomickou stránku věci. Existují tři základní možnosti přepravy vodíku [1]:

1. Pro přepravu plynného vodíku, včetně přepravy směsi vodíku a zemního plynu, je vhodné použití potrubí a cisternových vleků.
2. Další možností je využití nákladních automobilů, železnic, a lodí vybavených kryogenními nádržemi pro přepravu zkapalněného vodíku.
3. Třetí přístup zahrnuje využití chemických nositelů s vysokou energetickou hustotou, jako je etanol, metanol a další kapaliny získané z obnovitelné biomasy. Tyto nositele lze přepravovat a následně reformovat na vodík v místě použití.

Oblast přepravy vodíku se stále vyvíjí a výběr metod závisí na mnoha faktorech. I nadále je však nezbytné, aby vybrané technologie přepravy vodíku za všech okolností upřednostňovaly bezpečnost, dále ekonomickou stránku a s ní spojenou energetickou účinnost [51].

Pro přepravu vodíku ve velkých množstvích na delší vzdálenosti jsou ideální potrubní sítě [52]. Tato preference vyplývá především z inherentní bezpečnosti tohoto systému, zejména při použití malých průměrů a provozu při trvale nízkých tlacích [53]. Je však třeba poznamenat, že přenos vodíku potrubím vyžaduje podstatně vyšší energetický příkon pro provoz kompresorů. Kromě toho může použití běžných kompresorových maziv představovat problém s kontaminací, která může být považován za nepřijatelnou pro využití palivových článků. Proto je naléhavě zapotřebí vyvinout spolehlivější, energeticky účinnější a obecně levnější kompresní technologie přizpůsobené specificky pro poháněnní stlačeného vodíku [51].

Vliv povrchu materiálu, který přichází do styku s vodíkem, například oxidická vrstva, nebo povlak (např. sklokeramický) lze testovat pomocí testu propustnosti vodíku [54]. Ten napomáhá výzkumu a spolehlivé volbě vhodného bariérového materiálu, minimalizujícího nepřijatelné efekty difuze vodíku.

Křehkost materiálů způsobená vodíkem, tzv. vodíková křehkost (VK) je dobře zdokumentovaný jev pozorovaný u vysoko pevnostních materiálů [55]. VK je zodpovědná za podkritické šíření trhlin v materiálech, které iniciuje lomy a vede ke katastrofickým poruchám, což v konečném důsledku vede ke ztrátě základních mechanických vlastností, jako je tažnost, houževnatost a pevnost. Materiály s vysokou pevností jsou obecně velmi náchylné ke křehnutí vodíkem, jsou-li vystaveny prostředí bohatému na vodík [53]. Mezi materiály náchylné k VK patří mimo jiné vysoko pevnostní oceli, oceli s vysokým obsahem manganu, slitiny hliníku, titanu, hořčíku a slitiny hořčíku [38].

Zvláště náchylné k VK jsou oceli s pevností vyšší než 1000 MPa [37]. Tyto vysokopevnostní oceli nacházejí uplatnění v různých odvětvích, mimo jiné v leteckém a kosmickém průmyslu, jaderném průmyslu, vysokotlakých zásobnících vodíku, dopravním průmyslu a automobilovém průmyslu.

K náchylnosti materiálu k vodíkové křehkosti přispívá několik faktorů [56]:

1. Pevnost materiálu a zbytkové napětí: Vnitřní pevnost materiálu a případná zbytková napětí v něm.
2. Tlak, teplota a doba expozice: Podmínky prostředí, včetně tlaku, teploty a doby expozice.
3. Aplikovaná míra deformace a stav povrchu: Rychlost, s jakou se na materiál působí deformace, a stav jeho povrchu.
4. Koncentrace vodíku a místa zachycení: Koncentrace vodíku a přítomnost míst zachycení vodíku v materiálu.

5. Kovové povlaky a sraženiny: Existence kovových povlaků a specifických precipitátů v materiálu.
6. Mikrostruktura materiálu: Mikrostrukturní charakteristiky materiálu.
7. Chemie roztoku: Vlastnosti roztoků, které přicházejí do styku s kovy, zejména kyselých roztoků.
8. Tepelné zpracování: Tepelné zpracování: Procesy tepelného zpracování, které se na materiál aplikují.

Tolerance opotřebení potrubí je funkcí mechanického zatížení, druhu materiálu a tlaku vodíku [57]. Vzhledem k podobnosti s již průmyslově zažitým odvětvím transportace zemního plynu, lze problematiku řešit pomocí běžných postupů využívajících lomovou mechaniku. Existují výzkumné a vývojové programy, které se specializují na tenké bariérové povlaky, minimalizující difuzi vodíku do stěn potrubí, při transportu zemního plynu. Na vývojové poznatky tohoto odvětví lze dobře navázat s ohledem na potřeby transportu čistého vodíku. Výzkum probíhá také v odvětví metalurgie ocelových slitin a s nimi spojeným svařováním. V rámci něho jsou vyvíjeny nové druhy plněných přídavných drátů, specificky pro svařování potrubí čerpající vodík za vysokého tlaku [52].

Přeprava kapalných a plynných paliv s sebou neodmyslitelně nese riziko, jehož příčinou jsou jejich úniky. Vodík je čirý a bez zápachu, lidskými smysly je tak prakticky nezjistitelný, což stěžuje jeho brzkou detekci [58]. Běžným způsobem, jak tento problém řešit, je přidat do plynu pachové látky, které člověku umožní zaregistrovat únik. Běžné pachové látky však nejsou pro vodík vhodné, protože vzhledem k vysokému nepoměru velikosti molekul vodíku a pachové látky, mají velmi rozdílné proudové vlastnosti, a tak se ve vodíku nedokážou homogenně rozptýlit. Dochází tak postupně k segregaci a nepříznivému dvoufázovému proudění. Pachová látka navíc působí jako kontaminant palivových článků. V důsledku toho může použití odorantů pro odorizaci plynného vodíku představovat značnou výzvu [59].

Z výše uvedeného důvodu potrubní infrastruktura vyžaduje začlenění senzorů určených k detekci úniků vodíku. Jsou vyvíjeny levné a spolehlivé senzory vodíku, včetně technologií, jako je detekce úniku pomocí optických vláken [58]. Tyto senzory musí vykazovat vysokou citlivost a rychlou odezvu, aby umožnily včasnou detekci úniku a zajistily, že bude možné přijmout nezbytná opatření dříve, než směs vodíku a vzduchu dosáhne výbušné úrovně. Použití senzorů s optickými vlákny je slibné, protože dobře odpovídá cílům rychlé, spolehlivé a nákladově efektivní detekce.

Souhrnně lze říci, že v budoucnu převládající metodou přenosu vodíku bude potrubí. V důsledku jeho vlastností je nutná správná volba materiálu a povrchové úpravy, které budou přicházet do kontaktu s vodíkem. Dále musí být precizně provedené svarové spoje pro zajištění bezpečného a dlouhodobého provozu. Nedílnou aplikací pro zajištění bezpečnosti je využití senzorů pro rychlou identifikaci případných úniků vodíku [59].

6. BEZPEČNOST APLIKACE VODÍKU

Jedním z hlavních využití vodíku v blízké budoucnosti bude palivo pro osobní a logistickou dopravu. Benzín je z vybraných paliv tím nejjednodušeji skladovatelným palivem vzhledem k jeho vyššímu bodu varu, tím spojené nižší volatilitě a vyšší potřebnou energii pro zahoření. Nicméně vodík i methan (hlavní složky zemního plynu) mohou být již se současnými technologiemi bezpečně skladovány. Vodík v průmyslu byl a je bezpečně skladován ve stlačené, nebo zkapalněné formě. V současné době studované a rozvíjející se odvětví, řešící skladování vodíku v kovových hydridech, otevírá potenciálně ještě bezpečnější přístup. Bezpečnost vodíku v průmyslu byla ověřena časem, nicméně v okamžik masového rozšíření vodíku je nutné brát v potaz rizika plynoucí z kontaktu běžného spotřebitele s těmito technologiemi [60].

Vodík má slibné předpoklady pro využití jako palivo pro dopravní prostředky. Je proto důležité zkoumat rizika, pramenící z velkého množství pohybujících se tlakových nádob po silnicích. Je tak dobré zkoumat vozidlo ve všech možných stavech, tedy pojízdné, nepojízdné a v kolizi. Potenciální rizika dopravního prostředku jsou vztahována k pravděpodobnostem zahoření, exploze nebo toxického úniku. Toxicitu lze v případě vodíku úplně vyloučit, neboť vodík ani jeho spaliny nejsou toxické. Riziko vzniku nekontrolované exotermické reakce hrozí v případě selhání tlakové nádrže na vodík (vlivem výrobní vady, kolize, opotřebení atd.), vodíkového palivového článku a při nevhodném zacházení při tankování.

Na základě různých studiích, např. [59], bylo provedeno komplexní posouzení rizik s cílem analyzovat nejpravděpodobnější nebo nejzávažnější scénáře vodíkových havárií. Tyto scénáře zahrnují požáry nebo výbuchy palivových nádrží v otevřených prostorách a tunelech, úniky z potrubí ve venkovních prostorách a garážích a také havárie na čerpacích stanicích. Studie [11-18] uvádí následující závěry:

1. Dobře navržené vozidlo s vodíkovými palivovými články by mělo vykazovat vyšší úroveň bezpečnosti při kolizích na volném prostranství ve srovnání s vozidly na zemní plyn nebo benzin.
2. Při srážkách v tunelech by měla být vozidla vodíkovými palivovými články i vozidla na zemní plyn podobně bezpečná, přičemž obě by měla být bezpečnější než vozidla na benzin nebo propan.
3. Největší riziko vzniká v případě úniku vodíku v garáži bez řádného větrání, což by mohlo potenciálně vést k požáru nebo výbuchu.

Souhrnně lze říci, že vodík jako dopravní palivo vykazuje jak podobnosti, tak rozdíly ve srovnání s jinými palivy, přičemž některé faktory závažnost nehod zvyšují, zatímco jiné ji zmírňují. Proto stále není jednoznačné, zda je přeprava vodíku ze své podstaty nebezpečnější nebo bezpečnější než jiné alternativy. Dlouhá a bezproblémová historie nákladních vozidel přepravujících stlačený a zkapalněný vodík ve Spojených státech poskytují jistotu, že s používáním vodíkového paliva nejsou spojena žádná neznámá rizika. Navzdory názorům veřejnosti může být využívání vodíku jako paliva v dopravě v určitých aspektech bezpečnější než benzin nebo zemní plyn [32]. V důsledku toho lze obecně konstatovat, že:

1. Benzín je považován za jednodušší a možná i bezpečnější pro skladování ve srovnání s vodíkem a metanem, a to z důvodu vyššího bodu varu, nižší těkavosti a užšímu rozmezí hořlavosti a výbušnosti.
2. Hlavním nebezpečím v případě netěsných nebo prasklých nádrží ve vozidlech je možnost vzniku požáru. Vždy existuje riziko, že palivo způsobí požár, zejména pokud plamen není viditelný a rychle se šíří.
3. Ke zmírnění těchto rizik patří preventivní opatření zaměřená na bezpečnost konstrukce s cílem minimalizovat úniky, využití detektorů vybavených odoranty pro detekci úniku a zavedení automatického odpojení baterie, aby se zabránilo vznícení.

Opatření proti možným selháním dle [49] zahrnují následující:

1. Prevence úniků prostřednictvím vhodného návrhu technického zařízení, který respektuje známá rizika. Zavedení účinných konstrukcí, které respektují známá rizika, a tím minimalizují výskyt úniků.
2. Detekce úniku pomocí vhodných detektorů využívajících odoranty. Jde o použití detektorů vybavených pachovými látkami k rychlé identifikaci a signalizaci přítomnosti úniků.
3. Prevence vznícení pomocí automatického odpojení baterie. Jde o zavedení mechanismů, které automaticky odpojí baterii vozidla, aby se snížilo riziko vznícení v případě úniku.

7. ZÁVĚR

V posledních letech došlo v různých sektorech k vzrůstu využití vodíku. Nicméně pro další postup tohoto trendu je nutné dosáhnout obecného přijmutí této technologie veřejností. Zdráhavost pramení z obav ohledně bezpečnosti skladování a celkového využití vodíku. V tomto ohledu je zásadní předvídat potenciální rizika vodíkových systémů, na základě, kterých bude možné definovat bezpečnostní normy. Definované standarty budou sloužit jakožto směrnice dle kterých budou navrhovány a realizovány zaručeně bezpečné systémy.

Tento článek shrnul základní aplikace vodíku v dopravě, energetickém sektoru, jeho skladování a logistiku a bezpečnostní aspekty nakládání s vodíkem. Konečné shrnutí problémů spojených s vodíkovými procesy je následující:

1. ***Fyzikální nebezpečí*** představuje primárně vodíková křehkost, způsobená difuzí vodíku do materiálu, což vede k jeho degradaci a vyšší pravděpodobnosti selhání.
2. ***Chemická nebezpečí*** zahrnují široké rozmezí hořlavosti a výbušnosti vodíku, jeho nízkou zápalnou energii a vysokou rychlost spalin. Vykazuje však pozitivní vlastnosti rychlého rozptýlení do prostoru v případě úniku.
3. ***Fyziologická nebezpečí*** zahrnují riziko udušení, poranění přetlakem, jakož i tepelné a kryogenní popáleniny.
4. ***Skladování vodíku*** s sebou přináší nebezpečí, zejména v souvislosti s vysokou koncentrací výbušné látky na jednom místě. V případě úniku v uzavřeném prostoru a smísením s atmosférickým kyslíkem, vzniká velmi vysoké riziko vznícení.
5. ***Transport vodíku*** potrubím vyžaduje vyšší množství energie ve srovnání se zemním plynem. Mezi nedávné pokroky patří využití vysokotlakých výstupních elektrolyzérů.

6. ***Požadavky na senzory*** vede k vývoji spolehlivých a nákladově efektivních senzorů. Ty jsou nezbytné pro včasnou detekci úniků vodíku.
7. ***Bezpečnost vodíku ve vozidlech*** nabývá zásadního významu, přičemž specifické obavy se týkají požáru, výbuchu a toxicity. Vodík se ukazuje jako bezpečnější než benzín v případě otevřeného požáru.

Poděkování: Článek byl podpořen projektem SGS22/156/OHK2/3T/12 (Vliv povrchových úprav na kvalitu výrobních technologií).

LITERATURA

[1] JEŘÁBEK, D. Výroba a skladování vodíku. *Diplomová práce.* Praha: ČVUT 2023 České vysoké učení technické v Praze. Výpočetní a informační centrum, 2023, 129 p.
[2] RANGA DINESH, K.K.J., X. JIANG, J.A. VAN OIJEN, R.J.M. BASTIAANS, a L.P.H. DE GOEY. Hydrogen-Enriched Nonpremixed Jet Flames: Effects of Preferential Diffusion: Effects of Preferential Diffusion. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 38 (2013),11, pp. 4848-4863. Doi:https://doi.org/10.1016/j.ijhydene.2013.01.171
[3] FROLOV, S., S., MEDVEDEV, V. , BASEVICH, Y., FROLOV, F.. Self-Ignition of Hydrocarbon–Hydrogen–Air Mixtures. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 38 (2013), 10, pp. 4177-4184.
[4] LEE, K.J, KIM, Y. R., BYUN, C. H., LEE, J. T. Feasibility of Compression Ignition for Hydrogen Fueled Engine with Neat Hydrogen-Air Pre-Mixture by Using High Compression. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 38 (2013), 1, pp. 255-264.
[5] OLMOS, F., MANOUSIOUTHAKIS, V. I.. Hydrogen Car Fill-Up Process Modeling and Simulation. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 38 (2013), 8, pp. 3401-3418.
[6] WANG, D., CHEN, S., XU, C., XIANG, W. Energy and Exergy Analysis of a New Hydrogen-Fueled Power Plant Based on Calcium Looping Process. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 38 (2013), 13, pp.5389-5400.
[7] SARKAR, A., BANERJEE, R. Net Energy Analysis of Hydrogen Storage Options. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 30 (2005), 8, pp. , 867-877.
[8] MIRZA, N. R., DEGENKOLBE, S., WITT, W. Analysis of Hydrogen Incidents to Support Risk Assessment. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 36 (2011), 18, pp. 12068-12077.
[9] TOMIZUKA, T.,KUWANA, T., MOGI, T., DOBASHI, R., KOSHI, M. A Study of Numerical Hazard Prediction Method of Gas Explosion. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 38 (2013), 12, pp. 5176-5180.
[10] YU, M. S., MUY, F. QUADER, et al. *Combined Hydrogen, Heat and Power (CHHP) Pilot Plant Design*. ISSN 0360-3199. Elsevier, 2013.
[11] HEIDARI, A., X WEN, J. Flame Acceleration and Transition From Deflagration to Detonation in Hydrogen Explosions. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 39(2014), 11, pp. 6184-6200.
[12] BARTHÉLÉMY, H. Hydrogen Storage–Industrial Prospectives. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 37 (2012), 22, pp. 17364-17372.
[13] MOLKOV, V., SAFFERS, J. B. *Introduction to Hydrogen Safety Engineering*. Hydrogen Knowledge Centre 2011.
[14] SCHEFER, R. W. , KULATILAKA, W. D., PATTERSON, B. D. SETTERSTEN, T. B. Visible Emission of Hydrogen Flames. *Combustion and Flame*. ISSN 0010-2180. 156 (2009), 6, pp. 1234-1241.
[15] MACINTYRE, I. A., TCHOUVELEV, V., HAY, D., WONG, J., GRANT, J., BÉNARD, P. Canadian Hydrogen Safety Program. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 32 (2007), 13, pp. 2134-2143.
[16] GRIGORIEV, S. A., MILLET, P., KOROBTSEV, S. V., POREMBSKIY, V. I., PEPIC, M., ETIEVANT, C., PUYENCHET, C., FATEEV, V. N. Hydrogen Safety Aspects Related to High-Pressure Polymer Electrolyte Membrane Water Electrolysis. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 14, pp. 5986-5991.
[17] APREA, José Luis. Hydrogen Energy Demonstration Plant in Patagonia: Description and Safety Issues. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009),10, pp. 4684-4691.
[18] DUIJM, N., MARKERT, J. F. Safety-Barrier Diagrams as A Tool For Modelling Safety of Hydrogen Applications. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 14, pp. 5862-5868.

[19] BARALDI, D., KOTCHOURKO, A., LELYAKIN, A. et al. An Inter-Comparison Exercise on CFD Model Capabilities to Simulate Hydrogen Deflagrations in A Tunnel. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 18, pp. 7862-7872.
[20] GORENSEK, M. B., W FORSBERG, C. Relative Economic Incentives for Hydrogen from Nuclear, Renewable, and Fossil Energy Sources. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 9, pp. 4237-4242.
[21] JEPSEN, J., VON COLBE, J. M., KLASSEN, T., DORNHEIM, M. Economic Potential of Complex Hydrides Compared to Conventional Hydrogen Storage Systems. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 37 (2012), 5, pp. 4204-4214.
[22] HOUF, W, SCHEFER, R., EVANS, G., MERILO, E., GROETHE, M. Evaluation of Barrier Walls for Mitigation of Unintended Releases of Hydrogen. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 35 (2010), 10, pp. 4758-4775.
[23] YANG, J. C. Material-Based Hydrogen Storage. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 33 (2008), 16, pp. 4424-4426.
[24] RAMAMURTHI, K, BHADRAIAH, K. MURTHY, S. S. Formation of Flammable Hydrogen–Air Clouds from Hydrogen Leakage. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 19, pp. 8428-8437.
[25] GALASSI, M. C., PAPANIKOLAOU, E., BARALDI, D. et al. HIAD–Hydrogen Incident and Accident Database. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 37 (2012), 22, pp. 17351-17357.
[26] VENETSANOS, A.G., PAPANIKOLAOU, E., DELICHATSIOS, M. et al. An Inter-Comparison Exercise on The Capabilities of CFD Models to Predict The Short and Long Term Distribution and Mixing of Hydrogen in A Garage. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 14, pp. 5912-5923.
[27] ZHIYONG, Li, XIANGMIN, P., JIANXIN, M. Harm Effect Distances Evaluation of Severe Accidents for Gaseous Hydrogen Refueling Station. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 35 (2010), 3, pp. 1515-1521.
[28] FARDISI, S., A KARIM, G. Characteristics of Flammable, Buoyant Hydrogen Plumes Rising from Open Vertical Containers. *International Journal of Hydrogen Energy*. ISSN 0360-3199. Elsevier, 34 (2009), 15, pp. 6568-6579.
[29] CAIRNS, J. North American and International Hydrogen/Fuel Cell Standards. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 35 (2010), 7, pp.2767-2771.
[30] BUTTNER, W. J., POST, M. B., BURGESS,m R., RIVKIN, C. An Overview of Hydrogen Safety Sensors and Requirements. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 36 (2011), 3, pp. 2462-2470.
[31] BALL, M., WIETSCHEL, M. The Future of Hydrogen–Opportunities and Challenges. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 2, pp. 615-627.
[32] FARRELL, A. E., W KEITH, D., CORBETT, J. J. A Strategy for Introducing Hydrogen into Transportation. *Energy Policy*. ISSN 0301-4215. 31 (2003), 13, pp.1357-1367.
[33] NASA. *Safety Standard for Hydrogen and Hydrogen Systems*. Washington: Office of Safety and Mission Assurance 1997.
[34] KOTCHOURKO, A. Combustion E Part 2 Deflagration and Explosions. In: *4th International Conference on Hydrogen Safety ICHS*. 2011.
[35] CARCASSI, M. N. ICHS-2005: The First International Conference on Hydrogen Safety: The First International Conference On Hydrogen Safety. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 13 (2007), 32, pp. 2105.
[36] MOLKOV, V. V., SAFFERS, J-B.. *Introduction to Hydrogen Safety Engineering*. Hydrogen Knowledge Centre 2011.
[37] KANNAH, R Y., KAVITHA, S., KARTHIKEYAN, O. P., KUMAR, G. N., Vo DAI-VIE, BANU, J. R. Techno-Economic Assessment of Various Hydrogen Production Methods–A Review. *Bioresource Technology*. ISSN 0960-8524. 319 (2021), 12, pp. 41-75.
[38] NIKOLAIDIS, P., POULLIKKAS, A. A Comparative Overview of Hydrogen Production Processes. *Renewable and Sustainable Energy Reviews*. ISSN 1364-0321. 67 (2017), pp. 597-611.
[39] ISO. *ISO 14687 Hydrogen Fuel – Product Specification*. 2019.
[40] ISO. *ISO 16110-1:2007 Hydrogen Generators Using Fuel Processing Technologies – Part 1: Safety*.
[41] ISO. *ISO 17268:2006 Compressed Hydrogen Surface Vehicle Refuelling Connection Devices*.
[42] ISO. *ISO 22734-1:2008 Hydrogen Generators Using Water Electrolysis Process – Part 1: Industrial and Commercial Applications*.
[43] AIAA . *Guide to Safety of Hydrogen and Hydrogen Systems (G-095-2004e). http://www.AIAA.org*.

[44] EIGA. *IGC Document 122/04 Handbook for Hydrogen Refuelling Station Approval*.
[45] EIGA. *IGC Document 6/02 Safety in Storage, Handling and Distribution of Liquid Hydrogen*.
[46] EIGA. *IGC Document 23/00 Safety Training of Employees*.
[47] RIGAS, F., SKLAVOUNOS, S. Evaluation of Hazards Associated with Hydrogen Storage Facilities. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 30 (2005), 13-14, pp. 1501-1510.
[48] HUA, T. Q., AHLUWALIA, R. K., PENG, J-K., KROMER, M., LASHER, S., MCKENNEY, K., LAW, K., SINHA, J. Technical Assessment of Compressed Hydrogen Storage Tank Systems for Automotive Applications. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 36 (2011), 4, pp. 3037-3049.
[49] NAJJAR, Y. S. H. Hydrogen Safety: The Road Toward Green Technology. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 38 (2013), 25, pp. 10716-10728.
[50] PASMAN, H. J. Challenges to Improve Confidence Level of Risk Assessment of Hydrogen Technologies. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 36 (2011), 3, pp. 2407-2413.
[51] KURTZ, J., SPRIK, S., BRADLEY, H. D. Review of Transportation Hydrogen Infrastructure Performance and Reliability. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 44 (2019), 23, pp. 12010-12023.
[52] ADAMS, T., RAWLS, G., LAM, P-S., SINDELAR, R. Evaluation of Natural Gas Pipeline Materials and Infrastructure for Hydrogen/Mixed Gas Service. *Savannah River National Laboratory*. 2005.
[53] GRASSO, N., PILO, F., CIANNELLI, N., CARCASSI, M. C., MATTEI, N., CECCHERINI, F. Fire Prevention Technical Rule for Gaseous Hydrogen Transport in Pipelines. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 34 (2009), 10, pp. 4675-4683.
[54] BARTH, C. F., STEIGERWALD, E.A., TROIANO, A. R.. Hydrogen Permeability and Delayed Failure of Polarized Martenstic Steels. *Corrosion*. ISSN 1938-159X. 25 (1969), 9, pp. 353-358.
[55] SPATH, P. L., MANN, M. K. *Life Cycle Assessment of Hydrogen Production Via Natural Gas Steam Reforming*. National Renewable Energy Lab.(NREL), Golden, CO (United States), 2000.
[56] DWIVEDI, S. K., VISHWAKARMA, M. Hydrogen Embrittlement in Different Materials: A Review. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 43 (2018), 46, pp. 21603-21616.
[57] OHAERI, E., EDUOK, U., SZPUNAR, J. Hydrogen Related Degradation in Pipeline Steel: A Review. *International Journal of Hydrogen Energy*. ISSN 0360-3199. 43 (2018), 31, pp. 14584-14617.
[58] ZHANG, Y., PENG, H., QIAN, X., ZHANG, Y., AN, G., ZHAO, Y. Recent Advancements in Optical Fiber Hydrogen Sensors. *Sensors and Actuators B: Chemical*. ISSN 0925-4005. 244 (2017), pp. 393-416.
[59] SWAIN, M. R., SHRIBER, J., SWAIN, M. N. Comparison of Hydrogen, Natural Gas, Liquified Petroleum Gas, and Gasoline Leakage in A Residential Garage. *Energy & fuels*. ISSN 0887-0624. 12 (1998), 1, pp. 83-89.
[60] GUPTA, R. B. *Hydrogen Fuel: Production, Transport, and Storage*. ISBN 1420045776. London: CRC press 2008.

PROGRAM ŠKOLENÍ KRITICKÉHO PERSONÁLU JADERNÉ ELEKTRÁRNY PRO ZAJIŠTĚNÍ SPECIFICKÉ ODEZVY

TRAINING PROGRAM OF A CRITICAL PERSONNEL TO ENSURE A SPECIFIC RESPONSE OF NUCLEAR POWER PLANT

Jan Jiroušek

Statní úřad pro jadernou bezpečnost, lokalitní pracoviště Temelín, 373 05 Temelín-elektrárna, jan.jirousek@sujb.cz

Abstrakt: Na základě akčního plánu Státního úřadu pro jadernou bezpečnost se zpracovává plán odezvy Jihočeského kraje, v němž se nachází jaderná elektrárna Temelín, na nejhorší výpadek vnějšího elektrického napájení. Odezva je realizována souborem vysoce propojených technických a organizačních prací. Z tohoto důvodu je pro zajištění bezpečného procesu reakce důležitá akceschopnost jaderné elektrárny i regionu. To znamená zajistit organizační, technickou a odbornou připravenost zdrojů, sil a prostředků jak jaderné elektrárny, tak i regionu. Současné školení pracovníků kritických jaderných elektráren je zaměřeno na odezvy na projektové havárie. Reagovat na nejhorší scénář výpadku napájení elektrárny znamená zvládnout odezvu na nehodu přesahující projektové zadání. Na předmětnou odezvu personál dosud nebyl vyškolen. V tomto příspěvku se zabýváme obsahem školení kritického personálu v reakci na nejhorší scénář výpadku přívodu elektrického proudu.

Klíčová slova: Jaderná elektrárna, bezpečnost, nejhorší výpadek napájení, odezva, kritický personál, program výcviku.

Abstract: Based on the Action plan of the State Office for Nuclear Safety, a response plan is being prepared for the South Bohemian Region, in which the Temelín Nuclear Power Plant is located, to the worst outage of external power supply. The response is realized by a set of highly interconnected technical and organizational works. For this reason, the operational capability of both, the nuclear power plant and the region is important to ensure a safe response process. This means ensuring the organisational, technical and professional preparedness of the resources, forces and resources of both, the nuclear power plant and the region. The current training the critical personnel of nuclear power plant is focused on responses to design accidents. Responding to the worst-case scenario of a power failure means managing an accident response beyond the design specification. Staff have not yet been trained for such response. In this paper, we discuss the content of training critical personnel in response to the worst-case scenario of a power outage.

Key words: Nuclear power plant, safety, worst power outage, responsiveness, critical personnel, training program.

1. ÚVOD

Pro rozpracování další etapy Národního akčního plánu [1] v oblasti odezvy jaderné elektrárny Temelín a regionu na nejhorší dlouhodobý výpadek proudu (označovaný jako SBO – Station Black-Out) pomocí metody Feed and Bleed (F&B), bylo potřeba vypracovat plán připravenosti [2,3,4]. V současnosti tedy existuje:

- ověřené technické řešení SBO,
- jsou vytipovány zdroje rizik, které mohou narušit odezvu na SBO
- a plán řízení rizik při odezvě na SBO.

Pro zajištění připravenosti a odezvy jaderné elektrárny Temelín a regionu na SBO je nutné realizovat soubor vysoce propojených technických a organizačních opatření, které zajistí správnou koordinaci činností podle harmonogramu i reálných podmínek. Tato připravenost (provozní způsobilost) tedy znamená zajištění organizační, technické a odborné připravenosti zdrojů, sil a majetku jaderné elektrárny Temelín, zdrojů skupiny ČEZ a regionu. Akceschopnost je podmíněna dle [3]:

- vysoce kvalitním týmem,
- odpovídajícím vybavením
- a dobrém řízením procesu odezvy.

Kvalita týmu je podmíněna jak znalostmi a dovednostmi dostatečného počtu členů týmu, tak školením spolupráce při realizaci harmonogramu reakce. Dobré řízení procesu odezvy závisí na souladu s časovou osou propojené práce a na připravenosti potřebného vybavení a zdrojů [3].

Osvědčenými nástroji pro zajištění připravenosti jsou dle [3,4] připravenost:
- personálu,
- vybavení materiálních a technických prostředků,
- objekty včetně fyzické bezpečnosti, služeb atd.
- a okolí, tedy v posuzovaném případě připravenost Jihočeského kraje.

S ohledem na současné znalosti a zkušenosti lze dle [3] organizační, technickou a odbornou kapacitu zdrojů, sil a prostředků jaderné elektrárny Temelín a regionu zajistit pouze:
- pravidelným školením členů týmu odezvy z hlediska znalostí a dovedností,
- pravidelným procvičováním kritických úkolů,
- prováděním taktických cvičení z hlediska organizace a technologie,
- pravidelnými kontrolami a zkouškami stavu technických zařízení
- a pravidelné ověřování plánu vyrozumění kritického personálu.

Současné školení kritického personálu jaderné elektrárny Temelín a regionu je zaměřeno především na řešení projektových havárií. Reakce na nejhorší scénář SBO znamená, že řízení nehody přesahující stávající projekt není zatím školeno.

V příspěvku [5] jsme navrhli scénář reakce na nejhorší SBO, který se skládá z řady vzájemně propojených úkolů, je velmi náročný na koordinaci a je vystaven řadě rizik. Proto jsme v článku [6] vypracovali plán řízení části technických rizik, která lze očekávat během odezvy.

V tomto příspěvku se zabýváme obsahem školení kritických pracovníků v odezvě na nejhorší SBO, abychom zajistili jejich nové kompetence, které implementace této odezvy vyžaduje. Pro přehlednost proces odezvy rozdělujeme do podsekcí, které spadají do odpovědnosti jednotlivých manažerů odezvy[3,4]. Na základě analýzy požadavků na jednotlivé úkoly a organizačních pokynů pro zajištění koordinace určujeme obsah znalostí a dovedností, kterými musí zaměstnanci a jednotliví manažeři kritické odezvy disponovat pro její kvalitní provedení. Základní objem znalostí se skládá z okruhů:
- jaderná elektrárna je objekt kritické infrastruktury,
- povinnosti provozovatele jaderné elektrárny,
- plán připravenosti na havárii, která je schopna vyvolat krizovou situaci (tj. dle zákona č. 240/2000 Sb. plán krizové připravenosti),
- postupy řešení úkolů v jednotlivých podsekcích,
- dostupnost technických a komunikačních prostředků,
- povinnosti, odpovědnosti a práva kritického personálu v každé sekci,
- způsoby řešení možných konfliktů,
- dokumentace činností.

Abychom pravidelně hodnotili znalosti kritického personálu, sestavujeme sadu kontrolních seznamů pro jednotlivé procesy odezvy. Vzhledem k tomu, že odezva na nejhorší SBO je specifická, zahrnujeme do plánu krizové připravenosti subjekty zapojené do odezvy na nejhorší SBO a do plánu řízení rizik požadavek na pravidelné školení a pravidelné ověřování znalostí a dovedností kritického personálu pro odezvu na nejhorší SBO [3,4]. Zavádíme také požadavky na ověření spolupráce dílčích úseků při odezvě na nejhorší SBO, protože od roku 2002 je pravidelně testována pouze spolupráce Integrovaného záchranného systémů, jaderné elektrárny Temelín a Jihočeského kraje v odezvě na projektovou havárii [7].

2. PODMÍNKY PRO SESTAVENÍ AKČNÍHO PLÁNU

Na základě současného poznání [4,8] akční plán znamená zajistit připravenost na akci, kterou je odezva na nadprojektovou havárii. Na základě současných znalostí a zkušeností [3,8-10] akceschopnost vyžaduje mít k dispozici:
- kvalitní a dobře vyškolený profesionální tým,
- vysoce kvalitní technické vybavení
- a dobré řízení procesu odezvy.

Kvalita expertního týmu je podmíněna jak znalostmi a dovednostmi dostatečného počtu členů týmu, tak školením spolupráce při plnění harmonogramu prací. Dobré řízení procesu odezvy znamená:

- zajistit soulad propojených prací s časovým harmonogramem
- a připravenost a operabilitu nezbytných zařízení a zdrojů.

Osvědčené nástroje pro zajištění připravenosti k akci jsou podle [11-13]:
- připravenost osob,
- zajištění materiálních a technických prostředků,
- zajištění vybavení pomocnými prostředky a službami, včetně zabezpečení, a připravenosti okolí.

V sledovaném případě podle [12-14] organizační, technická a odborná způsobilost sil a majetku jaderné elektrárny Temelín a regionu k plnění úkolů odezvy na nejhorší výpadek stanice musí zajistit:
- pravidelné školení členů týmu odezvy z hlediska znalostí a dovedností,
- pravidelné procvičování kritických úkolů,
- provádění taktických cvičení z hlediska organizace a technologie,
- pravidelné inspekce stavu technických zařízení
- a pravidelné kontroly vnějších podmínek.

3. ROLE ŠKOLENÍ PERSONÁLU

Vzdělávání je proces získávání určitých schopností a dovedností, spojených se snahou začlenit se do dané kultury a společnosti a aktivně přispívat k jejich rozvoji. Probíhá ve všech fázích lidského životního cyklu. Zasedání Rady EU v Lisabonu ve dnech 23.-24. března 2000 postavilo vzdělávací politiku do popředí zájmů a cílů Evropské unie a tyto záměry byly potvrzeny na zasedání Rady ve Stockholmu v roce 2001.

Hlavním cílem následných hospodářských a vzdělávacích politik Evropské unie bylo "vytvořit nejvíce konkurence schopnou a nejvíce dynamickou ekonomiku založenou na znalostech a vzdělávání na světě, schopnou udržet hospodářský růst rozšiřováním a zlepšováním pracovních míst a větší sociální soudržností". Rozvinuté země se potýkají s vyčerpatelností zdrojů, a proto si již uvědomují, že vzdělávání je jedním z mála zdrojů, jehož objem lze trvale obnovit a dále zvýšit [16-19].

Potenciál a konkurenceschopnost každé společnosti není jen ve výrobních kapacitách strojů a technologických zařízení, ale především v zaměstnancích a know-how, tedy v nehmotném majetku. Pro rozvoj potřebuje každý podnik talentovaný personál, který je schopen generovat určité hodnoty. Aby bylo možné splnit očekávané požadavky, musí mít každý jednotlivec určité znalosti, dovednosti a motivaci. To znamená, že pro něj musí být vytvořeny určité podmínky. Základními podmínkami jsou ochrana zdraví, přístup ke vzdělání, protože inovace, které jsou nezbytné z hlediska rozvoje, vyžadují získání nových znalostí a přijetí nových dovedností.

Vzdělávání dospělých začalo v 19. století a kolem roku 1976 již mělo komplexní rámec a bylo chápáno jako vzdělávání a odborná příprava pracovníků v organizacích, jejichž cílem je zlepšit, prohloubit a rozšířit dosažený stupeň pracovních schopností [18]. Dnes je specifická forma vzdělávacích systémů přizpůsobena specifikům a potřebám podniku a legislativě příslušné země. Pracovní vzdělávání je plánovaný proces úpravy postojů, znalostí a dovedností učením zaměřeným na dosažení efektivního výkonu v určité činnosti nebo rozsahu činností. Jeho cílem z hlediska práce je rozvíjet schopnosti jednotlivce a uspokojovat současné a budoucí potřeby organizace týkající se pracovní síly [20-23].

MAAE [24] začala věnovat velkou pozornost vzdělávání krátce po roce 2000 s ohledem na zvýšenou fluktuaci kritického personálu v jaderných zařízeních. Hlavním cílem bylo zavedení integrovaného přístupu k řízení jaderných zařízení zaměřeného na bezpečný a spolehlivý provoz, který je založen na řízení znalostí. Důraz byl kladen na:
- nahrazení zastaralých přístupů novými, které jsou výsledkem výzkumu a provozních zkušeností a jsou bezpečnější
- a podporovat kulturu bezpečnosti.

Důraz se začal klást na pracovní vzdělávání, zejména na vzdělávání a školení kritického personálu na všech úrovních řízení. Bylo zdůrazněno, že plán vzdělávání a odborné přípravy musí být řešen dlouhodobými potřebami jaderného zařízení [25]. To znamená činnostmi souvisejícími s bezpečností a kulturou bezpečnosti. Plán školení musí být pravidelně přezkoumáván s ohledem na provozní zkušenosti. Školení personálu jaderných zařízení musí být systematické a musí odrážet potřeby konkrétních pracovních míst, a to jak znalostí, tak dovedností. Musí zahrnovat provozní i havarijní plánování. Musí vycházet z osvědčených postupů a poučení [26]. Podle [27-29] musí školení poskytovat požadované kompetence pro danou práci, přičemž kompetence znamená kombinaci znalostí, dovedností a postojů a školení pro spolupráci. Jaderný regulační orgán země musí pravidelně kontrolovat kvalitu školení kritického personálu [28]. Vedle toho je vzdělávání v oblast jaderného průmyslu podporováno a organizováno i OECD / NEA, EURATOM a WANO.

4. POUŽITÁ DATA A METODY

Současné školení pracovníků jaderné elektrárny Temelín respektuje všechny požadavky MAAE [11-14,25], OECD [18,22] a EU [21]. Vzdělávací program [30] je rozdělen podle pracovních potřeb a má modulární charakter. V oblasti odezvy na mimořádné události je zaměřen na odezvu na událost přesahující projektové nehody, s cílem vyhnout se přechodu události do nehody s tavením paliva. Proto pobíhá i pravidelné školení na simulátorech.

Odezva na nejhorší scénář SBO znamená zvládnout nehodu z oblasti rozšířených projektových podmínek, která dosud nenastala. Kvantitativní analýza takové odezvy je v dokumentu [31]. Na jeho základě sestavujeme program výcviku odezvy na SBO. Vytváříme program v modulární formě, se stejnou strukturou jako stávající vzdělávací moduly [30]. Při jeho sestavování používáme metodu doporučenou v [28]:

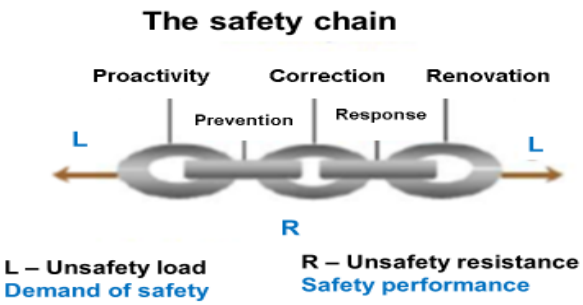
- analýzu potřeb odezvy na základě vypracovaného scénáře odezvy s přihlédnutím k rizikům odezvy zjištěným při práci [6],
- vypracování výcvikového programu odezvy na nejhorší výpadek stanice v jaderné elektrárně Temelín se zvláštním důrazem na kritické body procesu odezvy,
- vytvoření materiálů pro školení,
- a kontrolní seznamy k vyhodnocení účinnosti školení.

Protože při této odezvě je třeba využít postupů krizového řízení v České republice, zařazujeme do vzdělávacího programu důležité poznatky o krizovém řízení v České republice. Protože jaderná elektrárna Temelín patří k české i evropské kritické infrastruktuře, což je důležitý fakt pro bezpečný rozvoj státu a jeho obyvatel, zařazujeme i základní informace o kritické infrastruktuře. S ohledem na uvedenou skutečnost je nezbytné uvažovat jak plány ochrany zařízení a okolí před dopadem důsledků provozu při selhání, tak i s plány obnovy po případné havárii.

5. POŽADAVKY ODEZVY NA NEJHORŠÍ SBO

Integrální bezpečnost se neomezuje pouze na jednostranná řešení problémů, jako je represe, ale zabývá se situacemi ovlivňujícími určitou úroveň bezpečnosti prostřednictvím takzvaného bezpečnostního řetězce (obrázek 1), který se skládá z následujících částí:

- pro-aktivita (odstranění strukturálních příčin nejistot, které narušují bezpečnost, tj. ohrožují bezpečí a udržitelný rozvoj),
- prevence (opatření k odstranění přímých příčin narušení bezpečnosti),
- korekční opatření (opatření údržby a provozní předpisy pro zajištění bezpečnosti),
- odezva (opatření pro ochranu a zmírnění následků)
- a renovace (k zajištění podmínek pro obnovu a další zvyšování bezpečnosti).

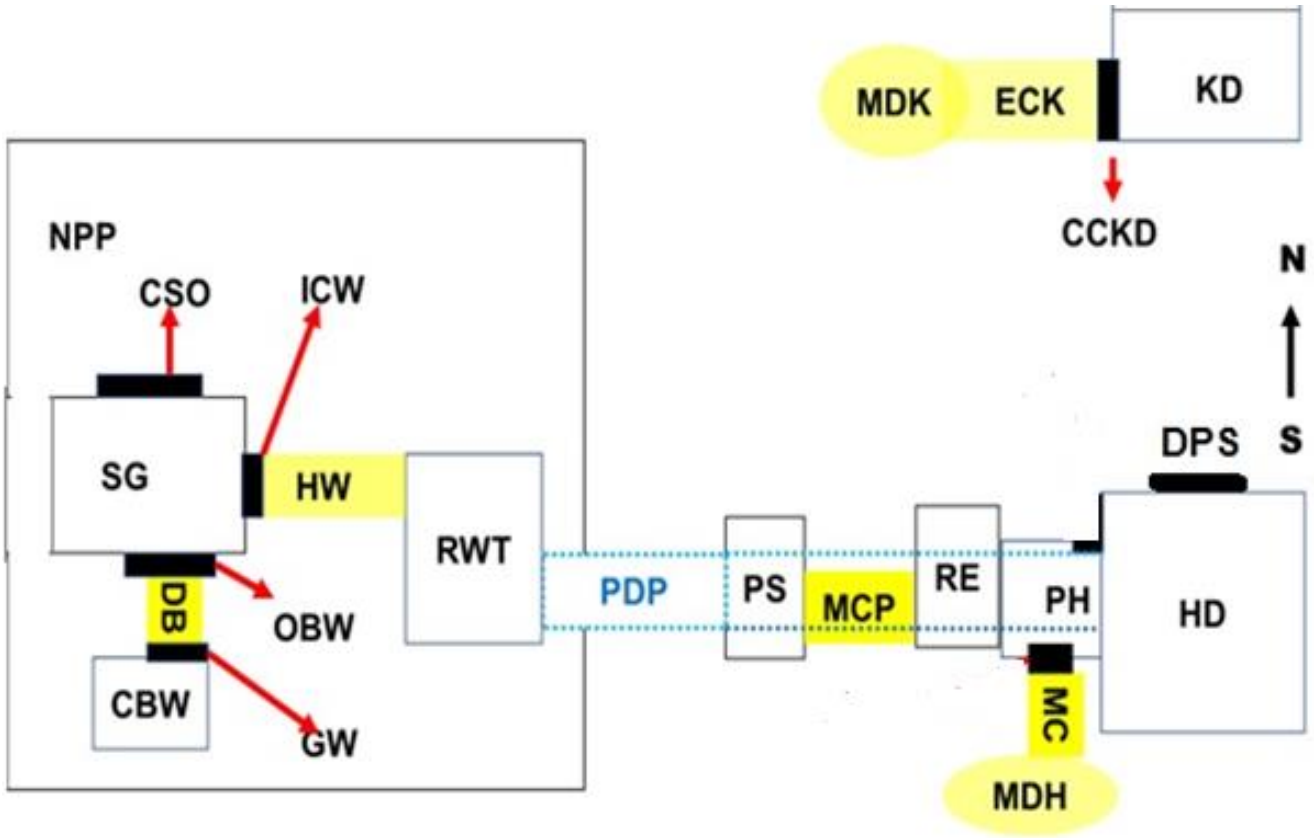


Obr. 1. Řetěz bezpečnosti, činnosti pro zajištění bezpečnosti [3].

V pracích [,65] jsme navrhli scénář odezvy na nejhorší SBO, který se skládá z řady vzájemně propojených úkolů a je velmi náročný na koordinaci. Celkový proces odezvy se skládá z úseků, které spadají do odpovědnosti tří organizačních jednotek účastnících se reakce:

- NPP-jaderná elektrárna Temelín,
- EH-vodní elektrárna Hněvkovice
- a FV-Povodí Vltavy (Povodí Vltavy, s. p. - organizační jednotka, která spravuje přehrady Hněvkovice a Kořensko).

Obrázek 2 ukazuje model, na kterém jsou vyznačeny objekty, které hrají roli při odezvě na SBO.



Obr. 2. Situační schéma na podporu odezvy u nejhoršího průběhu SBO. Označení:

1. ***Stabilní objekty:*** NPP - jaderná elektrárna Temelín; SG – parní generátor na JETE; ICW – vstup surové chladicí vody do SG; CSO – přepouštěcí ventil páry do atmosféry; OBW – výstup odluhované kotelní vody z SG; GW-nátrubek pro hadici k připojení odluhu do systému technické vody důležité; CBW – kolektor odluhu; RWT - vodojem surové vody v JETE; PDP-podzemní dvojité potrubí surové vody mezi čerpací stanicí surové vody z přehrady Hněvkovice do vodojemu; HD – přehrada Hněvkovice na Vltavě; PH – vodní elektrárna Hněvkovice; RE rozvodna ve vodní elektrárně Hněvkovice; CCPH – součást rozváděče elektrárny Hněvkovice; CCHD- manipulační část Hněvkovice přehrada; KD – přehrada Kořensko; CCKD- hydraulický rozváděč polí přehrady Kořensko; PS – čerpací stanice surové vody z přehrady Hněvkovice pro potřeby JETE; DPS – regulace odtoku z přehrady Hněvkovice; SG-parní generátor.
2. ***Mobilní objekty*** – prostředky pro odezvu: MDK - mobilní skupina pro regulaci hladiny vody na přehradě Kořensko; ECK-mobilní prostředky pro manipulací jezovými poli přehrady Kořensko; MDH mobilní dieselový generátor (50 kW) pro vodní elektrárnu Hněvkovice; MC-mobilní kabelové připojení do rozvodny elektrárny Hněvkovice; MCP – mobilní pomůcky a svorky k ruční manipulaci v rozvodně vodní elektrárně Hněvkovice k propojení na čerpací stanicí PS; HW-mobilní motorové čerpadlo a hadice pro propojení vodojemu surové vody v JE Temelín a parního generátoru.

Všechny organizační jednotky mají strukturu řízení v souladu s ISO 9000 v poslední verzi. Jednotlivé sekce jsou řízeny speciálními manažery. Hlavní úrovně odezvy na nejhorší strukturu SBO jsou:

- hejtman Jihočeského kraje,
- odborná podpora Státního úřadu pro jadernou bezpečnost
- velitel Integrovaného záchranného systému (Hasičský záchranný sbor) pro koordinaci činností: jaderné elektrárny Temelín; vodní elektrárny Hněvkovice; Povodí Vltavy; a mobilní objekty, které jsou pro tento účel nezbytné.; a ředitelů jaderné elektrárny Temelín a vodní elektrárny.

Všechny úkoly byly souhrnně popsány [30]. vyžadují správnou implementaci technických a organizačních opatření ve správný čas. Jednotlivé úkoly jsou uvedeny na časové ose v tabulce 1.

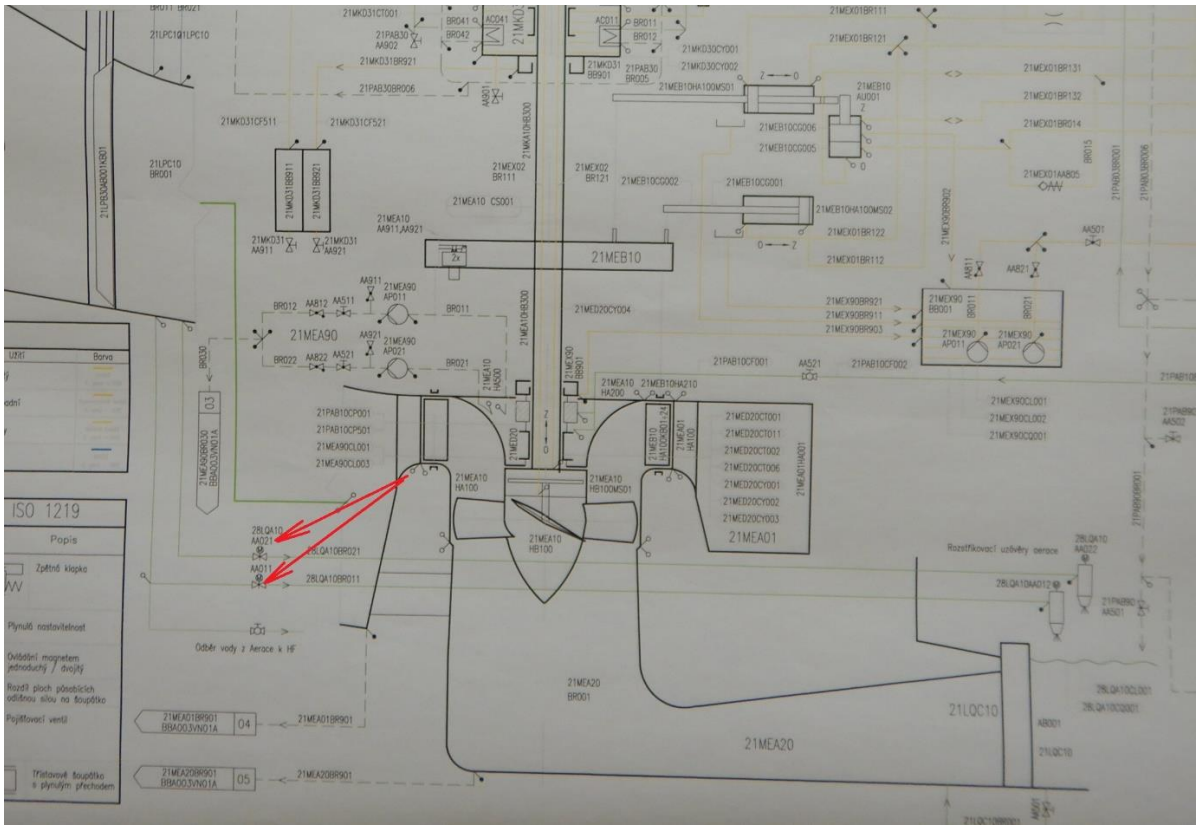
Tabulka 1. Přehled akcí v časové posloupnosti. D-doba trvání SBO v hodinách; DV-oblast platnosti opatření; SBR - Jihočeský kraj; PH – vodní elektrárna Hněvkovice; RBM - Povodí Vltavy; přehrada KD – Kořensko.

D	**DV**	**Organizační opatření**		**Technická opatření**
0	NPP	Provozní předpis pro úplnou ztrátu elektrického napájení havarijních sběrnic		Projektový stav. Reaktor je automaticky odstaven systémy řízení které vygenerují signál ke startu diesel-generátorů jako zdrojů střídavého napětí.
1	NPP	Aktivace předpisů pro abnormální provoz		Projektový stav – Zdroje stejnosměrného proudu zajišťují napájení nezbytných zařízení. Dochází k růstu tlaku ve všech parogenerátorech a otevírají pojistné ventily, postupně klesá hladina v SG [31].
2	NPP	NPP ředitel vyhlašuje zahájení činností podle nejhoršího plánu SBO. Šéf krizového štábu NPP zahajuje přípravu na odezvu pro nejhorší SBO podle předpisů pro abnormální provoz.		Projektový stav – Zdroje stejnosměrného proudu pracují. Je snižován tlak v SG prostřednictvím SCO. SG jsou postupně zaplavovány gravitačně vodou z napájecí nádrže (není na schématu). Dochlazování metodou Feed and Bleed je zahájeno. [31].
……				
9	NPP	Pokračuje práce podle předpisů pro abnormální provoz. Hasičský závodní sbor zahajuje čerpání vody do SG.		Napájecí nádrž je prázdná. Hasičský závodní sbor plní SG prostřednictvím motorového čerpadla z nádrží demineralizované vody na bloku. Postupně dochází kapacita projektových stejnosměrných zdrojů [31].
……				
24	SBR	Hejtman jihočeského kraje vyhlašuje stav nebezpečí.		Kraj zahajuje činnosti odezvy na nejhorší SBO
		NPP	Směna a hasiči NPP pokračují v práci podle stávajících předpisů pro abnormální provoz.	Technická opatření pokračují. Jsou připojovány mobilní prostředky pro sledování vybraných parametrů bloku[31].
		RBM	Ředitel zahajuje činnosti podle předpisů pro abnormální provoz HD při nejhorším SBO.	Je omezen odtok vody z HD, situace pro vytvoření prováděcího předpis je na obrázcích 2 a 3 [30].
……				
107	SBR	Havarijní podmínky pokračují.		Odezva na nejhorší SBO pokračuje..
		NPP	Směna a hasiči NPP pokračují v práci podle stávajících předpisů pro abnormální provoz.	Zásoby demineralizované vody jsou vyčerpány, hasiči začínají doplňovat SG surovou vodou z RWT. Je nově vytvořena trasa pro odluhování SG do CBW a zahájeno odluhování [6,30,31].
		RBM	Činnosti podle předpisů pro abnormální provoz HD při nejhorším SBO pokračují.	Technická opatření pokračují[30].
……..				
216	SBR	Havarijní podmínky pokračují.		Odezva regionu na nejhorší SBO pokračuje.
		NPP	Směna a hasiči NPP pokračují v práci podle předpisů pro abnormální provoz.	Technická opatření pokračují. [6,30,31]

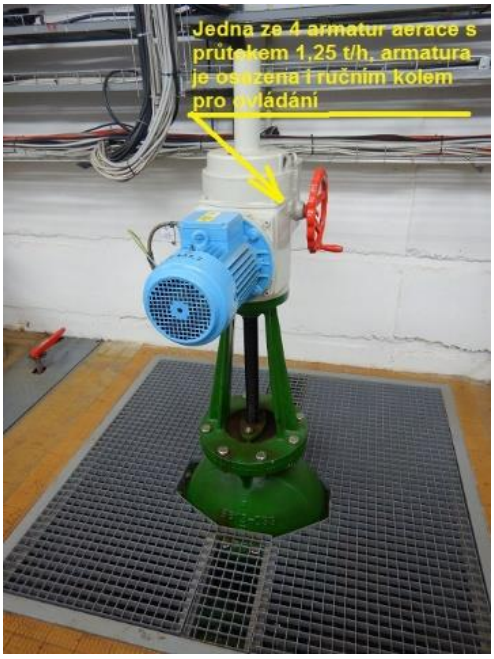
		PH	PH ředitel povoluje propojení RE and PS.	Je prostřednictvím MC připojen i DC zdroj MDH a propojeny RE and PS – obrázky 4 a 5 - specifický prováděcí předpis [30,32].
		RBM	Činnosti podle předpisů pro abnormální provoz HD při nejhorším SBO pokračují.	Technická opatření pokračují [30].
…….				
500	SBR	Havarijní podmínky pokračují.		Odezva regionu na nejhorší SBO pokračuje.
		NPP	Směna a hasiči NPP pokračují v práci podle předpisů pro abnormální provoz.	Technická opatření pokračují. Je prostřednictvím dodávky elektrické energie z PH zprovozněna PS zajišťující dodávku surové vody z HD do vodojemu RWT prostřednictvím podzemního vedení PDP [6,30,33] – specifický prováděcí předpis [30,32].
		PH	Práce PH pro PS podle předpisů pro abnormální provoz pokračuje.	Technická opatření pokračují. Obrázky 6 a 7 [30] – specifický prováděcí předpis [30].
		RBM	KD ředitel povoluje skupině MDK vstup do DK pro snížení polí.	Technická opatření pokračují. MCK prostřednictvím ECK zajišťuje gravitační spuštění 4 polí na KD [30] – specifický prováděcí předpis [30].
……				
683	SBR	Havarijní podmínky pokračují.		Odezva regionu na nejhorší SBO pokračuje.
		NPP	Směna a hasiči NPP pokračují v práci podle předpisů pro abnormální provoz.	Technická opatření pokračují. PS zajišťuje dodávku vody do RWT podzemním potrubím PDP.
		PH	Práce PH pro PS podle předpisů pro abnormální provoz pokračuje.	Technická opatření pokračují [30].
		RBM	Činnosti podle předpisů pro abnormální provoz HD a KD při nejhorším SBO pokračují.	Technická opatření pokračují [30].

Metoda F & B je podmíněna jak konvekčním přenosem tepla z aktivní zóny reaktoru vodou, tak varem na sekundární straně parogenerátoru, a proto nemůže teplota primární okruhu poklesnout pod 110 °C [1,31]. Ochlazení primárního okruhu na teplotu nižší než 110 °C proto vyžaduje obnovení elektrického napájení bezpečnostních sběrnic.

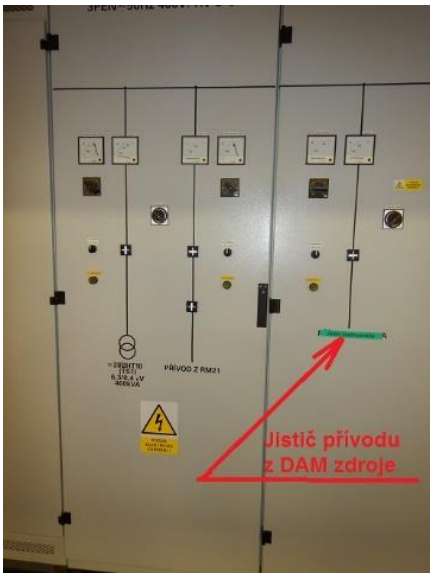
Na základě bezpečnostní dokumentace [1,3,30] dosahuje proces chlazení popsaný v tabulce 1 dostatečných podmínek pro bezpečnost, protože teplota primárního okruhu 110°C zajišťuje stále dostatečně vysokou rezervu pro zajištění, že nedojde k poškození nebo ztrátě integrity palivového pokrytí, tvořící první bezpečnostní bariéru. Stupeň a rozsah poškození palivového pokrytí determinuje jak velikost uniklého radioaktivního inventáře, tak i náklady a dobu do obnovení provozu JE [1,2], případně na její dílčí opravy. Opatření na odluhování parogenerátoru slouží jak minimalizaci možných úniků radioaktivních médií z primárního okruhu, tak snižují možnost poškození samotného parogenerátoru. Uvedený postup umožní jak snížit předpokládatelné náklady tak i dobu pro obnovení provozu.



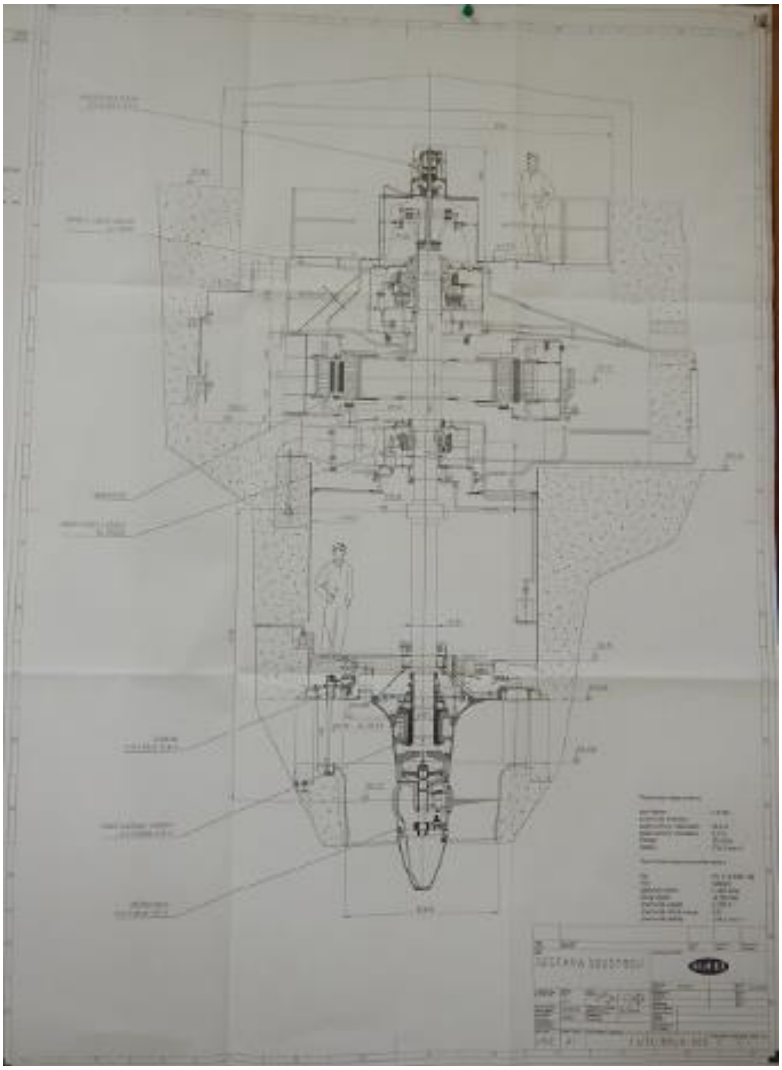
Obr. 2. Výřez ze schématu technologie přehrady Hněvkovice HD, vyznačené aerační armatury pro omezení odtoku z přehrady Hněvkovice.



Obr. 3. Aerační armatura, minimálního průtoku korytem Vltavy z z přehrady Hněvkovice.



Obr. 4. a 5. Připojovací místo (MC) pro vnější připojení mobilního diesel-generátoru 50kW, skříň rozvodny z přehrady Hněvkovice.



Obr. 6. Průřez vodní turbínou z přehrady Hněvkovice.

Obr. 7. V rozvodně RE vyznačeny vývody 6kV pro ruční manipulování vyvedení elektrického výkonu do PS (čerpací stanici Hněvkovice pro JETE).

6. VÝCVIK PERSONÁLU JETE A OSTATNÍCH ZÚČASTNĚNÝCH

Vzhledem k tomu, že odezva na nejhorší SBO je kritickým úkolem, jedná se o celoživotní učení účastníků odezvy [11,12,14]. Vzdělávací program je připraven formou modulárního systému, který umožňuje, aby kritický personál měl vhodné složení vzdělávání se zaměřením na potřeby dané odezvy a na požadovanou odbornost, jakož i možnou změnu profilování. Časové rozdělení vzdělávacího programu je určeno rozsahem modulů nastavených pro jednotlivé cílové skupiny.

Vzdělávací program pojímáme jako otevřený dokument, který z důvodu modulárního uspořádání umožňuje doplňování a aktualizaci podle měnících se potřeb odezvy a na základě výsledků výzkumu a vývoje a nových poznatků v souvisejících oblastech. Modulární uspořádání umožní jeho efektivnější integraci do stávajícího vzdělávacího systému v jaderné elektrárně Temelín a zvýší efektivitu školení kritického personálu, aby reagoval na nejhorší SBO [1,7,30].

Na základě výše uvedených odborných znalostí, požadavků české legislativy a analýzy scénáře reakce na nejhorší SBO pro elektrárnu Temelín jsme do základního svazku znalostí zařadili následující témata:
- jaderná elektrárna je objektem kritické infrastruktury (nařízení vlády č. 432/2010 Sb.),
- povinnosti provozovatele jaderné elektrárny jako objektu kritické infrastruktury (nařízení vlády č. 432/2010 Sb.),
- základy a principy krizového řízení, prvky krizového řízení, organizační struktura řízení (zákon. č. 240/2000 Sb., zákon. 110/1998 plk., zákon č. 241/2000 Sb., zákon č. 239/200 Sb.),
- plán krizové připravenosti jaderné elektrárny Temelín podle nařízení vlády č. 462/2000 Sb.
- principy metody feed and bleed (F&B) a zkušenosti s používáním IT,
- základní strategie odezvy na nejhorší SBO,
- popis odezvy na nejhorší SBO,
- kritické body odezvy na nejhorší SBO,
- demonstrace činností v kritických bodech,
- plán řízení rizik pro odezvě na nejhorší SBO,
- interní nouzové postupy pro SBO,
- postupy pro řešení úkolů v jednotlivých podoblastech,
- způsob komunikace během odezvy na nejhorší SBO,
- umístění a dostupnost technických a komunikačních prostředků,
- dovednosti, povinnosti, odpovědnosti a práva kritického personálu v každém segmentu odezvy,
- způsoby řešení konfliktů
- a dokumentace činností.

Pro všechna témata je připraven vzdělávací materiál.

Školení výkonného personálu vyžaduje též praxi v oblastech:
- pravidelná údržba zařízení pro odezvu,

- vyzvednutí a přemístění zařízení pro odezvu,
- specifické technické operace,
- přeprava a zapojení diverzních a mobilních prostředků-hadic, kabelů, generátorů dieselových motorů.

Pro každou pozici je třeba zajistit výcvik tří osob. Provádění činností musí být dokonalé a musí být splněn harmonogram odezvy. Proto musí být tato školení častější a kontrolovanější. Testy jsou přizpůsobeny podle pozice osoby v procesu odezvy; otázky jsou uvedeny v tabulce 2. Otázky jsou klasifikovány stupnicí 1 – 5; 1 je nejlepší. Výsledek každého testu je stanoven dle tabulky 3.

Tabulka 2. Kontrolní seznam pro test znalostí kritického personálu; A – míra rizika (nedostatek ve vzdělávání).

Otázka	**Odpověď**	**A**
Co udělat?		
Jak to udělat?		
Proč to udělat?		
Podle kterého nouzového předpisu postupovat?		
Jaká rizika lze očekávat?		
Jak zmírnit předmětná rizika?		
Které zásady kultury bezpečnosti je třeba respektovat?		
Které zásady komunikace s ostatními pracovníky odezvy je třeba respektovat?		
Jak musí být činnost odezvy dokumentována?		
CELKEM		

Tabulka 3. Stupnice pro vyhodnocení testu.

Míra rizika	**Výsledek**
Extrémně vysoká-5	Více než 43
Velmi vysoká-4	32 - 42
High-3	21 - 31
Střední-2	9 - 20
Nízká-1	9

Pokud je míra rizika určená testem u zkoušené osoby v kategorii 4-5, musí osoba okamžitě opakovat školení a test. Pokud je míra rizika 2-3, musí osoba opakovat test po třech měsících.

Školení pro zajištění spolupráce při odezvě na nejhorší SBO mezi ČEZ Jadernou elektrárnou Temelín a Vodní elektrárnou Hněvkovice, která patří ČEZ, se uskuteční jednou za rok.

7. ZÁVĚR

S ohledem na současné poznatky jsme vytvořili program vzdělávání kritického personálu pro odezvu na nejhorší výpadek vnějšího napájení elektrickým proudem u jaderné elektrárny Temelín. Vzhledem k tomu, že odezva na nejhorší SBO je příliš specifická, je třeba zajistit krizovou připravenost subjektů na tuto odezvu a plán řízení rizik [6,30].

Proto navrhujeme vložit do plánu revizí atomového zákona požadavek na pravidelné školení a pravidelné testování znalostí kritických pracovníků odezvy na nejhorší SBO. Zavádím také povinnost pravidelně (každý rok) testovat spolupráci dílčích úseků v rámci odezvy na nejhorší SBO, protože od roku 2002 je pravidelně testována pouze spolupráce JE a regionu v odezvě na projektové havárie.

Poděkování: Autor děkuje za vedení práce, návrhy a připomínky doc. RNDr. D. Procházkové, CSc. DrSc.

LITERATURA

[1] SÚJB. *Národní Akční Plán na posílení jaderné bezpečnosti jaderných zařízení v České republice*. Praha: SUJB 2018. https://www.sujb.cz/fileadmin/sujb/docs/dokumenty/Cesky_NAcP_Rev3_final.pdf.

[2] IAEA, *Site Survey and Site Selection for Nuclear Installations, IAEA Safety Standards Series No. SSG-35.* Vienna: IAEA 2015, 61 p. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1690Web419 34783. pdf

[3] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.

[4] ČR. *Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).*

[5] JIROUŠEK, J., PROCHÁZKOVA, D. Method of Extending the Operation of Steam-Generator on Nuclear Installation under Conditions of Long-Term Station-Black-Out. Doi:10.3850/978-981-18-2016-8_132-cd

[6] JIROUŠEK, J., PROCHÁZKOVA, D. Risk Management Plan for Long-term Power Blackout for Temelin Nuclear Power Plant. Doi:10.3850/978-981-18-5183-4_R18-03-079-cd

[7] ČEZ, a. s., Jaderná elektrárna Temelín, Jaderná elektrárna Temelín. podnikový archiv Temelín: JE 2023

[8] HASIČSKÝ ZÁCHRANNÝ SBOR. *Archiv.* Praha: HZS 2023. https://www.hzscr.cz

[9] EBY, L.T., ADAMS, D.M., RUSSELL, J. E. A., GABY, S. H. Perceptions of Organizational Readiness for Change: Factors Related to Employees' Reactions to the Implementation of Team-Based Selling**.** *Human Relations*, 53(2000), 3, pp. 419-442.

[10] SURI, G., SHEPPES, G., GROSS, J. J. The role of action readiness in motivated behavior. *J Exp Psychol Gen*. 144 (2015), 6, pp. 1105-110513. Doi: 10.1037/xge0000114.

[11] IAEA. *Arrangements for Preparedness for a Nuclear or Radiological Emergency. GS-G-2.1*. ISBN 92-0-109306-3. Vienna: IAEA, 2007, 159 p.

[12] IAEA. *Preparedness and Response for a Nuclear or Radiological Emergency, GSR Part 7*. ISBN 978-92-0-105715-0. Vienna: IAEA, 2011,136 p.

[13] IAEA.*Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency. GSG-2.* ISBN 978-92-0-107410-2. Vienna: IAEA,2011, 120 p.

[14] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OU-HRABKA, 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/BK.978800106 6751

15] ARMSTRONG, M. *Armstrong's Handbook of Human Resource Management Practice*. ISBN 978-0-7494-5242-1. London: Cogan Publishers 2009.

[16] BECKER, G. *Human Capital: a Theoretical and Empirical Analysis, with Special Reference to Education. 3rd* ed. ISBN 0-226-04120-4. Chicago: The University of Chicago Press 1993, 390 p.

[17] DE LA FUENTE, A., CICCONE, A. Human Capital in a Global and Knowledge-based Economy. *Final report*. Universita Pompeu Fabra, Instituto de Análisis Económico 2002.

[18] OECD. *Investment in Human Capital through Post-Compulsory Education and Training: Selected Efficiency and Equity Aspects*. Paris: OECD 2002, 60 p.

[19] VYCHOVA, H., MERTL, J. Relationships of Education and Health in the Context of Economic Development. *Politická ekonomie*, 57 (2009), No 1, pp.58-78.

[20] CLIFFORD, J., THORPE, S. *Workplace Learning & Development: Delivering Competitive Advantage to Your Organization.* ISBN 978-0-7494-4633-8.London: Cogan Publishers 2007.

[21] EU. *Archives.* http://europa.eu/legislation_summaries/education_training_youth/general.framework/ef 0016_cs.htm.

[22] OECD. *Beyond Rhetoric: Adult Learning Policies and Practices*. ISBN 92-64-19943-8. Paris: OECD 2003.

[23] PHILIPS, J. J. *Handbook of Training Evaluation and Measurement Methods*. ISBN 978-0-88415-387-0. New York: Routledge 2011.

[24] IAEA. *Guide to Knowledge Management Strategies and Approaches in Nuclear Energy Organizations and Facilities. NG-G-6.1*. ISBN 978-92-0-125821-2. Vienna: IAEA 2022, 82 p.

[25] IAEA. *Recruitment, Qualification and Training of Personnel for Nuclear Power Plants. SSg-75*. ISBN 978-92-0137222-2.Vienna: IAEA 2022, 66 p.

[26] IAEA. *Nuclear Educational Networks: Experience Gained and Lessons Learned. TECDOC-2007*. ISBN 978-92-0-135422-8. Vienna: IAEA 2022,110 p.

[27] IAEA. *Commissioning for Nuclear Power Plants: Training and Human Resource Considerations*; IAEA Nuclear Energy Series NG-T-2.2. ISBN 978-92-0-103608-7. Vienna: IAEA 2008.

[28] IAEA. *Systematic Approach to Training for Nuclear Facility Personnel: Processes, Methodology and Practices. NG-T-28.* ISBN 978-92-0-113520 -9. Vienna: IAEA 2021, 188 p.

[29] IAEA. *Mentoring and Coaching for Knowledge Management in Nuclear Organizations. TECDOC-1999*. ISBN 978-92-0-123822-1. Vienna: IAEA 2022, 126 p.
[30] JIROUŠEK, J. *Disertační práce- teze*, Praha: ČVUT 2023.
[31] ČEZ, a. s., Jaderná elektrárna Temelín. *Celoblokový předpis pro nouzové provozní stavy 0TC007/6, Činnosti při haváriích – Postupy pro úplnou ztrátu bezpečnostního napájení*, rev.3. Temelín: JE 2020, 237 p.
[32] ČEZ. *Technický operativní program*, 2TOP č. 2016/009 - ČEZ, a. s., Divize výroba, „2GO16 ZKOUŠKA SBO ETE - Poskytnutí napětí z MVE Hněvkovice“, 15p., Temelín: Archiv ČEZ, a. s.
[33] ČEZ, a. s., Jaderná elektrárna Temelín, *Celoblokový předpis pro použití prostředků DAM, dálkové ovládání armarur 0TC033R1/DZ01*, příloha 17, vydáno 2018, 9 p.

DIGITÁLNÍ DVOJČATA K PROAKTIVNÍ BEZPEČNOSTI SYSTÉMŮ SYSTÉMŮ

DIGITAL TWINS TOWARD PROACTIVE SAFETY IN SYSTEMS OF SYSTEMS

Tomáš Kertis[1], Dana Procházková[2]

[1] *KINT, s.r.o., Ke Hřišti 134, Babice. tomas.kertis@kint.cz*
[2] *ČVUT v Praze, Fakulta strojní, Technická 4, Praha 6, danuse.prochazkova@fs.cvut.cz*

Abstrakt: Bezpečnost systémů systémů (SoS), které reprezentují komplexní systémy s množstvím vazeb a interakcí různých logických i fyzikálních povah, je v posledních letech intenzivně zkoumána v mnoha výzkumech a vědeckých pracích. Tyto systémy, klíčové pro současnou společnost, odhalují zranitelnosti lidské společnosti, neboť mohou v nečekaných situacích způsobit značné ztráty a škody veřejným aktivům. Dochází k vzniku nebezpečných emergencí – neznámých stavů ohrožujících lidskou společnost. Tyto emergence, označované jako „černé labutě", se objevují v širokém spektru lidských aktivit. Vzhledem k rychlosti umělých systémů jsou někdy lidské reakce nedostačující. Z uvedených důvodů je nutné hledat způsoby snižování kritičnosti a zvyšování bezpečnosti SoS. Standardní nástroje řízení bezpečnosti však nemusí být dostatečně efektivní vzhledem ke komplexnosti SoS. Práce se zaměřuje na problémy bezpečnosti SoS, představuje koncept digitálních dvojčat a diskutuje možnosti jejich využití k zvýšení bezpečnosti.

Klíčová slova: Systémy systémů, digitální dvojčata, nebezpečné emergence, řízení bezpečnosti, kritičnost systémů.

Abstract: The safety of Systems of Systems (SoS), which represent complex systems with numerous logical and physical connections and interactions, has been intensively examined in various research studies and scientific papers in recent years. These systems are crucial for contemporary society, revealing our vulnerabilities, as they can cause significant losses of public assets in unexpected situations. This leads to the emergence of dangerous unknown conditions that threaten society, often referred to as "black swans", appearing across a wide range of human activities. Due to the speed of artificial systems, human reactions are sometimes insufficient. For these reasons, it is necessary to explore ways to reduce criticality and enhance the SoS safety. However, standard safety management tools may not be sufficiently effective due to the SoS complexity. This paper focuses on SoS safety issues, introduces the concept of digital twins, and discusses their potential for improving safety.

Key words: Systems of systems, digital twins, dangerous emergencies, safety management, system criticality.

1. ÚVOD

V současném komplexním světě technologií, kde systémy systémů (SoS) představují nezbytnou součást naší každodenní reality, se bezpečnost a kritičnost těchto systémů jeví jako klíčové komplementární aspekty vyžadující naši neustálou pozornost [1]. SoS, charakterizované jako soubory propojených systémů, které společně vytvářejí nové, nečekané funkce a vlastnosti, přinášejí bezpochyby řadu výhod, ale zároveň se mohou stát zdrojem značných rizik [1,2].

Cílem společnosti, která usiluje o to, aby byla bezpečná, je zkoumat bezpečnost SoS a vyhledávat možnosti jejího zlepšení, tj. snížení kritičností systémů. V tomto smyslu se práce zaměřuje na koncept digitálních dvojčat, která slouží jako nástroj simulace a analýzy skutečných systémů v digitálním prostoru [3]. Digitální dvojčata nabízejí možnost předvídat a analyzovat možná rizika, a tím přispívají k vytváření bezpečnějšího a stabilnějšího prostředí [4].

V předešlých pracích [1,4] byl představen procesní model zaměřený na snížení kritičnosti systémů, jehož aplikace v kontextu digitálních dvojčat je jedním z hlavních cílů předložené práce. Předmětný model poskytuje systematický přístup ke snižování rizik spojených se SoS a jeho implementace do modelu digitálních dvojčat bude detailně prozkoumána a diskutována v následujících kapitolách.

Práce poskytuje teoretický přehled konceptu SoS, digitálních dvojčat a významných bezpečnostních hledisek, následovaný praktickými návrhy a metodologií, jak efektivně zlepšit bezpečnost SoS prostřednictvím implementace a aplikace procesního modelu v digitálních dvojčatech.

2. TEORIE, POJMY A REŠERŠE SOUČASNÉHO STAVU

Systémy systémů (SoS) v kontextu naší práce definujeme jako soubory otevřených, vzájemně propojených systémů [5], které se skládají z podsystémů a objektů (komponent) s různými vlastnostmi a umístěními. Dle [6] se klasické pojetí systému a SoS liší v několika klíčových elementech:

- ***autonomie:*** složkové systémy vykonávají autonomii, aby naplnily účel globálního systému, tj. SoS,
- ***příslušnost***: složkové systémy si volí příslušnost na základě poměru nákladů a přínosů, a to vše s cílem naplnit vlastní účel a podpořit supra-účel SoS; v klasickém pojetí je příslušnost daná povahou a nemůže být svévolně změněna (např. jako členství v rodině),
- ***konektivita:*** existuje nesčetné množství možných propojení systémů a jejich částí, které zlepšují schopnosti SoS,
- ***diverzita***: neboli rozmanitost schopností SoS, je posílena autonomií různých složkových systémů, specifickou příslušností a otevřenou konektivitou,
- ***emergence*** *(náhlý vznik jevu nebo rysu)*: v kontextu SoS je důležitá zvýšená míra záměrné nepředvídatelnosti a tvorba podmínek pro možný vznik pozitivních emergencí (většinou zvýšení výkonu, schopnost převedení systémů na jiné funkce a plnění jiných cílů nebo umožnění včasné detekce a eliminace nepříznivého chování systémů při nežádoucích emergencí); nežádoucí emergence jsou reprezentovány výskyty nepředvídatelných nežádoucích událostí a pohrom.

Emergence má zásadní vliv na výběr metod pro práci se systémy: pro klasické systémy převažují exaktní metody, zatímco pro SoS se častěji využívají ***metody heuristické, včetně umělé inteligence (AI).***

Vazby mezi subsystémy a objekty zajišťují potřebné funkce a chování celého SoS [7]. Interdependence SoS, rozdělená dle [2,7,8] na žádané a nežádané (v normálních, abnormálních a kritických podmínkách), jsou fyzické, kybernetické, místní a logické povahy [2].

Žádané interdependence zlepšují vlastnosti systémů, zařízení a infrastruktur. ***Nežádané očekávané interdependence*** jsou běžně v projektech za normálních a abnormálních podmínek (projektových) ošetřeny dle legislativních požadavků [9]. ***Nežádané neočekávané interdependence*** mohou za kritických podmínek (nadprojektových) vést ke ztrátám systému, nesplnění funkcí nebo ohrožení systému a jeho okolí včetně lidí a lidské společnosti.

Pro exaktní řešení zvažovaných situací za jistých podmínek se používají projektová opatření. V případě, že nastanou nepříznivé jevy, resp. nehody, při kterých nedojde k překročení projektových kritérií, jde o tzv. projektové jevy (nehody), tak bezpečnost je zajištěna opatřeními vloženými do projektu. V případě, že dojde k překročení projektových kritérií (limitů), tak vznikají nadprojektové jevy, resp. havárie. Pojmy "projektové nehody" (Design Basis Accident) a "nadprojektové nehody" (Beyond Design Basis Accident) jsou formálně definované Mezinárodní agenturou pro atomovou energii (IAEA) [10] a běžně používané i v dalších oblastech řízení bezpečnosti technických děl [9].

Procesní model k snížení kritičnosti technického díla (tedy zvýšení bezpečnosti systému v rámci SoS) autoři zavedli a hodnotili v předchozí práci [1,8]. Model zahrnuje následující procesy a aktivity:

1. Identifikace (aktiv, zranitelností, důležitostí, zdrojů všech ohrožení systémů).
2. Interpretace dat (matice citlivostí, jejich transformace a vytvoření grafů).
3. Analýza a posouzení (zranitelností a kritičností, pomocí teorie citlivostí a grafů, *poznámka autora: možné využití dalších nástrojů****, např. heuristik a meta-heuristik včetně umělé inteligence***).
4. Vyhodnocení (primárních rizik na základě kritičností, scénářů dopadů).
5. Řízení (plán řízení primárních rizik, návrh opatření, stanovení odpovědností, realizace plánu, monitoring).

Digitální dvojčata, v souladu předešlých prací autorů [3,4], představují významnou technologii v současném digitálním věku a projektech 4.0. Jsou to virtuální obrazy fyzických objektů nebo systémů. Digitální dvojčata simulují reálné objekty v digitálním prostoru, což umožňuje podrobnou analýzu a předpovídání chování skutečných systémů v různých scénářích a podmínkách. Jsou nástrojem pro optimalizaci a zlepšení výkonnosti široké škály systémů, od průmyslových procesů po městské infrastruktury [4]. Vývoj a použití digitálních dvojčat je spojen s konceptem internetu věcí (IoT), kde zařízení navzájem v reálném čase komunikují a interagují. Tato synergická kombinace umožňuje nejen monitorovat a sledovat, ale i předvídat a reagovat na potenciální problémy a výzvy, dříve, než se v reálném světě vyskytnou [4].

Důležitou charakteristikou digitálních dvojčat je jejich schopnost nepřetržité aktualizace a učení se z dat v reálném čase, což zajišťuje, že poskytovaná data jsou relevantní a relativně přesná, což je klíčové pro informované a strategické rozhodování [1,2,4].

Z výše uvedeného vyplývá, že digitální dvojčata umožňují předpovídat nepříznivé/ nežádoucí emergentní situace a reagovat na ně včas díky relativně přesným datům v čase. Proto je považujeme za vhodnou technologii pro implementaci nových bezpečnostních metod a nástrojů, které zvyšují bezpečnost SoS. Poskytují příležitost pro posílení bezpečnosti SoS tím, že umožňují detailní analýzu a simulaci chování v různých podmínkách. Díky své schopnosti modelovat a předvídat komplexní interakce mezi složkami SoS, digitální dvojčata mohou sloužit i jako nástroj pro identifikaci a zmírňování rizik, což je klíčové pro zajištění bezpečnosti a odolnosti v dynamickém a nejistém prostředí dnešních složitých systémů.

Na druhou stranu, identifikované problémy implementace digitálních dvojčat na základě analýzy [11] jsou:
- náročnost vývoje,
- technologie vývoje,
- problémy kvality dat,
- problémy zabezpečení (security),
- náročná systémová integrace,
- míra znalosti provozního prostředí,
- organizační problémy,
- omezené HW kapacity
- a výkon.

Z uvedených fakt vyplývá, že implementace digitálních dvojčat je složitá. Proto je nutné konkrétní záměr zjednodušit a zefektivnit některé procesy, jelikož v současném stavu techniky je implementace jak technicky, tak organizačně náročná a nákladná.

Dle analýzy v předchozí práci autorů [4] a ze zdrojů [3,4,12] vyplývá, *že uvedený argument neplatí v případě zavádění umělé inteligence a virtuální reality, kde je vhodné 3D objekty virtuální reality identifikovat (např. přímo digitálním dvojčetem reálného fyzického prvku)*. Digitální dvojče, jakým je takový prvek, může integrovat bezpečnostní parametry dle výše uvedeného procesního modelu. To znamená, že lze zavést citlivostní parametry pro identifikovaný digitální objekt a posuzovat jeho kritičnost. Dále lze provádět požadované operace na základě teorie citlivostí či teorie grafů, výsledky interpretovat a digitálně vizualizovat.

V budoucnu lze očekávat standardizaci technologie digitálních dvojčat z důvodu eliminace uvedených implementačních bariér a její zlevnění. V tomto případě je nezbytné prosazovat zavedení bezpečnostních parametrů, tj. zavedení citlivostních parametrů a hodnocení důležitosti uzlů a vazeb v systému dle procesního modelu. V následujících částech bude tento koncept dále prozkoumán a diskutován v kontextu proaktivního zajištění bezpečnosti SoS

3. METODOLOGIE A ZPRACOVÁNÍ DAT

Metodologie použitá v této práci se opírá o systematickou rešerši a analýzu příkladů implementace digitálních dvojčat. Klíčovým cílem je vyhodnotit možnosti integrace bezpečnostních parametrů v souladu s navrženým procesním modelem. Získané výsledky jsou následně porovnány s aplikací tohoto modelu v předchozí práci, která se specificky zaměřovala na zajištění bezpečnosti v provozu pražského metra.

3.1. Rešerše a výběr příkladů

Pro výběr vhodných příkladů jsme využili veřejně dostupné zdroje (internet) a vědeckou online platformu Researchgate [13], kde jsou publikované abstrakty a plné příspěvky uvedené v řadě dostupných vědeckých databází.

Kritériem výběru vhodného článku byla věcnost a konkrétnost implementačních příkladů digitálních dvojčat, jelikož na běžně dostupných stránkách technologických firem jsou většinou uvedené pouze obecné marketingové informace týkající se možnosti aplikací bez konkrétních referencí. Jedná se o poměrně mladou a moderní technologickou oblast, jejíž původ se dle [14] datuje do roku 1991 jako koncept [15] a jeho první implementace až roku 2002 pro NASA [16], tudíž dostupnost kvalitních prací v oblasti zájmu, specificky pro integraci bezpečnostních resp. citlivostních parametrů, je zatím dost limitovaná.

Vedle již výše uvedených publikací jsme provedli rešerši dále uvedených prací:

1. „Digital Twins of Organization: Implications for Organization Design“ [17].
2. „Digital Twin as a Service (DTaaS): A Platform for Digital Twin Developers and Users“ [18].
3. „Digital Twin for Healthcare Systems“ [19].

Na základě provedené rešerše má největší poměr odborných prací v oblasti digitálních dvojčat oblast zdravotnictví. Jde o využívání digitálních dvojčat při podpoře diagnostiky a léčby různých zdravotních indikací.

3.2. Analýza a porovnání výsledků

Použitá metody analýzy možností zavedení bezpečnostních parametrů v příkladech implementace digitálních dvojčat je založená především na porovnání současného stavu a praxe na základě rešerše popsané v předchozím odstavci a reálné implementace zavedeného procesního modelu v pracích [4,8].

Předchozí práce zaměřená na bezpečnost provozu pražského metra [8], neobsahuje část zahrnující implementaci technologie digitálních dvojčat, ovšem nabízí konkrétní metodologie zavedení procesního modelu založené na kombinaci heuristických metod (např. bezpečnostní výzkum založený na metodě Dephi) s exaktními a pravděpodobnostními metodami interpretace (teorie citlivostí a teorie grafů) s moderními metodami řízení bezpečnosti (defence in depth). Uvedené metody jsou detailněji popsané v [8]. Představená metodologie obsahuje části implementovatelné v rámci digitálních dvojčat.

3.3. Shrnutí

Rešerše a porovnání provedené v předložené práci spočívají v hledání společných metodických oblastí, ve kterých se jednotlivé kroky implementace procesního modelu překrývají, nebo alespoň nevylučují s technologií digitálních dvojčat. Cílem je nalezených oblastech najít synergie pro efektivní implementaci uvedeného procesního modelu do technologie digitálních dvojčat na vhodné úrovni abstrakce.

4. VÝSLEDKY A HODNOCENÍ

Práce zaměřená na implementaci digitálních dvojčat (dále jen ***DT***) v organizaci, zavádí více typů DT [17]:
- fyzické objekty nebo věci (***DTT***),
- podnikové procesy (***DTBP***), a
- jejich transformace do podnikové organizace (***DTO***).

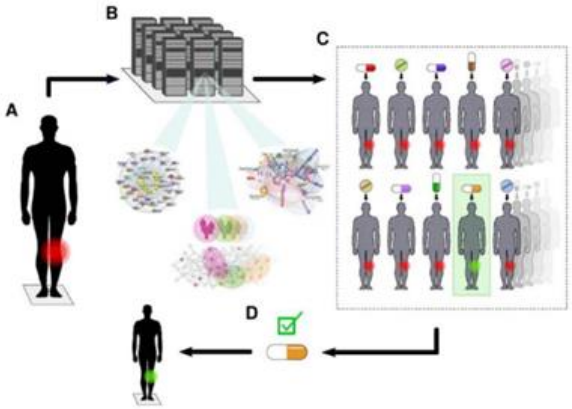
Tři typy DT můžeme přirovnat k posuzovaným skupinám aktiv v rámci procesního modelu dle [4,8]:
- konstrukce,
- technika,
- personál,
- místa,
- funkce,
- vazby a toky,
- organizace a ekonomika.

Jednotlivá aktiva v uvedených skupinách jsou poté vhodnými adepty pro zavedení entity digitálního dvojčete. Typy DTT, DTBP a DTO jsou ve skupinách aktiv zastoupeny, ale mají odlišné rozdělení. Identifikace aktiv a rozdělní do skupin je předmětem 1. procesu dle našeho procesního modelu (kapitola 2). Metody identifikace a rozdělení v rámci DT stále chybí a jde o základní bariéru implementace DT, tj. problém znalosti provozního prostředí, organizace a kvality dat. Problém organizace má být řešen podle náznaků v současných pracích pomocí DTO.

Implementace DT například ve zdravotnictví, jak popisují např. práce [14,19], jsou zaměřené na prediktivní analýzu zdravotního stavu lidí a prediktivní intervenci, tj. proaktivní preventivní léčba. DT implementuje procesy učení a simulací pro následné vyhodnocování stavů a možností prevence a léčby. Práce [19] s odkazem na [20] popisuje následující principy konceptu DT:

1. Vytváření neomezených replik ***sítě*** vzorců všech molekulárních, fenotypických a environmentálních faktorů souvisejících s mechanismy nemocí u jednotlivých pacientů pomocí digitálních dvojčat.
2. Výpočetní léčení těchto digitálních dvojčat tisíci léčiv k identifikaci nejlépe fungujícího léku.

3. Léčba pacienta tímto lékem, viz obrázek 1.



Obr. 1. Koncept Digitálního Dvojčete pro Personalizovanou Medicínu [19], *zpracováno dle* [20].

V bodě 1 se tedy jedná o identifikaci aktiv, hrozeb a vztahů mezi nimi, interpretované sítí, které lze definovat teorií grafů (proces 2. dle procesního modelu, uvedeného v odstavci 2). Bod 2. je operace s grafy pomocí známých algoritmů, resp. se zde nabízí algoritmy nové, popřípadě doplněné o heuristiky provedené umělými výpočetními systémy, tj. umělou inteligencí (proces 3. dle procesního modelu, uvedeného v odstavci 2). Třetí bod, léčba, je už reakce na základně vyhodnocení (proces 5. dle procesního modelu, uvedeného v odstavci 2).

Obrázek 1 ilustruje koncept digitálního dvojčete pro personalizovanou medicínu. Jak popisuje [19]:
- *„pacient ve fázi A má regionální symptom nemoci na obrázku 1 červený bod.*
- *Ve fázi B vzniká neomezené množství kopií pacientova digitálního dvojčete. Tyto kopie jsou vytvořeny na základě výpočetních modelů, reprezentujících tisíce proměnných souvisejících s nemocí.*
- *Ve fázi C je každé dvojče výpočetně léčeno jedním nebo více z tisíců léků. To vede k digitální léčbě pacienta (zelená).*
- *Ve fázi D je pro léčbu pacienta vybrán lék, který měl nejlepší účinek na digitální dvojče.“*

Analogicky lze výše uvedený model převést i do průmyslu a řízení bezpečnosti technických děl. Manažer odpovědný za bezpečnost musí ale k jednotlivým výsledkům přistupovat individuálně a průběžně je validovat.

Nadějnou míru abstrakce použitelnou pro více oblastní poskytuje práce [18], která popisuje ***DT na platformě poskytující DT jako službu (DTaaS)***. Softwarová platforma DTaaS považuje DT za znovupoužitelná aktiva. Tato aktiva skládá a konfiguruje určitým způsobem a používá čtyři kategorie aktiv: data (D), model (M), funkce (F) a nástroj (T).

Data (D) se vztahují ke zdrojům a cílům digitálního dvojče (DT). Zdroje dat mohou být výsledky měření fyzického dvojčete (PT) nebo testovací data od výrobců. Cíle dat zahrnují software pro vizualizaci, externí uživatele a úložiště dat.

Modelu (M) popisuje různé aspekty fyzického dvojčete (PT) a jeho prostředí s různou úrovní abstrakce. Je možné mít pro stejné PT více modelů. Například robot v automobilové výrobně může mít model(y) struktury sledující opotřebení dílů. Tento robot může mít i model(y) chování popisující bezpečnostní záruky a model(y) funkčnosti, které popisují jeho výrobní schopnosti.

Funkce (F) slouží především k přípravě a pozdějšímu zpracování datových vstupů a výstupů, včetně kontrolních výstupů. Funkce vytvořené odborníky v konkrétním oboru mohou s vhodnými datovými vstupy usnadnit kalibraci modelů digitálních dvojčat. Funkční aktiva také zpracovávají data senzorů a fyzických a digitálních dvojčat.

Aktiva DT dle práce [18] nejsou aktivy modelů uvedených předchozích případech, ale dle teoretického rozboru umožňují jejich implementaci. Práce [18] poskytuje také odkaz na zdrojový kód popisovaného softwarového nástroje. DTaaS nabízí konfigurovatelnou implementaci DT v různých oblastech, protože implementuje pouze abstraktní prvky, které je zapotřebí v rámci finálního nasazení konfigurovat.

DTaaS může po analýze legislativních a licenčních politik sloužit jako vhodný nástroj pro validaci nastavených bezpečnostních parametrů v rámci navrženého procesního modelu. Bezpečnostní parametry a volba metod

neexistují zcela samostatně bez konkrétních systémových DT. Proto je potřeba vytvořit více příkladů a na reálných datech příklady testovat.

5. DISKUZE A ZÁVĚR

Výzkum prezentovaný v této práci ukazuje potenciální přínosy implementace digitálních dvojčat (DT) v různých oblastech, především v průmyslu, se zaměřením na zlepšení bezpečnosti technických zařízení a děl. Výzkum identifikuje klíčové výzvy, jako jsou potřeba hlubšího pochopení prostředí pro implementaci DT, nutnost správné organizace a zajištění kvality dat.

Předložená práce poukazuje na možnosti implementace digitálních dvojčat (DT) v průmyslu, se zaměřením na zlepšení bezpečnosti technických zařízení a System of Systems (SoS). Zjištění potvrzují, že integrace DT do procesního modelu SoS může snížit kritičnost technických děl, což je klíčové pro zajištění vyšší bezpečnosti. Přesto je třeba tuto metodu dále testovat a ověřovat na konkrétních případech v praxi.

Naše studie zdůrazňuje potřebu dalšího systematického výzkumu a analýzy v oblasti bezpečnosti SoS s použitím DT, včetně vývoje specifických nástrojů, algoritmů a heuristik pro efektivní nasazení DT v průmyslu. Závěry poskytují podklad pro budoucí výzkum a praktické aplikace DT ke zlepšení bezpečnostních opatření technických systémů a zařízení.

LITERATURA

[1] KERTIS, T., PROCHÁZKOVÁ, D. Řízení bezpečnosti technologických děl z pohledu systémů systémů. In: *Řízení rizik procesů a bezpečnost složitých technických děl*. ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 277-287.

[2] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 978-80-01-06180-0, e-ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364 p. Doi: 10.14311%2FBK.9788001061824

[3] KINT. *Co je to IIoT, Digital Twin a Industrial Metaverse*? https://www.kint.cz/cs/veda-technika/iot-digital-twin-industrial-metaverse/ ISSN 2788-161X

[4] KERTIS, T., PROCHÁZKOVÁ, D. Využití moderních technologií Průmyslu 4.0 v bezpečnosti. In: *Řízení rizik procesů, zařízení a složitých technických děl zacílené na bezpečnost.* ISBN 978-80-01-07060-4. Praha: ČVUT DSPACE 2022, pp. 80-86. http://hdl.handle.net/10467/104996. Doi:10.14311/BK.9788001070604

[5] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. ISBN 978-80-01- 05103-0. Praha: ČVUT 2012, 318 p.

[6] BOARDMAN, J., SAUSER, B. System of Systems – the Meaning of. In: *IEEE/SMC International Conference on System of Systems Engineering*. Los Angeles: CA 2006, 6 p. Doi: 10.1109/SYSOSE.2006.1652284

[7] KERTIS, T., PROCHÁZKOVÁ, D. Reduce of Criticality of Critical Infrastructure Facilities in the Railway Domain. In: *Smart Cities Symposium Prague 2015 Proceedings - Czech Technical University in Prague*. Praha: IEEE 2015, pp. 1-4. Doi: 10.1109/SCSP.2015.7181565.

[8] KERTIS, T. Posouzení bezpečnosti vybraného kritického objektu z pohledu integrální bezpečnosti a návrh na snížení kritičnosti objektu. *Doktorská disertační práce.* Praha: ČVUT 2021, 124 p.

[9] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. Doi: 10.14311%2FBK.9788001066096

[10] IAEA. *IAEA Safety Glossary: 2018 Edition*. Vienna: IAEA 2018, 261 p. https://www.iaea.org/publications/11098/iaea-safety-glossary2018-edition

[11] PERNO, M., HVAM, L., HAUG, A. Implementation of Digital Twins in the Process Industry: A Systematic Literature Review of Enablers and Barriers. *Computers in Industry*, 134 (2022). doi: 10.1016/j.compind.2021.103558

[12] SIEMENS. *Siemens and NVIDIA To Enable Industrial Metaverse*. https://www.plm.automation.siemens.com/global/en/our-story/newsroom/siemens-xcelerator-nvidia-omniverse-industrial-metaverse/108414

[13] RESEARCHGATE. https://www.researchgate.net

[14] ÜNAL, ALIYE, TORAMAN, AYNUR. Evaluation of Digital Twin Technology. *SDU Healthcare Management Journal.* ISSN 2757-5888. 5 (2023),1, pp. 1-25.

[15] GELERNTER, D. *Mirror Worlds: or the Day Software Puts the Universe in a Shoebox...How It Will Happen and What It Will Mean*. ISBN 0-19-506812-2. Oxford: Oxford University Press 1993, 256 p.

[16] GRIEVES, M. W., VICKERS, J. H. *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*. In: *Transdisciplinary Perspectives on Complex Systems*. E-ISSN 978-3-319-38756-7. Springer 2017, pp 85–113.
[17] LYYTINEN, K., WEBER, B., BECKER, M., PENTLAND, B. Digital Twins of Organization: Implications for Organization Design. *Journal of Organization Design* 2023. doi: 10.1007/s41469-023-00151-z.
[18] TALASILA, P., GOMES, C., MIKKELSEN, P., GIL, S., KAMBURJAN, E., LARSEN, P. Digital Twin as a Service (DTaaS): *A Platform for Digital Twin Developers and Users* 2023.
[19] VALLÉE, A. Digital Twin for Healthcare Systems. *Frontiers in Digital Health*. 5 (2023). doi: 10.3389/fdgth.2023.1253050.
[20] SDTC. *Swedish Digital Twin Consortium "The Concept*". SDTC 2012. https://www.sdtc.se/#concept.

PŘESNOST MĚŘENÍ TLOUŠŤKY POVLAKŮ A RIZIKA ZPŮSOBENÁ ŠPATNĚ ZVOLENOU MĚŘÍCÍ TECHNIKOU

ACCURACY OF COATING THICKNESS MEASUREMENT AND RISKS CAUSED BY POORLY SELECTED MEASURING TECHNIQUE

Jiří Kuchař, Milan Petřík, Viktor Kreibich, Eva Jančová

ČVUT v Praze, Fakulta strojní, Technická 4, 166 07, Praha 6; jiri.kuchar@fs.cvut.cz

Abstrakt: Článek pojednává o měření tloušťky povlaků a o rizicích způsobených špatně zvolnou měřící technikou, která způsobí, že tloušťka povlaku je nepřesně změřena. Je popsán základní princip měření tloušťky. Na zhotovených vzorcích bylo provedeno měření tloušťky povlaku a jejich následné vyhodnocení v porovnání s mikroskopickými měřeními povlaku.

Klíčová slova: Povrchová úprava, měření tloušťky, povlak, riziko, tloušťka.

Abstract: The article deals with the measurement of coating thickness and the risks caused by poorly selected measuring techniques, which cause the coating thickness to be inaccurately measured. The basic principle of thickness measurement is described. The samples were used to measure the thickness of the coating and to evaluate them in comparison with microscopic measurements of the coating.

Key words: Surface treatment, thickness measurement, coating, risk, thickness.

1. ÚVOD

Vhodně zvolená povrchová úprava a kontrola jejich vlastností, např. správně aplikované povrchové úpravy a správné tloušťky povlaku, určuje spolehlivost výrobku. Měření tloušťky povlaku a vrstev, v oboru povrchových úprav, je důležitým faktorem, na kterém závisí životnost a spolehlivost výrobku, který je používán v určitém prostředí. Tloušťka povlaků a vrstev se dá zjistit různými způsoby. Základní rozdělení způsobů měření je:

- destruktivní metody měření tloušťky (DT), kdy je nutné měřený objekt destruktivně upravit,
- nedestruktivní měření tloušťky (NDT), kdy je měření rychlé a kdy není třeba měřený objekt destruktivně upravovat.

Cílem článku je porovnání výsledků metod nedestruktivních a metod destruktivních a zhodnocení, která technologie měření povlaku je vhodná pro daný typ povrchové úpravy i použitý základní materiál.

2. MĚŘENÍ TLOUŠŤKY POVLAKŮ A VRSTEV

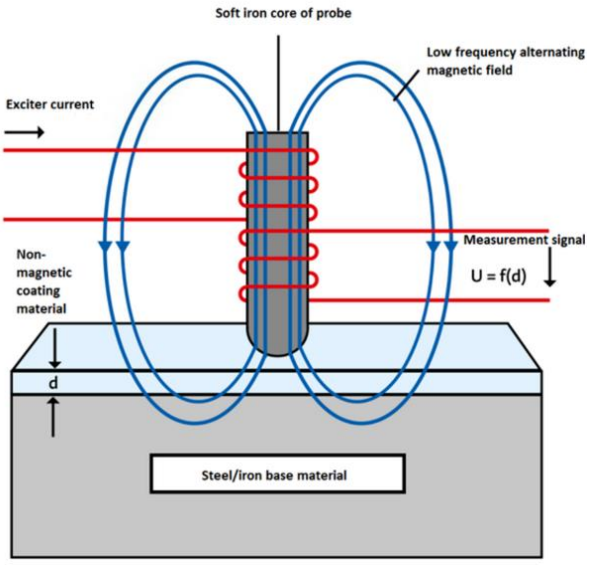
Měření tloušťky povlaků a vrstev lze rozdělit na destruktivní a nedestruktivní technologie. Rozdíl mezi tím je, jestli je nutné výrobek destruktivně připravit, aby bylo možno měření provést, nebo jestli ho lze rovnou měřit, aniž by se musel výrobek nějak upravovat, respektive destruktivně připravovat povlak k následnému měření.

2.1 Destruktivní technologie měření tloušťky

Nejčastěji jsou používány čtyři destruktivní technologie (DT). Profilometrická metoda [1] je využitelná pro kovové povlaky v rozsahu měření od 0,01 až 1000 μm pro rovinné a ve speciálních případech i válcové povrchy; nedoporučuje se využívat v nižším rozsahu měření tloušťky. Další technologií je mikroskopická metoda [2], kdy lze zhotovit příčný nebo klínový řez povlaku, ze kterého pak lze následně pod světelným mikroskopem stanovit tloušťku povlaku. Předmětná metoda je vhodná i pro tenké povlaky a nezáleží na typu povlaku a druhu základního materiálu [2,3]. Coulometrickou metodu [4] lze také využít na měření tloušťky kovových povlaků, poněvadž využívá elektrickou vodivost povlaku k jeho rozpuštění. Tuto technologii měření je možné využít i pro vícevrstvé povlaky[4]. Gravimetrická metoda [5] využívá rozdíl plošné hmotnosti před a po pokovení a je využitelná pro kovové a nekovové povlaky pro kovové a nekovové podklady.

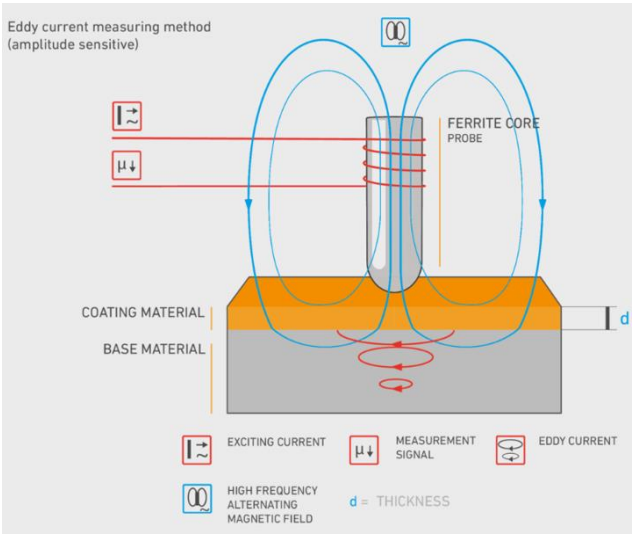
2.2 Nedestruktivní technologie měření tloušťky

Nedestruktivních metod (NDT) měření je celá řada, zmíníme se o metodách, které jsou používány nejčastěji. Patří sem magnetická metoda [6], která využívá vlastnosti feromagnetických materiálů, které přitahuje magnet a je využitelná pro kovové a nekovové povlaky na feromagnetických materiálech. Další metodou je magneticko-indukční metoda [2,7], která se využívá k měření nemagnetických povlaků na magnetickém základním materiálu, kdy se při měření využívá cívka budiče, která je navinuta na železné jádro, kterým je poté veden nízkofrekvenční střídavý proud v rozsahu Hz . Schéma měření magneticko-indukční metodou je na obrázku 1.



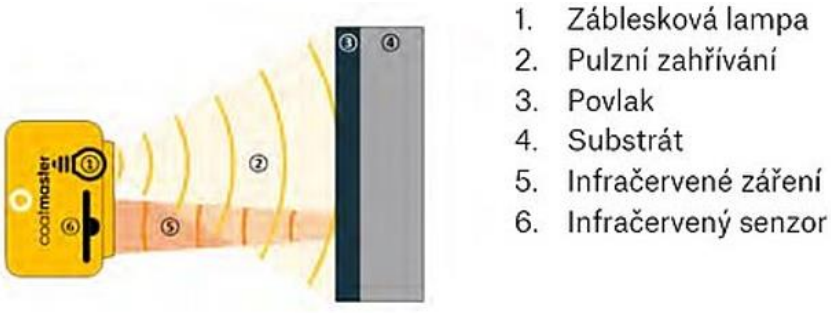
Obr. 1 Scéma měření magneticko-indukční metodou [7].

Metodu vířivými proudy [2,8] lze použít pro nekovové povlaky na nemagnetickém podkladu, protože využívá principu vyhodnocování zpětného působení vířivých proudů vybuzených v nemagnetickém kovovém podkladu. Měření tloušťky povlaku ultrazvukem [9,10] využívá šíření ultrazvukového signálu povlakem, odraz signálu na rozhraní odlišných materiálů. Předmětnou metodu měření lze použít pro širokou škálu materiálů zahrnující kovy, plasty, kompozity a keramiku. Schéma měření metodou vířivých proudů je na obrázku 2.



Obr. 2. Scéma měření vířivými proudy [8].

V poslední době byla vyvinuta metoda k měření tloušťky povlaku, která je nazývána ATO, neboli „Advanced Thermal Optics“ (pokročilá tepelná optika) [11,12], která měří povlaky už ve stavu, kdy je povlak nanesen a ještě nezaschl, bezkontaktně. Metoda je velmi přesná a reprodukovatelná. Tato metoda impulsně zahřívá měřený povrch, kde následně stanovuje dynamiku ochlazování pomocí vysokorychlostních infračervených senzorů, kde se povrch skenuje bezkontaktně a pomocí algoritmů je stanovena tloušťka povlaku. Schéma měření pomocí bezkontaktní tepelné optiky je na obrázku 3.



Obr. 3 Scéma měření pomocí bezkontaktní tepelnou optikou [12].

Dále lze nedestruktivně měřit povlaky, tzv. rentgeno-spektrometrickou metodou [13,14], u které princip měření spočívá v tom , že rentgenové záření dopadá na povrch s povlakem, měří se intenzita sekundárního záření vysílaného podkladem a tlumeného povlakem.

3. EXPERIMENT

K experimentu byly použity vzorky s různými povrchovými úpravami na vybraných základních materiálech. Byly použity tyto kombinace:
- ocelový smaltovaný vzorek se základním a krycím smaltem,
- ocelový vzorek galvanicky pozinkován,
- ocelový vzorek žárově pozinkován,
- ocelový vzorek s chemickou předúpravou a práškovým plastem,
- vzorek Inconel 625 s niklovým návarem s příměsí bóru,
- hliníkový vzorek s anodickou oxidací
- a hliníkový vzorek s povlakem z práškového plastu.

Posléze byly vzorky nedestruktivně měřeny různými technologiemi, a to:
- metodou magneticko–indukční,
- metodou vířivých proudů
- a ultrazvuková metodou.

Celkem bylo naměřeno 12 hodnot tloušťky povlaku, ze kterých byla odstraněna nejvyšší a nejnižší hodnota a zbytek hodnot byl zprůměrován.

Následně byly vzorky děleny a zabroušeny, kvůli aplikaci metod DT. Tloušťky povlaků byly stanoveny pomocí dvou mikroskopů. Naměřená data byla upravena stejně jako při měření nedestruktivním způsobem.

Naměřené výsledky z NDT a DT metod byly porovnány a každému vzorku byly přiřazeny vhodné NDT metody, podle podobnosti s výsledky z mikroskopického měření.

4. VÝSLEDKY MĚŘENÍ NEDESTRUKTIVNÍMI METODAMI A POROVNÁNÍ S MIKROSKOPY

Všechna měřidla byla před použitím kalibrována pomocí kalibračních fólií, popř. kalibračních měrek. Nejdříve bylo využito magneticko-indukční metody, následně byla použita metoda měření tloušťky povlaku pomocí vířivých proudů a jako poslední využita metoda ultrazvuková. Pro proměření vzorků nedestruktivními metodami bylo přistoupeny k rozřezání, odebrání a úpravě vzorku k měření pomocí mikroskopů.

Dle literatury [15] byla využita následující měřící technika:

1. Positector, který kombinuje princip měření magneticko-indukční metody s metodou měření pomocí vířivých proudů a je vhodný pro duplexní povlaky kovového charakteru v kombinaci s organickým charakterem povlaku.
2. Elcometer 456, který využívá magneticko-indukční metody.
3. Leptoskop Karl Deutsch, který využívá měření tloušťky povlaku pomocí vířivých proudů.
4. Pro měření pomocí ultrazvuku přístroje Olympus 72 DL a Olympus 38 DL.
5. Mikroskop Keyence VHX-6000.
6. Stereomikroskop SZ61.

Pro měření magneticko-indukční metodou použit tloušťkoměr Elcometer 456 s měřící sondou FM3. Pro měření vířivými proudy byl použit tloušťkoměr Leptoskop Karl Deutsch a dvou sond, kde jedna byla pro feromagnetické (Fe) podklady (KD Fe 0-3000 µm 2442.100 10153) a druhá pro neferomagnetické (NFe) podklady (KD NFe 0-1000 µm 2442.130 10081). K měření ultrazvukem byly použity přístroje Olympus 72 DL Plus se sondou 75 MHz M2102. Druhý byl ultrazvuk Olympus 38 DL Plus se sondou 5 MHz D7906-RM. Pro porovnání byly využity následující mikroskopy: Olympus SZ61 a Keyenece VHX-6000.

Bylo provedeno 12 měření, kdy největší a nejmenší hodnota byla zanedbaná a ostatní hodnoty byly zprůměrovány. V tabulkách 1 až 8 jsou hodnoty zprůměrovaných měření a porovnání použité přístrojové techniky k měření tloušťky. Tyto hodnoty naměřené nedestruktivními technologiemi byly následně porovnány s mikroskopickými hodnotami.

Tabulka 1. Porovnání jednotlivých metod měření pro smaltovaný vzorek [15].

Smalt											
Positector		Elcometer		Víř. Proudy		Ultrazvuk		Stereoscope		VHX - 6000	
B	Č	B	Č	B	Č	B	Č	B	Č	B	Č
146,5	31,6	127,7	21,7	153	25,6	57,5	Ø	108,7	24,3	106	27,9

Pomocí magnetické indukce a měření pomocí vířivých proudů se měřila celá vrstva povlaku po celé ploše. Byl proměřen povlak složený se základního a krycího smaltu. Dále byly obě hodnoty odečteny (hodnota v tabulce označená jako B mínus hodnota v tabulce označená jako Č), získají se správné výsledky tloušťky bílého krycího smaltu.

Tabulka 2. Odečtené hodnoty pro stanovení tloušťky bílého krycího smaltu [15].

Smalt		
B	B	B
114,9	106	127,4

Po proměření a porovnání jednotlivých metod jsou mikroskopickým hodnotám nejblíže naměřené magneticko-indukční metodou a metodou pomocí vířivých proudů. Odchylky v měření jsou způsobeny typem povlaku a jeho nestejnoměrné tloušťce v jednotlivých místech měření. Pro tento typ vzorku (povlaku a základního materiálu) jsou použitelné technologie na bázi magneticko-indukční metody a metody měření pomocí vířivých proudů. Naopak se při tomto měření projevilo nevhodné použitý ultrazvuku k měření tloušťky.

Tabulka 3. Porovnání jednotlivých metod měření pro galvanický pokovený vzorek [15].

Galv. Zinek					
Positector	Elcometer	Víř. Proudy	Ultrazvuk	Stereoscope	VHX - 6000
5,3	3,9	5,2	36,9	Ø	Ø

Pro měření povlaku typu galvanický zinek nastal problém s pozorováním a změřením tloušťky povlaku i při použití mikroskopů. Povlak byl sice tenký, ale při lepší přípravě vzorku a správném naleptání by bylo možné pozorovat i měřit dané povlaky mikroskopicky. Všechny nedestruktivně použité metody jsou použitelné pro určení tloušťky povlaku vytvořených galvanickým vylučováním. Sice hodnoty z Elcometeru jsou o něco nižší, ale to může být způsobeno měřením tloušťky povlaku po ploše, a ne ve stejných místech. Ultrazvuk je pro tento typ povlaku nevhodné použít.

Tabulka 4. Porovnání jednotlivých metod měření pro galvanicky pokovený vzorek [15].

Žár. Zinek					
Positector	Elcometer	Víř. Proudy	Ultrazvuk	Stereoscope	VHX - 6000
74,3	67,6	75,7	54,3	Ø	50,5

Pro žárově pozinkovanou ocel bylo vhodné využití magneticko-indukční metody i metody měření pomocí vířivých proudů. Překvapivé bylo, že i ultrazvuk dokázal vhodně naměřit tloušťku žárově pokoveného zinku, což mohlo být zapříčiněno i danou technologií pokovení, která difunduje do základního materiálu.

Tabulka 5. Porovnání jednotlivých metod měření pro práškově povlakovaný ocelový vzorek s chemickou předúpravou železitým fosfátováním [15].

Prášek bílá							
Positector	Elcometer	Víř. Proudy	Ultrazvuk	Stereoscope		VHX - 6000	
225,2	193,1	223,7	225,2	B 126,4	Č 105,6	B 120,5	Č 106,3
				232		226,8	

Při tomto měření použité tloušťkoměry měřily povlak jako celek a nebylo jimi možné určit mezivrstvu (chemickou předúpravu železitým fosfátem). Naopak měření pod mikroskopy byla vrstva povlaku dobře viditelná a měřitelná. Pokud by byl požadavek na celkovou tloušťku povlaku s vytvořenou mezivrstvou, bylo by možné použít využité technologie NDT. Pokud by byl povlak vícevrstvý a bylo by potřeba znát každou vrstvu povlaku zvlášť, bylo by nutné použít jinou technologii měření povlaku, např. destruktivní mikroskopickou metodu, či NDT metodu měření povlaku na bázi ručních rentgenových analyzátorů.

Tabulka 6. Porovnání jednotlivých metod měření pro anodickou oxidaci na slitině hliníku [15].

Elox					
Positector	Elcometer	Víř. Proudy	Ultrazvuk	Stereoscope	VHX - 6000
Ø	Ø	4,6	22,9	Ø	Ø

Při tomto měření byla vrstva anodické oxidace velmi malá a těžko měřitelná i pod mikroskopy. Pokud by se lépe vzorek metalograficky připravil, byla by dobře měřitelná i pomocí mikroskopů. Naopak pro tento typ povlaku a základního materiálu je dobře použitelná metoda měření pomocí vířivých proudů.

Tabulka 7. Porovnání jednotlivých metod měření pro práškově povlakovaný hliníkový vzorek [15].

Prášek žlutá					
Positector	Elcometer	Víř. Proudy	Ultrazvuk	Stereoscope	VHX - 6000
38,1	Ø	57,3	31,7	70	52,9

Práškový plast na hliníkový vzorek byl nanesen v nepravidelné tloušťce, proto u tohoto typu vzorku byla statistika při měření velmi důležitá. Vzorek byl lehce měřitelný pomocí mikroskopů, pokud by bylo ale nutno použít nedestruktivní metodu měření, bylo by vhodné použít měření tloušťky pomocí vířivých proudů.

Tabulka 8. Porovnání jednotlivých metod měření návaru na Inconel 625 [15].

Návar						
Positector	Elcometer	Víř. Proudy	Ultrazvuk		Stereoscope	VHX - 6001
Ø	Ø	Ø	Vršek 13 900	Spodek 10 150	3 638	3580
			3 750			

Návar na Inconelu byl těžce měřitelný díky použité přístrojové technice a jejím rozsahů. Pomocí mikroskopů byl návar lehce měřitelný a při použití ultrazvuku byl měřen na dvakrát, kdy se měřil vzorek z vrchu, kde byl návar a vzorek ze spodu, kde byl základní materiál. Po proměření těchto hodnot musely být hodnoty od sebe odečteny, aby se získala správná tloušťka návaru. Ultrazvuk se tedy ukázal vhodný při měření návarů, popř. svarů.

6. RIZIKA SPOJENÁ S MĚŘÍCÍ TECHNIKOU

Výsledky experimentů odhalily, že přesnost měření závisí na:
- technice měření a kvalitě měřícího přístroje u jednotlivých metod (odchylky některých měření byly příliš velké, a tak je bylo třeba vyloučit, aby střední hodnota byla rozumná), což souhlasí s poznatky uvedenými v práci [16]. Proto bude třeba aplikovat při experimentech PSM (Process Safety Management), jak doporučuje práce [17,18],
- propojení měřící techniky a materiálového složení povlaku i jeho přípravě.

Uvedená fakta budou uplatněna při dalších měřeních.

7. ZÁVĚR

Přístrojová technika neustále posouvá své hranice, jak z hlediska svých limitů, či z hlediska své přesnosti. Cílem experimentů bylo zjistit a ověřit možnosti měřících přístrojů pro vybrané typy materiálů a vybrané typy povrchových úprav. Bylo studováno, jestli vůbec daný měřící princip daný vzorek naměří a s jakou přesností. Závěrem bylo doporučení, která měřící technika je vhodná pro vybrané vzorky, respektive základní materiály a jejich povrchové úpravy, čímž lze eliminovat riziko špatně zvolené měřící techniky, a nejen její kalibrace.

Poděkování: Článek byl podpořen projektem SGS22/156/OHK2/3T/12 (Vliv povrchových úprav na kvalitu výrobních technologií).

LITERATURA

[1] ÚNMZ. ČSN EN ISO 4518. *Kovové povlaky: měření tloušťky povlaku. Profilometrická metoda.* Praha. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví 2021.
[2] ÚNMZ. ČSN EN ISO 2808. *Nátěrové hmoty: stanovení tloušťky nátěru.* Praha. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví 2020.
[3] ÚNMZ. ČSN EN ISO 1463. *Kovové a oxidové povlaky: měření tloušťky povlaku. Mikroskopická metoda.* Úřad pro technickou normalizaci, metrologii a státní zkušebnictví 2021.
[4] ÚNMZ. ČSN EN ISO 2177. *Kovové povlaky: měření tloušťky povlaku. Coulometrická metoda anodickým rozpouštěním.* Úřad pro technickou normalizaci, metrologii a státní zkušebnictví 2004.
[5] ÚNMZ. ČSN EN ISO 10111. *Kovové a jiné anorganické povlaky - Měření plošné hmotnosti - Přehled gravimetrických a chemických analytických metod.* Úřad pro technickou normalizaci, metrologii a státní zkušebnictví 2019.
[6] ÚNMZ. ČSN EN ISO 2178. *Nemagnetické povlaky na magnetických podkladech - Měření tloušťky povlaku - Magnetická metoda.* Úřad pro technickou normalizaci, metrologii a státní zkušebnictví 2017.

[7] DOERKEN. *Magnetic Induction Measurement.* https://www.doerken.com/global/en/services/coatings /glossary/ magnetic-induction-measurement
[8] FISCHER. *Amplitude Sensitive Eddy Current.* https://www.helmut-fischer.com/measurement-technologies-in-use/amplitude-sensitive-eddy-current
[9] FLYABILITY. *Ultrasonic Testing: A Guide*. https://www.flyability.com/ultrasonic-testing
[10] EWP. *Ultrasonic Testing.* https://www.wermac.org/others/ndt_ut.html
[11] BOGNER, M., REINKE, N. A. *Process Optimization with Contactless Measurement*. Doi:10.1007/s35784-021-0352-9
[12] POSPÍŠILOVÁ, M. *Bezkontaktní měření tloušťky povlaku*. https://www.gamin.cz/profil-spolecnosti/pu blikace /bezkontaktni-mereni-tloustky-povlaku/
[13] ÚNMZ. ČSN EN ISO 3497. *Kovové povlaky - Měření tloušťky povlaku - Rentgenospektrometrické metody*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví 2002.
[14] GIURLANI, W. G. BERRETTI, E. INNOCENTI, M. LAVACCHI, A. *Coating Thickness Determination Using X-ray Fluorescence Spectroscopy: Monte Carlo Simulations as an Alternative to the Use of Standards.* ISSN 2079-6412. https://www.mdpi.com/2079-6412/9/2/79
[15] TYLE, O. Destruktivní a nedestruktivní metody měření tloušťky povlaků a vrstev v rámci technologií povrchových úprav. *Bakalářská práce FS ČVUT v Praze*. Praha: ČVUT 2023, 70 p.
[16] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Data a metodika jejich zpracování pro potřeby inženýrských disciplín*. ISBN 978-80-01-05792-6. Praha: ČVUT 2015, 186 p.
[17] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessee: US DOE 1996, 180 p.
[18] PROCHAZKOVA, D. Methodology for Implementation of Process Safety Management into Experiment Life Cycle. *Design, Construction, Maintenance.* E-ISSN 2732-9984. 3 (2023), pp. 187-196 Doi: 10.37394/232022.2023.3.16

RIZIKA PROVOZU JADERNÝCH ZAŘÍZENÍ

RISKS OF OPERATION OF NUCLEAR FACILITIES

Martina Malá[1], Karel Vidlák[2]

[1] *Centrum výzkumu Řež s.r.o., martina.mala@cvrez.cz*
[2] *ČEZ, a.s., Jaderná elektrárna Temelín, 373 05, Temelín, karel.vidlak@cez.cz*

Abstrakt: Při provozu jaderné elektrárny vznikají různá rizika, se kterými je třeba se vypořádat tak, aby po celou dobu jejich životnosti byla zajištěna jejich bezpečnost a koexistence s okolím. Způsob problematiky řešení vychází se současného preferovaného přístupu, ve kterém je bezpečnost nadřazena spolehlivosti.

Klíčová slova: Jaderná elektrárna, riziko, technické dílo, bezpečnost, zdroje rizik, havárie.

Abstract: During the operation of a nuclear power plant, various risks arise, which must be dealt with in such a way as to ensure their safety and coexistence with the surrounding world throughout their lifetime. The method of solving the problem is based on the current preferred approach, in which safety is superior to reliability.

Key words: Nuclear Power Plant, risk, technical facility, safety, sources of risks, accident.

1. ÚVOD

Jaderné elektrárny jsou významným veřejným aktivem, které nám zajišťují energetickou soběstačnost státu, a tak přispívají ke kvalitě života lidí. Proto je důležité zajistit jejich bezpečnost, tzn. cíleně a proaktivně pracovat s riziky [1].

Každá lidská činnost přináší rizika, a proto je důležité nejprve rozpoznat zdroje rizik, ocenit jejich nepřijatelné dopady v jednotlivých místech a stanovit velikost možných ztrát a škod v závislosti na rozložení veřejných aktiv, a dále rozdělit rizika na přijatelná, podmíněně přijatelná a nepřijatelná. Celý svět se dynamicky mění, a tak se mění i procesy, které vyvolávají jevy. Z tohoto důvodu se škodlivý potenciál pohrom v čase mění a s ním i velikost rizik, které pohromy pro veřejná aktiva představují [1,2].

Rizika spojená s technickými díly, tedy i jadernými elektrárnami, dle [1,2] jsou rozdělena na:
- nepřijatelná – u nich je zapotřebí zajistit aplikaci účinných preventivních opatření vůči jejich zdrojům,
- podmíněně přijatelná – u nich je nutné mít připravena zmírňující, reaktivní a obnovující opatření pro sledovaná aktiva,
- přijatelná – u nich je třeba sledovat, zda v čase nedojde ke zvýšení škodlivého potenciálu jejich příčin.

Uvedeným způsobem dle [1,2] provádíme činnost nazvanou „řízení rizik“.

Pojem riziko je obecně používán již od středověku. V dnešní době můžeme najít obecnou definici říkající, že riziko je součin velikosti následků určité události a pravděpodobnosti, že k události dojde v určitém časovém období [3]. Každý jednotlivec si pod pojmem riziko představí jinou, jemu vlastní definici. Z tohoto důvodu je třeba sjednotit definované pojmy a standardy, aby bylo riziko porovnatelné. Pro oblast energetiky je riziko definováno jako pravděpodobná velikost nežádoucích dopadů (ztrát, škod a újmy) na chráněná aktiva při výskytu pohromy. Souvisí s pohromou a s místem, ve kterém se nachází sledované aktivum. Ohrožení souvisí s pohromou, ale nesouvisí s místem, kde se nachází sledované aktivum [1]. Riziko [1] je místně specifické a závisí, zda v daném místě jsou sledovaná aktiva.

2. RIZIKA JADERNÝCH ZAŘÍZENÍ OBECNĚ

Žádné technické dílo není možné navrhnout a postavit stoprocentně bezpečné. Nějaká rizika tu budou vždy. Pak ale záleží na tom, jaká jsou a zda jsou přijatelná, nebo ne. Nikdy nelze vyloučit lidský faktor, ať už se jedná o jakoukoliv technologii. Zde pak také mluvíme o přijatelnosti rizika pro lidskou společnost. Některá rizika jsou pro člověka přijatelná a denně se s nimi potýká (např. způsob životního stylu), jiná méně. Potřeba je také dodat, že

vnímání rizik člověkem je subjektivní a jedno riziko může pro různé lidi znamenat jinou míru rizikovosti. Navíc může člověk některá rizika vnímat zkresleně, např. z nedostatku informací.

Průmyslový rozvoj některá rizika snižuje a některá jiná zase zvyšuje. Můžeme klidně říct, že rizika jaderných elektráren jsou na srovnatelné úrovni s riziky v ostatních průmyslových odvětvích, jako je těžba surovin, výstavba přehrad, lodní doprava, rafinerie apod.

Pro srovnání, na rakovinu v ČR zemře ročně cca 28 tisíc lidí [4]. V důsledku znečištění ovzduší jemnými částicemi v EU v roce 2020 předčasně zahynulo, dle odhadů Evropské agentury pro životní prostředí, kolem čtvrt miliónu lidí [5]. Na druhé straně se odhaduje, že jaderná energetika celosvětově zachránila již 1,84 miliónů lidí, kteří by zemřeli na zdravotní následky spojené se znečištěním ovzduší [6].

S provozem jaderných zařízení je spjata celá řada rizik jako u jiných technologických celků. Ovšem ta nejvíce viditelná jsou právě rizika spojená s použitím jaderného paliva a produkcí radioaktivních látek a doprovodného ionizujícího záření, včetně rizika vzniku jaderné nehody či havárie s potencionálním dopadem na obyvatelstvo.

Úroveň bezpečnosti jaderného zařízení závisí významně na úrovni a způsobu řízení rizik. Vlastník a provozovatel jaderného zařízení by měl znát současná rizika jaderného zařízení i rizika předvídatelná, a neustále správně vyhledávat nová rizika, všechna rizika správně pochopit a vyhodnotit a kontrolovat, zda se s nimi optimálně nakládá. Práce s riziky spočívá ve správném ocenění velikosti možných událostí všeho druhu, které mohou být zdrojem rizik pro jaderné zařízení, a vypořádat se tímto rizikem tak, aby bylo přijatelné ve smyslu principu ALARA [2].

Princip ALARA dle [7] znamená, že:
- obecně přijatelným rizikům se nevěnuje pozornost,
- pro podmínečně přijatelná rizika se přizpůsobuje řízení technického díla tak, aby dopady takového rizika byly přijatelné,
- pro nepřijatelná rizika se provedou opatření v projektu a na základě soustavného monitoringu proměnných rizik, která nelze zmírnit opatřeními v projektu, se upravuje řízení technického díla i řízení jeho okolí tak, aby se zmírnily nepřijatelné dopady.

To znamená, že pro úspěšné řízení rizik jakéhokoliv technického díla je zapotřebí řešit prioritní rizika a jejich aspekty. Prioritní riziko je takové riziko, při jehož realizaci průměrné škody, ztráty a újmy na chráněných aktivech na zvolenou časovou jednotku jsou větší než zvolená hranice přijatelnosti [2].

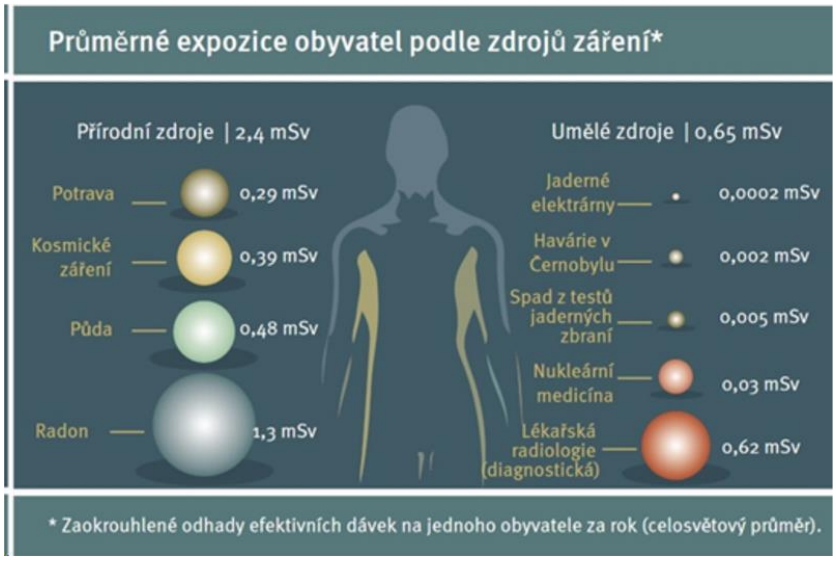
Mezi další vnímaná rizika jaderných zařízení můžeme zařadit zranitelnost důležité infrastruktury v důsledku terorismu, geopolitické nestability nebo ztrátu dostupnosti surovin pro výrobu jaderného paliva. V poslední době vzniká nová hrozba v podobě kybernetického útoku na jaderná zařízení, který může mít značné nepřijatelné důsledky. V průběhu provozu vznikají nová rizika plynoucí z opotřebování a vyčerpání životnosti kritických komponent a nutnosti nových investic do obnovy těchto komponent a také investic do neustálého zlepšování bezpečnosti. Nemalé riziko představují rozsáhlé výpadky elektrické sítě, kdy jaderné zařízení je nuceno pracovat v ostrovním režimu. Provoz dále ovlivňují výkyvy cen energií a s tím spojený ekonomický ukazatel provozu i obecný názor obyvatel na provoz jaderného zařízení a s tím související nejvíce vnímané riziko ionizujícího záření a jeho vlivu na obyvatelstvo. Příspěvek dávek z provozu jaderných zařízení je zanedbatelný [8], jak je uvedeno na obrázku 1. Procentuální rozdělení dávek obyvatelstva z různých přírodních a umělých zdrojů záření [8] je uveden v grafu na obrázku 2.

3. BEZPEČNOST JADERNÝCH ZAŘÍZENÍ

Již nařízení US Atomic Energy Council [9] z roku 1947 uvádí, že pravděpodobnost havárií s velkým únikem radioaktivních látek musí být maximálně snížena, následky těchto havárií musí být minimalizovány, projekt reaktoru musí mít kontejnment a musí být umístěn v odlehlé oblasti. V roce 1949 Edward Teller [10] uvedl, že skutečné nebezpečí pro bezpečnost je její podcenění v důsledku našeho sebeuspokojení. Stejné havárie se nesmí opakovat, jejich opakování znamená, že událost nebyla dostatečně analyzována, nebyla zjištěna kořenová příčina, anebo nebyla navržena a realizována potřebná nápravná opatření.

Zpráva WASH-740 z roku 1957 [10] hovoří o teoretických možnostech a následcích havárií velkých jaderných zařízení spojených s tavením paliva nebo havárií s velkými radiačními následky. V průběhu více jak 18 tisíc reaktor-roků provozu jaderných elektráren ve světě došlo k řadě havárií jaderných zařízení [11,12], některé i s tavením paliva, např. v roce 1979 elektrárna v USA, TMI-2 s typem reaktoru PWR [13,14], v roce 1986 v bývalém SSSR, elektrárna Černobyl s typem reaktoru RBMK-1000 [15] nebo poslední v roce 2011 v Japonsku, Fukushima Daiichi s reaktory typu BWR [16]. Tyto události ukázaly na nutnost včas a objektivně informovat

obyvatelstvo a sdělovací prostředky. Jen pro zajímavost, reaktory umístěné na lodích a ponorkách mají ve světě více než 13,5 tisíc reaktor-roků provozu [17].



Obr. 1. Průměrná expozice obyvatel podle zdrojů záření [8].

Obr. 2. Rozdělení zdrojů dávek pro obyvatelstvu [8]

Jaderné havárie se hodnotí podle mezinárodní stupnice hodnocení závažnosti jaderných událostí INES (International Nuclear Event Scale). Tato stupnice má 7+1 stupňů [18]:

1. Stupeň 0: odchylky: bez bezpečnostního významu, a tedy mimo stupnici.
2. Stupně 1–3: nehody:
   - 1: anomálie: např. přezáření jednotlivce z obyvatel dávkou přesahující stanovené limity,
   - 2: nehoda: významné selhání bezpečnostních opatření (předpisů) bez skutečných následků,
   - 3: vážná nehoda: „téměř havarijní stav“ v jaderné elektrárně, kdy nezůstala k dispozici žádná bezpečnostní opatření, v provozním prostoru dávkové příkony > 1 Sv/hod., vážná kontaminace v prostoru, kde to projekt nepředpokládá, ale s malou pravděpodobností významného ozáření obyvatel, neletální deterministický zdravotní účinek (např. popáleniny) v důsledku ozáření.

3. Stupně 4–7: havárie:
   - 4: havárie s místními následky: Tavení paliva nebo poškození paliva vedoucí k uvolnění více jak 0,1% inventáře aktivní zóny, uvolnění významného množství radioaktivních látek uvnitř zařízení s vysokou pravděpodobností významného ozáření obyvatel, minimálně jedno úmrtí v důsledku radioaktivního záření,
   - 5: havárie s širšími následky: vážné poškození aktivní zóny jaderného reaktoru, uvolnění velkého množství radioaktivních látek uvnitř zařízení s vysokou pravděpodobností významného ozáření obyvatel, ke kterému by mohlo dojít při velké kritické havárii nebo požáru, Omezený únik radioaktivních látek, který bude pravděpodobně vyžadovat nasazení některých plánovaných protiopatření, Několik úmrtí v důsledku radioaktivního záření,
   - 6: těžká havárie: Významný únik radioaktivních látek, který bude pravděpodobně vyžadovat nasazení plánovaných protiopatření,
   - 7: velmi těžká havárie: Velký únik radioaktivních látek s rozsáhlým rozptýlením; účinky na zdraví obyvatel a životní prostředí vyžadující nasazení plánovaných a rozšířených protiopatření.

Stupnice INES byla zavedena Mezinárodní agenturou pro atomovou energii (IAEA) a OECD/NEA až v roce 1990 [18], tudíž hodnocení událostí, které nastaly dříve, se provádělo zpětně.

4. RIZIKA JADERNÝCH ZAŘÍZENÍ

Příčiny rizik, které způsobily havárie jaderného zařízení, můžeme rozdělit do následujících skupin [2]:
- lidský faktor,
- chyby v řízení jaderného zařízení,
- design elektrárny s technickými nebo technologickými nedostatky,
- nedostatečná kultura jaderné bezpečnosti,
- nulový/nedostatečný dozor,
- nedostatečné vnímání rizik,
- nedostatečné řízení rizik,
- přítomnost radioaktivních látek,
- přítomnost ionizujícího záření,
- útoky.

Příčinou havárií nebývá vždy jen jedna příčina, ale v převážné většině se jedná vždy o souběh událostí a kumulace více slabých míst jaderného zařízení [14-16]. Pro příklad můžeme uvést havárii první Československé jaderné elektrárny Jaslovské Bohunice, která byla uvedena do provozu v roce 1972 s reaktorem typu KS-150, který byl plynem chlazený a těžkou vodou moderovaný a používal přírodní uran jako palivo [19,20] (poznámka: stávající bloky v Dukovanech a Temelíně používají palivo s obohaceným uranem). Tento reaktor umožňoval kontinuální výměnu paliva za provozu. Slabiny designu „experimentální elektrárny“, který měl prověřit provozuschopnost daného typu reaktoru [21], malé provozní zkušenosti a lidský faktor [22] vedly ke dvěma událostem INES. První se stala v roce 1976, kdy došlo k nedosednutí palivového souboru a následnému úniku chladiva, což zapříčinilo ztrátu chlazení reaktoru, zamoření reaktorové místnosti radioaktivními látkami a únik chladiva CO_2 [11]. Právě únik CO_2 způsobil udušení dvou zaměstnanců. Událost byla ohodnocena INES 2-3 [22]. V únoru 1977 došlo k zanesení paliva a ztrátě chlazení palivového souboru. To způsobilo propálení paliva a následnou kontaminaci technologie radioaktivními látkami. [19,22] Událost byla hodnocena stupněm INES 4 [23]. Tato druhá událost pak vedla k trvalému odstavení jaderné elektrárny z provozu [19].

Dalším příkladem je jaderná elektrárna Three Mile Island (TMI-2), která byla postavena době „boomu“ jaderné energetiky s ověřeným tlakovodním reaktorem západní konstrukce PWR, který používá tlakovou vodu jako chladivo i moderátor [14]. Slabý design primárního okruhu, provedení blokové dozorny, nedostatečně dimenzovaný kontejnment a lidský faktor [14,24,25] byly příčinou havárie, ke které došlo v březnu 1979. Na elektrárně došlo k netěsnosti za kompenzátorem objemu a následnému vypuštění chladiva z primárního okruhu. Nastalo obnažení palivových souborů a únik radioaktivních látek mimo kontejnment. Havárie byla hodnocena stupněm INES 5. Poškozený blok byl vyřazen z provozu [14].

Událost hodnocena nejvyšším stupněm INES 7 se stala v dubnu 1986 v jaderné elektrárně Černobyl [15,26]. Nevhodně plánovaný test doběhu turbíny a prodloužení provozu v době plánované odstávky bloku, kdy mělo palivo vysoký stupeň vyhoření na konci kampaně, snížení výkonu reaktoru pod povolenou mez, odpojení ochran reaktoru, ignorování zkušeností z podobných provozů, na test nepřipravená nová směna, porušení pravidel a nedokonalý design umožňující vnos kladné reaktivity, která způsobuje zvyšování výkonu vedly k velké havárii v jaderné

energetice. Při havárii došlo ke značnému úniku aktivity (v řádu 10^{19} Bq) [26]. Bylo evakuováno celé město Pripjať a kolem elektrárny vytvořena uzavřená tzv. „Zóna“ [27]. Havárie způsobila akutní nemoc z ozáření u pracovníků elektrárny a hasičů, více o tom je v [26]. Vyšší dávky záření dostalo více jak 600 tisíc osob podílejících se na likvidaci havárie a osob žijících v blízkosti zničeného reaktoru [26,28]. S havárií se pojí také značná ekonomická zátěž [26]. K havárii přispělo nevhodné bezpečnostní řešení některých prvků reaktoru typu RBMK a utajování informací o tomto modelu reaktoru [29]. Do dnešního dne je v provozu ještě 8 bloků tohoto typu reaktoru, z toho 3 až do roku 2050 [30].

Design elektrárny navržený pro menší vlnu tsunami, nevhodné umístění baterií, nepřipravené diesel generátory a chybějící provozní předpisy pro takto těžké havárie byly příčinou další velké havárie jaderné v elektrárně Fukushima Daiichi v březnu 2011 a jejích následků [16,31,32,33]. Tato událost byla hodnocena také nejvyšším stupněm INES 7. Zemětřesení v Tohoku o síle 9 Richterovy stupnice způsobilo záplavovou vlnu tsunami. Tři bloky v té době byly v provozu a během zemětřesení byly bezpečně odstaveny. Tím se snížilo největší riziko, a to značný tepelný výkon reaktoru. Odstavením reaktoru sice není možné tepelný výkon reaktoru zcela vypnout, dále je generován zbytkový výkon paliva a aktivní zónu je třeba nadále dochlazovat, ovšem takto generovaný tepelný výkon je řádově nižší. Dalším dopadem v daném případě je ionizující záření. Jaderné palivo je po odstavení reaktoru více aktivní než po delší době dochlazování v bazénech. Chladicí voda palivo nejen dochlazuje, ale také stíní generované ionizující záření. Při ztrátě chlazení se začne voda přehřívat, odpařovat a palivo se obnaží, začne se přehřívat, při překročení jisté meze začne oxidovat za vzniku vodíku, až může nakonec dojít k tavení paliva. Krátce po zemětřesení však ještě pracovaly záložní zdroje energie a odstavené reaktory byly chlazeny. Zbylé tři bloky elektrárny byly v odstávce, na čtvrtém bloku bylo palivo vyvezeno z reaktoru do bazénu a na pátém a šestém bloku bylo palivo v reaktoru.

Ovšem po asi jedné hodině dorazila vlna tsunami, na jejíž velikost nebyla elektrárna dimenzována. Došlo k zaplavení diesel generátorů a přerušení externího napájení. Výčet událostí byl delší, ovšem to není předmětem tohoto článku. U prvního, druhého a třetího bloku došlo ke ztrátě chlazení, obnažení aktivní zóny s palivem a jejímu následnému poškození (došlo k tavení paliva). U prvního a třetího bloku navíc došlo k vodíkové explozi. U čtvrtého bloku, který nebyl v provozu, také došlo k vodíkové explozi, neboť se na něj přes propojené systémy dostal vodík ze třetího bloku. Pátý a šestý blok poškozeny nebyly. Následky této události byly značné. Havárie poukázala na řadu slabin (rizik) projektu elektrárny. S dopady této havárie se společnost potýká ještě dnes [16,31,32,33].

5. ZÁVĚR

V předchozím textu je uveden výčet několika příkladů jaderných havárií s různým stupněm INES. K největším rizikům provozu jaderných zařízení patří právě použití jaderných materiálů/radioaktivních látek s doprovodným ionizujícím zářením. Neboť takové podmínky pak zhoršují nepřijatelné dopady na samotnou technologii a případně také životní prostředí a obyvatele v případě havárie. Dojde-li k havárii, pak je velkým rizikem ztráta chlazení, neboť taková událost by mohla vést k obnažení paliva a jeho následnému poškození. To je spojeno s rizikem úniku radioaktivních látek z elektrárny do životního prostředí, rizikem vlivu na zdraví zaměstnanců i obyvatelstva, ale také rizikem vlivu na samotnou technologii, kterou bude nutné vyřadit z provozu dříve než po ukončení její životnosti. U poškozených bloků se pak doba vyřazování z provozu prodlužuje dle toho, jak je zrovna možné elektrárnu demontovat dostupnými technologiemi v závislosti na míře jejího poškození. Také likvidace následků havárie je potom obtížnější, neboť je limitována přítomností ionizujícího záření. To nakonec ukázaly havárie jaderných zařízení a jejich likvidace v různých místech světa [19,22,23].

Pro všechna jaderná zařízení však obecně platí, že mají společná i další rizika, a to technologická a lidský faktor. V dnešní době se do popředí dostávají ještě navíc rizika spojená s oblastí kybernetické bezpečnosti a geopolitickou situací [34].

Technologická rizika se z pohledu autorů článku týkají převážně designu elektrárny a jeho nedostatkům, jako je nedostatečně robustní design zařízení, nepřehlednost technologie, nevhodné provozní postupy nebo chybějící provozní postupy pro určité události [26,31].

Rizika lidského faktoru pak z pohledu autorů článku představuje nerespektování pravidel a postupů, nedostatečná kultura jaderné bezpečnosti, nedostatečné zaškolení personálu, malé zkušenosti s provozem jaderných zařízení, ignorování zkušeností z předchozích událostí, nulový či nedostatečný jaderný dozor [20,26].

Závěrem je nutné dodat, že ačkoliv je seznam jaderných havárií dlouhý a seznam rizik provozu jaderných zařízení také, tak se provozovatelé, výrobci a další odborníci z nastalých rizik poučují a jaderné technologie se dále vyvíjejí a zdokonalují. Pozornost byla zaměřena nejen na technická vylepšení projektu jaderné elektrárny, ale také na

významné omezení pravděpodobnosti selhání člověka [26]. Po černobylské události došlo k zahájení mezinárodního sdílení zkušeností v oblasti jaderné oblasti, neboť havárie ukázala, že jaderná bezpečnost není otázkou pouze státu, ve kterém se jaderné zařízení nachází [26]. Dalším příkladem mohou být zavedená nápravná opatření na podporu bezpečnosti elektráren ve světě, které po havárii ve Fukushimě prošly stress testy [35]. Dalším příkladem může být urychlení vývoje jaderných paliv odolných vůči haváriím, a to také po události ve Fukushimě [36].

LITERATURA

[1] 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

[2] 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/BK.978800106 6751

[3] JANKŮ, J. Ekologická rizika, monitoring a analýza. https://cv.vscht.cz/files/uzel/0014041/0029~~MzIwtNQNNQ7TdcxLzKmsSlQoyqzKzAYA.pdf?redirected

[4] https://www.novinky.cz/clanek/domaci-pocet-lidi-s-rakovinou-se-ztrojnasobi-40228452

[5] https://www.eea.europa.eu/cs/highlights/pocet-predcasnych-umrti-v-dusledku

[6] https://atominfo.cz/2015/08/jsou-rizika-jaderne-energetiky-opravdu-tak-velka/, dne 25. 07. 2023

[7] SMITH, D., SIMPSON, K. *Safety Critical Systems Handbook – A Straightforward Guide to Functional Safety*, IEC 61508 and Related Standards. ISBN 978-0-08-096781-3. Geneve: ISO 2010. 270 p.

[8] https://www.sujb.cz/radiacni-ochrana/prirodni-zdroje-ionizujiciho-zareni/ozareni-z-prirodnich-zdroju-zareni, dne 20. 05. 2023

[9] MAZUZAN, G. T., WALKER, J. S. *Controlling the Atom. The Beginnings of Nuclear Regulation 1946-1962.* ISBN 0-520-05182-3. Berkley: University of California Press. 1985. 529 p.

[10] KŘÍŽ Z. *Poučení z havárií a událostí v jaderné oblasti.* Řež: Centrum výzkumu Řež 2016.

[11] http://edu.techmania.cz/cs/encyklopedie/fyzika/atomy-castice/jaderna-elektrarna/nejvetsi-havarie-jadernych-elektraren

[12] https://www.sujb.cz/jaderna-bezpecnost/ines/priklady-udalosti

[13] https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html

[14] https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/three-mile-island-accident.aspx

[15] https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

[16] https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-daiichi-accident.aspx

[17] https://world-nuclear.org/information-library/current-andfuture-generation/nuclear-power-in-the-world-today.aspx, dne 20. 05.2023

[18] https://www.sujb.cz/jaderna-bezpecnost/ines/stupnice-ines

[19] https://www.osel.cz/11052-kolik-stoji-likvidace-vyslouzile-jaderne-elektrarny.html

[20] https://inis.iaea.org/collection/NCLCollectionStore/_Public/37/110/37110257.pdf

[21] https://www.cez.cz/edee/content/file/static/encyklopedie/vykladovy-slovnik-energetiky/hesla/je_jaslboh.html

[22] https://edu.techmania.cz/cs/encyklopedie/fyzika/atomy-castice/jaderna-elektrarna/jaslovske-bohunice

[23] https://www.cez.cz/edee/content/file/static/encyklopedie/encyklopedie-energetiky/03/havarie_7.html

[24] https://www.nrc.gov/docs/ML0614/ML061430367.pdf

[25] https://tmi2kml.inl.gov/Documents/2b-Rogovin/NUREGCR-1250V1,%20TMI,%20A%20Report%20To%20The%20Commissioners%20And%20To%20The%20Public%20(Rogovin%20Report)%20(1980-01).pdf

[26] https://www.sujb.cz/fileadmin/sujb/docs/cernobyl/cernobylska_havarie.pdf

[27] https://www.sujb.cz/fileadmin/sujb/docs/cernobyl/2021/Havarie_Cernobyl_-_35_let_pote.pdf

[28] https://www.osel.cz/6247-ernobyl-a-fukusima.html

[29] https://www.osel.cz/9537-soucasny-stav-a-budoucnost-jaderne-energetiky.html

[30] https://www.world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/appendices/rbmk-reactors.aspx

[31] https://www.osel.cz/5627-japonsko-prirodni-katastrofa-zasahla-ctyri-jaderne-elektrarny.html

[32] https://www.osel.cz/6196-je-fukusima-srovnatelna-s-ernobylem.html

[33] https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1710-ReportByTheDG-Web.pdf

[34] https://www.sujb.cz/aktualne/detail/nukib-a-sujb-spoji-sve-sily-pri-posilovani-bezpecnosti-cr

[35] https://www.sujb.cz/aktualne/detail/fukusimska-havarie-rok-pote
[36] https://www.nrc.gov/reactors/power/atf/roadmap/origins.html

SPRÁVA AKTUALIZACÍ: KLÍČOVÝ PRVEK V BOJI PROTI KYBERNETICKÝM HROZBÁM

PATCH MANAGEMENT: A KEY ELEMENT IN THE FIGHT AGAINST CYBER THREATS

Andrej Pastorek

ČVUT v Praze. Fakulta dopravní. Konviktská 20, 110 00 Praha 1. Česká republika. andrej.pastorek@gmail.com

Abstrakt: Článek je zaměřen na problematiku automatizace správy a evidence update firmware a software v heterogenních sítích v rámci specifických systémů i jednoúčelových technologií Internetu věcí, využívaných v kritických infrastrukturách, s primárním zaměřením na oblast zdravotnické techniky v nemocnicích. Zabývá se analýzou kybernetické bezpečnosti v oblasti správy a evidence aktualizací, oprav a záplat, ale i v nastavení procesů, které pomáhají získávat, testovat a instalovat opravy existujících aplikací v počítačích a dalších systémech, jež mají udržovat systémy na potřebné úrovni zabezpečení proti kyberútokům. Tato činnost aktualizací základních funkčních FW zůstává pro většinu organizací správy IT na okraji zájmu. Přitom s nástupem Internetu věcí se digitální technologie rozšiřují do mnoha dalších oblastí a k Internetu se připojí miliardy nových zařízení. Je již dostatečně prokázáno, že kybernetické útoky, využívající slabiny a chyby firmware v zařízeních, která až dosud pracovala v off-line režimu, mohou paralyzovat celou počítačovou síť a způsobit milionové škody.

Klíčová slova: Správa aktualizací, kybernetická zranitelnost, zdravotnická zařízení a přístroje, kybernetické útoky na nemocnice.

Abstract: The article is focused on the issue of automated administration and evidence of firmware and software updates in heterogeneous networks within specific systems and single-purpose Internet of Things technologies, used in critical infrastructures, with a primary focus on the field of medical technology in hospitals. It deals with the analysis of cyber security in the area of managing and recording updates, upgrades and patches, as well as setting up processes that help acquire, test and install patches of existing applications in computers and other devices to maintain systems at the necessary level of security against cyberattacks. This activity of updating basic functional firmware remains of marginal interest for most IT management organizations. With the advent of the Internet of Things, digital technologies are expanding to many other areas, and billions of new devices will connect to the Internet. It has already been amply proven that cyberattacks exploiting weaknesses and firmware bugs in devices, which have been until now operating offline, can paralyze the entire computer network and cause millions of dollars in damage.

Key words: Patch management, cybersecurity vulnerability, medical devices and instruments, cyberattacks on hospitals.

1. ÚVOD

Patch management systémy jsou dnes klíčovou součástí správy IT infrastruktury v organizacích po celém světě. Jejich důležitost spočívá v tom, že umožňují efektivní a bezpečnou aktualizaci softwarových aplikací a operačních systémů. Aktualizace, známé také jako "patche," jsou klíčové z několika důvodů:

1. Bezpečnostní ochrana: Patche často obsahují opravy a aktualizace, které eliminují známé bezpečnostní chyby a zranitelnosti v softwaru. Ignorování těchto aktualizací může způsobit, že organizace bude zranitelná vůči kybernetickým útokům, což může mít katastrofální následky.
2. Optimalizace výkonu: Aktualizace mohou zlepšit výkon aplikací a systémů, což znamená rychlejší a efektivnější práci zaměstnanců a snížení rizika výpadků.
3. Dodržování předpisů: Mnoho organizací podléhá regulacím a zákonům týkajícím se ochrany dat a zabezpečení. Patch management systémy pomáhají zajistit dodržování těchto předpisů tím, že udržují systémy aktuální a bezpečné.
4. Minimální rušení provozu: Dobře spravované patch management systémy umožňují plánovat a provádět

aktualizace bez výrazného narušení běžného provozu organizace, což minimalizuje přestávky a výpadky.

Patch management systémy jsou nepostradatelné pro zajištění bezpečnosti, stability a efektivity IT infrastruktury organizace. Ignorování této důležité složky správy IT činí příslušnou organizaci zranitelnou a ohroženou různými hrozbami.

2. SOUČASNÝ STAV

Udržování aktuálního stavu softwarových systémů pomocí aplikací bezpečnostních oprav je zásadním bezpečnostním požadavkem, který se bohužel zanedbává. Řešení této situace je proto jedním z hlavních cílů nařízených kontrolních skenů vycházejících z článku 11. směrnice EU NIS2 [1]. Selhání při opravě systémů může vést ke zničujícím následkům a významný počet narušení kybernetické bezpečnosti je tudíž výsledkem zneužití zranitelnosti operačních systémů nebo firmware, pro kterou již byla aktualizační oprava většinou k dispozici, ale nebyla instalována. Otevření dveří pro kybernetický útok neaktualizováním bezpečnostních záplat je jedním z nejčastějších důvodu úspěchu kyber-zločinců způsobujících milionové škody. Minimalizace škod a jejich příčin je také jedním z úkolů vyplývajícího z dokumentu „Akční plán k národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025“ [2].

V současné době existují sice systémy řešení průběžného a co nejvíce automatizovaného systému managementu aktualizací [3], ale ty jsou většinově zaměřeny na kontroly aktuálnosti operačních systémů a aplikací, nikoliv na systémový firmware nepočítačových zařízení. Organizace se spoléhají na aktivitu výrobce zařízení, popřípadě dodavatele. Pokud ale tato povinnost aktualizovat nevyplývá ze smlouvy, nejedná se o závadu, a odpovědnost za škody je tak na provozovateli zařízení.

Evidence verzí firmware se obvykle nevede a jediné údaje jsou obvykle součástí ekonomické evidence dodávek. Zodpovědný informatik vede někdy evidenci v rámci excelovské tabulky, bohužel ovšem s periodicitou ověřování aktualizací velmi sporadickou, popřípadě žádnou.

Tomuto nežádoucím stavu by měly odpomoci automatizované prostředky evidence a ověřování dostupnosti aktualizací, a to jak napříč obecně používanými systémy výrobců, tak i specializovaných výrobců zařízení. S rostoucím počtem nových specializovaných zařízení disponujících svou počítačovou části s možností připojení do sítě roste podíl otevřeného prostoru pro kybernetickou infiltraci a zvýšení zranitelnosti.

Správa bezpečnostních oprav ve velkých a složitých systémech je velmi náročný úkol, který zahrnuje různé zúčastněné strany a vzájemně provázaná technologická a sociálně-ekonomická hlediska. Vysoká míra četnosti vydání opravných aktualizací, narušení chodu organizace, způsobené potenciálními chybnými opravami a případnou nutností restartu po instalaci opravy činí daný proces ještě náročnějším. Podle nedávných statistik americké Komise pro cenné papíry (US Securities and Exchange Commission) [4] se více než 50 % organizací nachází ve stavu, kdy nejsou schopny opravit kritické zranitelnosti do 72 hodin od vydání záplaty a přibližně 15 % „děravých“ systémů zůstává neopraveno i po 30 dnech. Důkazy, plynoucí z rostoucího počtu bezpečnostních incidentů naznačují, že bude zapotřebí značné množství úsilí, které by pomohlo překonat tento tíživý stav, jenž dnes platí při využívání tradičních IT zařízení, systémů a aplikací. S nástupem Internetu věcí lze očekávat významné rozšíření a prohloubení problematického stavu. To vedlo i tvůrce směrnice EU NIS2 [5] k výraznému rozšíření zodpovědnosti a zvýšení sankcí s ohledem na dopady v rámci kybernetické bezpečnosti nejenom na ekonomiku států, ale i politicko-ekonomické důsledky hybridních konfliktů.

Na úrovni známých řešení se jedná o systémy skoro výhradně v intencích a pod správou jednotlivých výrobců. I když projevují jistou míru automatických režimů, přesto zůstává přímá instalace na vůli a času správců IT. Prozatím neexistuje žádné řešení spojující evidenci, aktuálnost, varování a následnou kontrolu v oblasti základních firmware hardwarových zařízení obecně. Také není v rámci specifika České republiky zohledněn historický stav mnoha dodavatelů různých značek a výrobců. Tito mnohdy již neexistují, popřípadě byli pohlceni konkurencí, a přesto se jejich výrobky i nadále používají bez ohledu na známá rizika. Systém aktualizací by tudíž měl i zohlednit tyto situace a přinejmenším varovat správce aktiv a manažéry kybernetické bezpečnosti pře integrací těchto zařízení do sítě. Zároveň by měl pružně reagovat na varování v rámci zákonných nařízení NÚKIB [6] a umět identifikovat zařízení a SW dodavatelů a jejich řetězců z rizikových oblastí.

Správa oprav zabezpečení v organizaci totiž zahrnuje více zúčastněných stran s různými úrovněmi zájmů a znalostí procesu. Chybějící komplexní znalosti na úrovní jednotlivých účastníků procesu vedou ke konfliktům mezi zúčastněnými stranami. Například vyšší management se dozvídá o nevhodnosti výrobce X ze země Y, ale obvykle se více zajímá o stabilitu chodu organizace, a tudíž věnuje pozornost stálosti a dostupnosti IT systémů, zatímco zájmy odborníků na bezpečnost se zaměřují na minimalizaci rizika a zájem aplikovat bezpečnostní záplaty co

nejdříve. To ovšem může mít za následek prostoje a výpadky systému, které ohrožují jeho trvalou dostupnost a mohou způsobovat nevoli u uživatelů. Přitom ale nejsou nijak stanoveny metodické postupy pro zhodnocení rizika jak v rovině společenské přiměřenosti, tak ekonomické náročnosti. Nedostatek znalostí představuje tradiční riziko, ale metody jeho hodnocení jsou dnes z hlediska potenciálních škod způsobených kyberútokem zastaralé. Jednou z hlavních nevýhod současných přístupů k hodnocení zranitelnosti a stanovení priorit je neschopnost pochopit jejich dynamický kontext.

3. PŘÍKLADY KYBERNETICKÝCH ÚTOKŮ NA ZDRAVOTNICKÁ ZAŘÍZENÍ PROSTŘEDNICTVÍM NEAKTUALIZOVANÉHO SOFTWARE NEBO FIRMWARE.

Pro ukázku naléhavosti řešení sledované problematiky uvedeme několik příkladů:

1. Jedním z nejpozoruhodnějších příkladů je útok ransomwaru WannaCry [7], ke kterému došlo v květnu 2017 [8]. Útok WannaCry zneužil zranitelnost, pro kterou byla vydána aktualizace několik měsíců před útokem. Mnoho organizací však opravu nepoužilo, takže jejich systémy byly vůči útoku zranitelné. Malware WannaCry se rychle šířil po sítích, šifroval soubory na infikovaných počítačích a požadoval platbu výměnou za dešifrovací klíč. Útok zasáhl více než 200 000 počítačů ve více než 150 zemích, včetně mnoha zdravotnických organizací [9]. Ve zdravotnictví útok WannaCry narušil provoz v nemocnicích a na klinikách, což způsobilo mj. odloženou léčbu. V některých případech byli pacienti kvůli útoku odmítnuti.
2. Lékařské kardiologické přístroje St. Jude - V roce 2017 vydal americký Úřad pro kontrolu potravin a léčiv (FDA) varování o zranitelnostech v srdečních zařízeních vyrobených společností St. Jude Medical (nyní Abbott) [10]. Tyto chyby zabezpečení by mohly útočníkovi umožnit vzdálené ovládání zařízení, což by způsobilo jeho poruchu nebo vybití baterie. FDA doporučila pacientům s postiženými zařízeními, aby kontaktovali svého poskytovatele zdravotní péče o aktualizaci.
3. Infuzní pumpy Hospira – V roce 2015 vydala FDA bezpečnostní sdělení o zranitelnostech infuzních pump vyráběných společností Hospira (nyní vlastněnou společností Pfizer) [11]. Tyto chyby zabezpečení by mohly útočníkovi umožnit vzdálené ovládání zařízení, což by způsobilo, že by buď nadměrně užíval léky nebo úplně zastavil infuzi. FDA doporučila poskytovatelům zdravotní péče, aby přestali používat postižené pumpy a přešli na alternativní infuzní systémy [12].
4. Přístroje MRI - V roce 2020 výzkumníci z Ben-Gurionovy univerzity v Izraeli demonstrovali útok na přístroj MRI. Útok zneužil zranitelnost ve firmwaru počítače k přepsání dat pacientů a vložení škodlivého kódu do softwaru stroje [13]. I když byl útok proveden v kontrolovaném prostředí a nepředstavoval skutečnou hrozbu, upozorňuje na potenciální rizika spojená se zranitelnými zdravotnickými prostředky.

4. EXISTUJÍCÍ PATCH MANAGEMENT SYSTÉMY

Problém lze částečně řešit využitím systémů pro management záplat (Patch Management Systems – PMS) [14]. Většinou se ovšem jedná o systémy pro management aktualizací na úrovni klasických operačních systémů a aplikací, které ale opomíjejí problematiku firmware, a tudíž se nehodí pro Internet věcí a nepočítačová zařízení, u nichž často platí rovnice, že firmware = kombinace velmi zjednodušeného OS + účel zařízení splňující aplikace. Přehled nejznámějších systémů tohoto druhu je uveden v tabulce 1.

Tabulka 7. Přehled PMS.

Systém	**Popis**
Ninja RMM [15]	Ninja RMM poskytuje nástroje pro správu endpointů (koncových zařízení), jako jsou počítače, servery, mobilní zařízení a další. Mezi hlavní funkce Ninja RMM patří monitorování stavu počítačových sítí a správa záplat.
Avast Business Patch Management [16]	Avast Business Patch Management nabízí automatizované řešení pro správu záplat, což znamená, že IT oddělení nemusí ručně hledat, stahovat a instalovat záplaty a aktualizace pro každý počítač v síti organizace. Avast Business Patch Management automaticky skenuje počítače v síti a detekuje chybějící záplaty a aktualizace. Nepodporuje

	aktualizace firmware, nejnižší úrovní jsou aktualizace ovladačů HW.
N-Central [17]	N-Central nabízí široké spektrum funkcí, včetně správy endpointů (koncových zařízení) jako jsou počítače, servery, mobilní zařízení a další. Tento software umožňuje IT oddělením spravovat a monitorovat své klienty a jejich počítačové sítě z jednoho centrálního rozhraní.
Cloud Acronis Cyber Protect [18]	Jedná se o integrovaný software, který kombinuje různé funkce jako zálohování a obnova dat, správu záplat, antivirovou ochranu, detekci a reakci na hrozby, správu koncových zařízení a další.
Jamf Pro [19]	Jamf Pro je software pro správu mobilních zařízení (MDM) a správu koncových zařízení (UEM) pro Apple produkty, jako jsou iPhone, iPad, Mac a Apple TV. Jamf Pro umožňuje organizacím snadno spravovat a nasazovat Apple zařízení a aplikace v rámci podnikového prostředí.
ManageEngine Desktop Central [20]	Desktop Central nabízí řadu funkcí, jako jsou: Správa konfigurace: umožňuje organizacím snadno nastavit a spravovat konfiguraci koncových zařízení, jako jsou Wi-Fi sítě, hesla, profily a další. Správa softwaru: umožňuje organizacím snadno spravovat a distribuovat software pro koncová zařízení. Desktop Central umožňuje organizacím vytvářet a spravovat vlastní software, ale také nabízí integraci s App Store a dalšími aplikacemi třetích stran. Správa aktualizací: umožňuje organizacím snadno spravovat aktualizace software pro koncová zařízení.
Syxsense [21]	SYXSENSE je cloudové řešení pro správu a zabezpečení IT, které poskytuje správu oprav, správu koncových bodů, nasazení softwaru a další související služby. Syxsense je navržen pro provoz v cloudu, protože se jedná o řešení Software-as-a-Service (SaaS), ke kterému se přistupuje prostřednictvím webového prohlížeče.

5. UPDATE SYSTÉMŮ VÝROBCŮ

Někteří z výrobců zdravotnické techniky poskytují pro své výrobky proprietární systémy patch managementu firmware:

1. Philips e-Alert - Philips [22] nabízí systém správy oprav nazvaný e-Alert, který je určen pro jejich zdravotnické prostředky. Systém automaticky odesílá oznámení poskytovatelům zdravotní péče, když je k dispozici oprava nebo aktualizace softwaru, a může vzdáleně opravu implementovat. Poskytuje také přehled o stavu oprav zařízení a také vytváří sestavy pro analýzu dodržování předpisů.
2. Capsule Patch Management - Capsule Technologies [23] nabízí systém správy oprav firmwaru pro zdravotnické prostředky, který se integruje s jejich platformou pro zapojení zdravotnických prostředků do sítě. Systém poskytuje automatickou detekci aktualizací firmwaru a oprav a může vzdáleně implantovat aktualizace do zařízení.
3. Banyan Medical Systems - Banyan Medical Systems [24] nabízí systém pro správu oprav firmwaru nazvaný Live Update, který je určen pro jejich software pro monitorování zdravotnických prostředků. Systém může vzdáleně provádět aktualizace.
4. Greenbone Networks [25] nabízí platformu pro správu zranitelností, která zahrnuje i možnosti správy záplat firmwaru. Systém je navržen pro různá odvětví, včetně zdravotnictví, a může skenovat zranitelná místa a automaticky nasazovat opravy a aktualizace. Zahrnuje také nástroje pro podávání zpráv o dodržování předpisů a hodnocení rizik.

6. PROBLEMATIKA NASAZENÍ SYSTÉMU

U organizací v naprosté většině neexistuje evidence, zda jsou existující aktualizace také použity. Aktualizace jsou tak zodpovědností jednotlivých uživatelů a správci aktiv. Toto však v praktickém provozu není řešeno ani technicky, ani organizačně, a to zvláště u organizací typu zdravotních služeb.

V současné době dle předběžného odhadu stavu v ČR a statistik ze zahraničí, velká většina institucí a středních a menších firem nepoužívá žádný systém evidence aktualizací. Výsledkem je stav, kdy za aktualizaci zařízení zodpovídají přímo jejich uživatelé, z nichž většina není počítačově tak gramotná, aby vyhledávala a instalovala aktualizace sama. V oblasti operačních systémů a u velkých komerčních aplikací je tento stav částečně sanován periodickým vydáním a automatizací aktualizací ve formě služby, se kterou se většina uživatelů obeznámena (např. Microsoft Update).

Pro firmware klasických IT zařízení a pro IoT komponenty se tato forma vyskytuje jen velmi zřídka, typicky v mediálních zařízeních (např. u set – top boxů nebo "chytrých" televizí). Počet zařízení vyžadujících aktualizace bude narůstat, a leckteré z nich budou představovat kritické hrozby ve zdravotnictví (např. infuzní pumpy, rentgenové skenery, analyzátory krevních plynů nebo zařízení na podporu života, jako jsou ventilátory), přičemž na základě předběžných zjištění [26] nevede evidenci aktualizací z deseti v ČR oslovených nemocnic ani jedna. Podobně nebezpečnou oblastí může být firmware autonomních vozidel, chytrých zásuvek, včetně nabíjecích stanic pro elektromobily, atd. apod.

7. ZÁVĚR

Z pohledu podniků spadajících do kritické infrastruktury státu je získání okamžitého přehledu o nutnosti aktualizací, jejich provádění, organizačním zajištění a stanovením zodpovědnosti nezbytnou podmínkou sine quo non pro zvýšení kybernetické bezpečnosti a odolnosti proti útokům. Zavedení evidenčního systému může přinést doplňující benefity (např. při kybernetickém útoku rychle identifikovat nejzranitelnější zařízení, tj. ta, u kterých nebyla aktualizace provedena, a ty buď urychleně vypnout nebo odpojit od IT sítě, aby se omezilo šíření nákazy. Podobně bude při evidenci komplikací spojených s update firmware již dopředu známo, která zařízení nebo aplikace nebudou po provedení aktualizace pracovat, což je častý případ u mnoha IoT zařízení.

LITERATURA

[1] https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS
[2] https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf
[3] https://doi.org/10.6028/NIST.SP.800-40r4
[4] https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf
[5] https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS
[6] https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf
[7] https://www.nukib.cz/cs/infoservis/hrozby/1455-ransomware-wannacry/
[8] https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
[9] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/
[10] https://www.reuters.com/article/us-abbott-stjude-heart-idUSKBN14T1WT
[11] https://www.reuters.com/article/us-hospira-fda-cybersecurity-idUSKCN0Q52GJ20150731
[12] https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/
[13] https://www.medicaldevice-network.com/news/medical-scans-cybersecurity-study/
[14] https://www.techtarget.com/searchenterprisedesktop/definition/patch-management
[15] https://www.ninjaone.com/
[16] https://www.avast.com/en-us/business/products/patch-management#pc
[17] https://www.n-able.com/
[18] https://www.acronis.com/cs-cz/products/cloud/cyber-protect/
[19] https://www.jamf.com
[20] https://www.manageengine.com/products/desktop-central/
[21] https://www.syxsense.com/patch-management
[22] https://www.philips.cz/healthcare/product/HC8950-00/philips-e-alert-alerting-solution-for-mri-systems
[23] https://capsuletech.com/capsule-platform
[24] https://banyanmed.com/
[25] https://www.greenbone.net/en/

[26] PASTOREK, A. Telefonické rozhovory s řídícími pracovníky a správci IT v nemocnicích. *Ústní sdělení.*

PŘÍČINY DOPRAVNÍCH NEHOD NA ŽELEZNIČNÍCH PŘEJEZDECH

CAUSES OF ACCIDENTS ON RAILWAY LEVEL CROSINGS

Radek Pavelka

Vysoké učení technické v Brně, Antonínská 548/1, 601 90 Brno. Česká republika. pavelkarad@seznam.cz

Abstrakt: Kritickým místem železnic jsou místa, ve kterých dochází ke křížení se silnicemi, tj. přejezdy. Přejezdy jako takové existovaly na železnici od jejího vzniku, avšak ve zcela jiném režimu. Článek se zabývá zdroji dopravních nehod na zmíněných přejezdech a identifikuje především jejich novodobé příčiny.

Klíčová slova: Železniční přejezd, signál, závažnost, statistické vyhodnocení, kritická analýza, opatření pro snížení nehodovosti.

Abstract: The critical point of railways are places where they are crossings with roads, i.e. level crossings. Level crossings as such have existed on the railway since its origin, but in a completely different regime. The article deals with the sources of traffic accidents at the mentioned level crossings and identifies mainly their modern causes.

Key words: Rail crossing, signal, relevancy, statistical evaluation, critical analysis, measures to reduce accidents.

1. ÚVOD

Kritickým místem železnic jsou místa, ve kterých dochází ke křížení se silnicemi, tj. přejezdy. Přejezdy jako takové existovaly na železnici od jejího vzniku, avšak ve zcela jiném režimu. Přejezdů bylo podstatně méně a násobně převyšoval počet přejezdů, které byly zabezpečeny výstražnými kříži, dříve označovány jako „Nechráněné“. Jediné zabezpečení bylo u některých přejezdů tvořeno závorami, které obsluhoval závorář přímo u přejezdu.

Na nehody na železničních přejezdech lze pohlížet z různých úhlů pohledu. Tyto různé pohledy přirozeně vycházejí z různých druhů dopravy. Pro soudní znalectví je však třeba pokusit se o jejich co největší synergii. Jedno mají však všechny úhly pohledu bez rozdílů zcela určitě společné, a to je závažnost těchto nehod. Na základě databáze havárií na železničních přejezdech byla provedena jejich kritická analýza a statistické vyhodnocení.

Ze statistických analýz vyplývá, že počty nehod na železničních přejezdech v roce 2020 téměř stagnoval, ale v roce 2021 měl tento počet vrůstající tendenci a v roce 2022 za volantem kvůli haváriím na přejezdech z nepozornosti zemřelo 65 lidí.

Příčin havárií na železničních přejezdech je několik. Předložený článek uvádí hlavní příčiny, které vedou k závažným nehodám na železničních přejezdech v České republice. Patří mezi ně: špatné meteorologické podmínky; nevhodné umístění přejezdu; alkohol za volantem; nepozornost řidiče; používání mobilních telefonů při řízení; neznalost zákona; i vliv změn ve společnosti. Nepozornost řidiče může být způsobená spoustou jevů. Dle šetření nejčastější příčiny nepozornosti patří používání nebo volání mobilním telefonem při jízdě bez použití hands-free sady. a poté ukazuje možnosti, jak haváriím předcházet. V závěru jsou uvedeny návrhy opatření na snížení nehodovosti na přejezdech, která je třeba zapracovat do legislativy.

2. NEHODY NA ŽELEZNIČNÍCH PŘEJEZDECH

Kritická místa železnic jsou místa, kde železnice kříží silnice, tedy úrovňové křižovatky. Vzhledem k této skutečnosti patří toto křížení k místům častých dopravních nehod. Místem křížení silniční a železniční dopravní cesty jsou železniční přejezdy, na kterých dochází k výše jmenovaným dopravním nehodám. V České republice je evidováno necelých osm tisíc přejezdů [1]. Příčiny a faktory, které ovlivňují vznik dopravních nehod na železničních přejezdech je celá řada.

Analytické zpracování příčin, faktorů a jejich rozbor je podkladem pro zpracování kvalitních znaleckých posudků v rámci šetření nehod na přejezdech pro potřeby soudu, jiných orgánů a institucí. Tyto skutečnosti vyzývají

zabývat se efektivním zpracováním všech dostupných podkladů dopravních nehod na přejezdech, jejichž výsledkem bude kvalitní znalecký posudek.

Přejezdy jako takové existovaly na železnici od jejího vzniku, avšak ve zcela jiném režimu. Přejezdů bylo podstatně méně a násobně převyšoval počet přejezdů, které byly zabezpečeny výstražnými kříži, dříve označovány jako „Nechráněné“. Jediné zabezpečení bylo u některých přejezdů tvořeno závorami, které obsluhoval závorář přímo u přejezdu. Nutno podotknout, že v době rozvoje železnice (19. století) byl nepoměrně menší počet jak vlaků, tak hlavně automobilů. Počet osobních aut na českých silnicích se za 100 let zvýšil řádově tisíckrát. Zatímco na začátku 20. let minulého století bylo v tehdejším Československu registrováno necelých 5000 vozů, v současnosti je to 5,7 milionu.

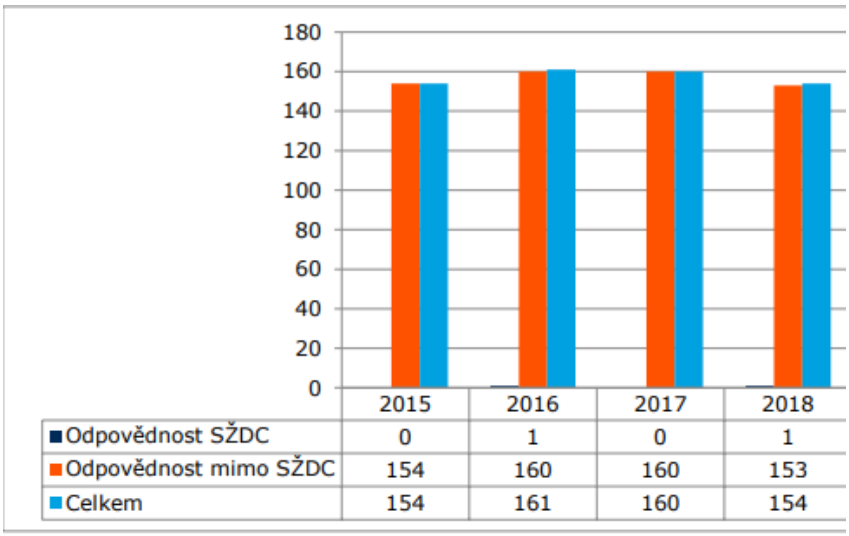
Množství vozidel se za první republiky rychle zvyšovalo. V roce 1930 už v Československu jezdilo přes 100.000 aut. Na začátku 60. let minulého století to byl trojnásobek. V roce 1989 bylo v registru 3,2 milionu osobních a dodávkových vozů. Vyplývá to z údajů Svazu dovozců aut a ČTK [2]. S narůstajícím počtem vlaků, ale hlavně automobilů, došlo i k nárůstu dopravních nehod, těch na železničních přejezdech nevyjímaje. S tímto nárůstem nehod se objevily i otázky, proč vlastně k takovým nehodám dochází a co vede řidiče motorového vozidla k tomu, že přehlédne výstražnou signalizaci na přejezdu nebo se obecně nechová tak, jak mu ukládá Zákon č. 361/2000 Sb. a Vyhláška o provozu na silničních komunikacích.

Zabezpečení přejezdů dle [3] je v ČR různé:

1. Přejezdy zabezpečené automaticky jízdou vlaku mají:
   - přejezdové zabezpečovací zařízení světelné bez závor,
   - přejezdové zabezpečovací zařízení světelné se závorami.
2. Přejezdy obsluhované místně, obslužným zaměstnancem (dochází k jejich rušení, nově nezřizují) zahrnují:
   - přejezdy s mechanickou závorou,
   - přejezdy se světelnou signalizací.
3. Přejezdy zabezpečené výstražnými kříži (dříve označovány jako „nechráněné“) jsou pouze na tratích regionálních nebo místního významu).

3. STATISTIKY DOPRAVNÍCH NEHOD NA PŘEJEZDECH

Na základě dat Drážní inspekce [4] jsou sestaveny statistiky. Grafy na obrázku 1 ukazují počty dopravních nehod na železničních přejezdech pro léta 2015-2018. Tabulky 1-3 ukazují dopravních počty na železničních přejezdech v dalších letech. V tabulkách je provedeno roztřídění dle měsíců - celkový počet nehod, počet usmrcených a počet zraněných.



	2015	2016	2017	2018
Odpovědnost SŽDC	0	1	0	1
Odpovědnost mimo SŽDC	154	160	160	153
Celkem	154	161	160	154

Obr.1. Počty dopravních nehod na železničních přejezdech 2015-2018 [4].

Tabulka 1. Srovnání počtu dopravních nehod pro léta 2019 a 2020 [4].

Střetnutí na železničních přejezdech

	2020			2019		
	počet MU	usmrceno	zraněno	počet MU	usmrceno	zraněno
leden	11	1	6	22	2	3
únor	8	1	14	11	0	3
březen	7	2	4	11	2	6
duben	9	6	4	18	4	8
květen	11	4	5	18	4	3
červen	13	4	19	13	1	6
červenec	26	7	10	24	10	27
srpen	12	4	3	16	3	15
září	15	4	13	10	3	9
říjen	8	3	4	17	7	8
listopad	12	0	6	15	5	2
prosinec	14	3	5	6	2	3
Počet MU 1.1. - 31.12.	*146*	*39*	*93*	*181*	*43*	*93*

Tabulka 2. Srovnání počtu dopravních nehod pro léta 2020 a 2021 [4].

Střetnutí na železničních přejezdech

	2021			2020		
	počet MU	usmrceno	zraněno	počet MU	usmrceno	zraněno
leden	17	5	2	11	1	6
únor	17	0	10	8	1	14
březen	12	7	4	7	2	4
duben	9	3	2	9	6	4
květen	11	1	9	11	4	5
červen	12	0	3	13	4	19
červenec	19	2	11	26	7	10
srpen	14	0	10	12	4	3
září	9	5	2	15	4	13
říjen	16	3	7	8	3	4
listopad	10	1	3	12	0	6
prosinec	14	2	6	14	3	5
Počet MU 1.1. - 31.12.	*160*	*29*	*69*	*146*	*39*	*93*

Tabulka 3. Srovnání počtu dopravních nehod pro léta 2021 a 2022 [4].

Střetnutí na železničních přejezdech

	2022			2021		
	počet MU	usmrceno	zraněno	počet MU	usmrceno	zraněno
leden	13	1	5	17	5	2
únor	9	2	4	17	0	10
březen	9	2	4	12	7	4
duben	18	4	7	9	3	2
květen	21	4	11	11	1	9
červen	11	1	5	12	0	3
červenec	15	6	15	19	2	11
srpen	15	2	10	14	0	10
září	15	2	6	9	5	2
říjen	16	6	13	16	3	7
listopad	10	2	8	10	1	3
prosinec	13	3	6	14	2	6
Počet MU 1.1. - 31.12.	*165*	*35*	*94*	*160*	*29*	*69*

4. VYHODNOCENÍ PŘÍČIN DOPRAVNÍCH NEHOD A OPATŘENÍ PRO ZVÝŠENÍ BEZPEČNOSTI

Mezi hlavní příčiny, které vedou k vážným nehodám na železničních přejezdech v České republice, patří podle dosavadních znalostí [5]:

- špatné meteorologické podmínky,
- nevhodné umístění přechodu,
- alkohol za volantem,
- nepozornost řidiče,
- používání mobilních telefonů za jízdy,
- neznalost legislativy,
- dopad změn ve společnosti.

Z údajů v odstavci 3 vyplývá, že počet dopravních nehod na železničních přejezdech neklesá. Počet usmrcených osob narostl o 6 případů. Je tedy evidentní, že situace se v nehodovosti na železničních přejezdech nelepší. Tato skutečnost není nijak uspokojivá. Nejvyšší počet dopravních nehod je na přejezdech, které jsou sice zabezpečeny, ale nejsou vybaveny závorami. Tento počet je téměř poloviční z celkového počtu všech nehod na železničních přejezdech za sledované období. Je tedy zřejmé, že absence závor na zabezpečených přejezdech má zásadní význam pro sled událostí při přejíždění železničního přejezdu silničním vozidlem. I na základě těchto statistik se při rekonstrukcích přejezdů ve správě SŽ nově neaktivují tyto typy přejezdů. Při všech rekonstrukcích jsou nyní všechny přejezdy vybaveny břevny závor, a to bez ohledu na třídu komunikace, tedy i na lesních i polních cestách, které kříží železniční trať.

Z výzkumů chování řidičů na železničních přejezdech, kterými se zabývá např. CDV (Centrum dopravního výzkumu) *Centrum dopravního výzkumu* [6] se jeví břevna závor skoro jako takový malý „zázrak“. Přejezdy takto vybavené jednoznačně vykazují zcela jiné počty nehod jako u ostatních přejezdů, dokonce ty zcela nejnižší ze všech sledovaných, vyjma přejezdů zabezpečených pouze mechanicky, tedy pouze břevny závor.

Nových příčin dopravních nehod na železničních přejezdech je několik. V první řadě je to nepozornost řidičů, která je způsobená řadou příčin. Mezi ně patří používání nebo volání mobilním telefonem při jízdě bez použití hands-free sady [7]. Používání mobilu za jízdy, psaní textových zpráv a s tím spojená nepozornost při řízení patří v posledních letech k nejčastějším příčinám nehod na tuzemských silnicích. V roce 2021 za volantem kvůli nehodám z nepozornosti zemřelo 65 lidí [7].

Telefonování, a hlavně psaní zpráv za volantem, je závažný problém především mezi mladými lidmi, ale nejen mezi nimi. Průzkumy [7] ukázaly, že řidiči, kteří se věnují za jízdy svému telefonu, mají sníženou vnímavost okolí a je pravděpodobnější, že se neudrží ve svém pruhu – při rychlosti 90 km/h a pohledu na 5 s do mobilu se ujede vzdálenost 125 m. Potom není těžké porozumět, proč je používání mobilního telefonu takový problém a proč má na svědomí desítky lidských životů ročně.

V České republice samozřejmě platí pro řidiče automobilů zákaz používání mobilního telefonu [8], v zahraničí však jsou přísnější pravidla [6].

Analýza dat Drážní inspekce [4] ukazuje, že dalšími příčinami nehod na železničních přejezdech jsou:

1. Agresivní a neodpovědné chování řidičů, zejména mladých. K tomu lze směle přičíst nekontrolovatelný a všude přítomný sklon ke spěchu bez reálného důvodu. Nemalou měrou k současnému vývoji přispívá i současná hektická doba, která se přenáší i do silničního provozu.
2. Neznalost Zákona č. 361/2000 Sb. a konkrétně § 29 zmíněného zákona, který jasně vymezuje, kdy nesmí řidič vjíždět na železniční přejezd. I přes toto zcela přesné vymezení dochází poměrně často k jeho porušení. Pro ilustraci můžeme použít hned první odrážku odstavce 1 § 29 Zákona č. 361/2000 Sb. Ta říká, že řidič nesmí vjíždět na železniční přejezd, je-li dávána výstraha dvěma červenými střídavě přerušovanými světly signálu přejezdového zabezpečovacího zařízení.
3. Reprodukce hudby v autě (rádio).
4. Nastavování navigace za jízdy.
5. Obsluha doplňkových funkcí automobilu (různá vyhřívání, nastavení klimatizace apod.),
6. Reakce na projevy dětí, zejména malých.
7. Spěch, který je spojen s dnešním životem.

Správa železnic investuje od r. 2017 značné prostředky na snížení nehodovosti na železničních přejezdech [1], např. systematicky úrovňová křížení zabezpečená výstražným křížem.

5. ZÁVĚR

Ústav soudního inženýrství VUT v Brně připravuje metodiku hodnocení příčin dopravních nehod, která je založena na metodice hodnocení bezpečnosti procesů (PSM – proces safety management) [8], která přesněji určí příčiny dopravních nehod na železničních přejezdech důkladnou analýzou procesů – jízda automobilu a jízda vlaku a příslušené vnější podmínky.

LITERATURA

[1] www.spravazeleznic.cz
[2] www.securitymagazin.cz
[3] ČD. *Předpis pro obsluhu přejezdových zabezpečovacích zařízení.* Č.j.: 59 968 / 2001-O11. Z2. Praha: ČD 2001.
[4] DRÁŽNÍ INSPEKCE. *Databáze šetřených dopravních nehod.* www.dicr.cz
[5] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Rizika spojená s pozemními komunikacemi.* ISBN 978-80-01-06843-4. Praha: ČVUT 2021, 296 p., http://hdl.handle.net/10467/94283
[6] CENTRUM DOPRAVNÍHO VÝZKUMU. www.cdv.cz
[7] www.tipcars.com
[8] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessee: US DOE 1996, 180 p.

ZVYŠOVÁNÍ EFEKTIVITY VÝVOJE A PROVOZU SOFTWARE PRO KYBER-FYZICKÉ SYSTÉMY

INCREASING THE EFFECTIVENESS OF DEVELOPMENT AND OPERATION OF SOFTWARE FOR CYBER PHYSICAL SYSTEMS

Jan Procházka[1], Petr Novobilský [1], Dana Procházková[2]

[1] *Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Česká republika., jpr@qma.cz, pno@qma.cz*
[2] *České vysoké učení technické v Praze, Technická 4, 166 00 Praha 6, Česká republika. danuse.prochazkova@fs.cvut.cz*

Abstrakt: Kyber-fyzikální systémy (CPS) rozmístěné na velkém území vyžadují bezpečnou komunikaci nejen mezi různými částmi systému, ale také s operačním (řídícím) střediskem. Budování vlastních komunikačních sítí provozovatelem systému je finančně náročné, a proto se používají více či méně otevřené komunikační systémy. S tím souvisí i vyšší požadavky na zabezpečení aplikací provozovaných CPS. Evropský projekt COSMSOS vytváří nástroj, který aplikuje vývojové technologie DevOps z oblasti IT do oblasti vestavěných systémů. Na příkladu požadavků pro drážní operační systém ukazujeme, že pro použití musí být tento velmi složitý software přizpůsoben reálným požadavkům pro drážní operační systém.

Klíčová slova: Kyber-fyzické systémy, riziko, bezpečnost, zabezpečení, návrh založený na rizicích, zaměření softwaru.

Abstract: Cyber-Physical Systems (CPS) distributed over a large territory, require secure communication not only among various parts of system, but also with operation centre. Building its own communication networks by the system operator is financially demanding, which is why more or less open communication systems are used. This is connected with higher requirements for the security of applications, operated in a CPS. European project COSMSOS has been creating a tool that applies DevOps development technologies from the IT field to the field of embedded systems. On the example of requirements on railway operation system, we show that for use this very complex software must be adapted to real requirements on railway operation system.

Key words: Cyber-Physical systems, risk, safety, security, risk-based design, software aim.

1. ÚVOD

V současné době se počet dálkově ovládaných zařízení a systémů zvyšuje velkým tempem. Dotčená zařízení a systémy jsou nezbytnou součástí kritických infrastruktur, které patří k základním veřejným aktivům, protože zajišťují základní funkce státu. Proto je z hlediska potřeb lidské společnosti a lidského bezpečí nezbytné, aby dotyčná zařízení a jejich celé sady byly bezpečné a efektivní. Jedná se o vzájemně propojené technické sítě, které jsou ovládány systémy řízení, ve kterých se zvyšuje automatizace; mluvíme o kyber-fyzických systémech.

Kyber-fyzické systémy (CPS) rozmístěné na velké ploše vyžadují bezpečnou komunikaci nejen mezi různými částmi systému, ale také s operačním (řídícím) střediskem. Budování vlastních komunikačních sítí provozovatelem systému CPS je finančně náročné, a proto se používají více či méně otevřené komunikační systémy. S tím souvisí vyšší požadavky na bezpečnost a zabezpečení procesů v CPS. CPS, stejně jako kritické infrastruktury (jako jsou železnice), musí splňovat vysoký standard v oblasti bezpečnosti komunikací.

Reakce na nové kybernetické hrozby je důležitou součástí kybernetické bezpečnosti (tj. jde o kybernetické zabezpečení CPS), a proto integrátoři nebo dodavatelé CPS musí být schopni poskytovat aktualizace softwaru včas. Efektivní poskytování těchto služeb vyžaduje efektivní nástroje, které dokáží identifikovat a eliminovat chyby ve fázi vývoje a během provozu, a které lze použít k odvrácení kybernetického útoku.

Článek se zabývá podmínkami, za kterých je možné využít software, který se vyvíjí v projektu COSMOS [1] při řízení bezpečného provozu vlaků.

2. AUTOMATIZACE A JEJÍ PROBLÉMY

Automatické řízení je obvykle rozděleno na logické, spojité, diskrétní a fuzzy řízení. Při jeho aplikaci se nejčastěji používají rozdělení pravděpodobnosti: normální; log-normální; Weibullovo; a Gamma. Při řízení se aplikují: teorie Markových procesů; Kolmogorovovy rovnice; a další [2]. V teorii automatického řízení je zdůrazněn význam systémového přístupu při řešení automatizačních úloh a praxe vyžaduje mnoho znalostí z oblasti informačních technologií [3]. Automatické řízení je stále více realizováno pomocí kybernetických sítí propojených přes internet. Vzhledem k tomu, že internet se vyznačuje anonymitou uživatelů, globální dostupností a současným používáním mnoha různých technologií, je zabezpečení informačních systémů připojených k internetu poměrně obtížné.

Na základě prací [4-8] jsou v současné době pro každý technický systém vytvořena pravidla automatického řízení na základě modelování, které je založeno na teorii spolehlivosti. Spolehlivost zařízení je postavena pouze na základě údajů o náhodných procesech, a proto není zaručena bezpečnost zařízení za všech podmínek, tj. kritických a extrémních podmínek, které jsou způsobeny mezerami ve znalostech nebo extrémními vnějšími vlivy. Uvedená fakta tudíž představují řadu dalších zdrojů rizika pro technické systémy, a to zejména pro ty, které využívají dálkový přenos dat.

Na základě myšlenky propojení řídicího a řízeného systému [9] je zřejmé, že základem automatického řízení jsou zpětné vazby, na jejichž základě řídicí systémy upravují provoz celého technického díla podle informací z řízených systémů. Pozitivní zpětná vazba podporuje výsledky řízených procesů a negativní zpětná vazba je oslabuje. Řídicí systémy mají algoritmy, které dávají příkazy a provádějí některé operace. Řídicí (ovládací) systém zajišťuje, že specifikované fyzikální veličiny systému jsou udržovány na předem stanovených hodnotách. V procesu regulace mění řídicí systém stav řízeného systému působením na akční proměnné tak, aby bylo dosaženo požadovaného stavu.

V případě řídicího systému podle současných koncepcí, které kladou nejvyšší důraz na bezpečnost (tj. i zabezpečení vůči vnějším hrozbám), jsou zdůrazněny vlastnosti:
- bezpečnost (úroveň dodržování stanovených provozních podmínek a nevytváření škodlivých (nepřijatelných) dopadů na samotný systém a jeho okolí),
- funkčnost (úroveň provedení požadovaných akcí),
- provozuschopnost (úroveň plnění požadovaných úkolů v závislosti na běžných, abnormálních a kritických podmínkách),
- provozní stálost (úroveň plnění stanovených podmínek provozu v průběhu času)
- a inherentně zabudovaná odolnost vůči pohromám.

Řízený systém je obvykle komplexní nelineární systém, který se vyznačuje tím, že:
- se skládá z konečného počtu prvků,
- každý jeho prvek je jednoznačně popsán konečným počtem měřitelných veličin,
- propojení mezi prvky je jasně formulováno.

Dynamické vlastnosti řízeného systému lze popsat pomocí diferenciálních rovnic, jejichž řešením je stavový vektor. Stavový vektor umožňuje určit stav systému v libovolném časovém okamžiku pomocí minimálního počtu veličin [9].

Pokud není možné u daného zařízení zcela vyloučit zdroje rizik, což platí například pro přírodní pohromy, je další nejlepší volbou ochrana zařízení před dopady spojenými s výskytem rizik, a to minimalizací dopadů rizik na zařízení tak, že příslušná bezpečnostní ochranná opatření (tzv. systémy pro zajištění bezpečnosti) jsou přímo začleněna jak do návrhu zařízení, tak do provozních podmínek zařízení. Dalšími opatřeními v pořadí priorit ochrany jsou systémy v zařízení pro zmírňování dopadů rizik (systémy pro podporu bezpečnosti), která mají pouze ochranné funkce. Jedná se například o pojistné ventily, které chrání před neoprávněným přetlakem v případech, kdy nelze zcela zabránit nepřijatelnému zvýšení tlaku v zařízení [2,10].

Podle poznatků shrnutých v práci [11] jsou systémy pro zajištění bezpečnosti navrženy jako pasivní nebo aktivní zařízení. Nejúčinnější zařízení jsou pasivní zařízení, která pracují na fyzikálních principech (např. gravitaci) a nepotřebují k aktivaci žádný další impuls. Příkladem pasivního zařízení pro zajištění bezpečnosti je v námi sledované oblasti železniční semafor, jehož rameno automaticky přejde do polohy "stop", kdykoli je přerušen elektrický proud v napájecím kabelu. Aktivní zařízení/systémy pro zajištění bezpečnosti jsou méně vhodné, protože k jejich aktivaci jsou zapotřebí speciální iniciační impulsy, aby se zabránilo nehodě, anebo se zmírnily její dopady. Jejich vytváření zahrnuje detekci nebezpečí a rozpoznání vhodného postupu pro zajištění bezpečnosti. Příkladem systému aktivní bezpečnosti je detektor kouře, který je připojený ke sprchovému systému.

Současné technické poznatky umožňují použití hybridních bezpečnostních systémů, které se vypínají samostatně, pokud podmínky nejsou v rozsahu podmínek stanovených pro provoz aktivních systémů [2,10].

Systém řízení bezpečnosti (Safety Management System – SMS) musí být vždy vybaven opatřeními k minimalizaci škod v případech, kdy bezpečnostní opatření a bezpečnostní systémy selžou nebo vznikne neidentifikované ohrožení. Opatření pro minimalizaci škod může mít podobu výstražných a varovných signálů, školení, instrukcí a postupů pro chování v nebezpečných situacích nebo izolace nebezpečných zařízení od obydlených center. Opatření pro předcházení nehodám, včetně havarijního plánování, musí být vypracována před uvedením zařízení do provozu., protože když dojde k nehodě, tak na to nemusí být dostatek času [12].

3. UMĚLÁ INTELIGENCE A KYBER-FYZICKÉ SYSTÉMY

Umělá inteligence (dále jen AI) se stala významnou inovační silou a je jedním z pilířů čtvrté průmyslové revoluce. Aby se umělá inteligence (AI) stala plně všudypřítomnou, je třeba vytvořit nové postupy . Jedná se o tvorbu velkých komplexních datových sad, které označujeme „Big data“. Strukturovaná i nestrukturovaná data jsou tudíž integrována do systémů, které obsahují obrovské množství informací z (geograficky) distribuovaných datových zdrojů. Jejich kvalitní zpracování umožňuje získávat výsledky pro sledované úseky v reálném čase, které zohledňují široký interval aspektů. Pro řešení úkolů praxe vyžadují specifické nástroje pro zpracování dat.

Big data představují agregované údaje z mnoha různorodých zdrojů a aplikací. Tradiční mechanismy integrace dat, jako je extrakce, transformace a načtení, obecně nejsou pro tento úkol dostačující. Zpracování dat vyžaduje nové strategie a technologie pro analýzu velkých datových sad v rozsahu terabajtů či dokonce petabajtů. Pro big data je nutné mít úložiště, která se používají nejčastěji ve formě datových skladů (cloudů). Data jsou do cloudu přenášena v předem daných cyklech a následně je nad nimi provedena analýza již připravenými algoritmy. Pro zpracování big dat jsou speciální nástroje [13].

Big data umožňují získávat ucelenější odpovědi, protože jsou založeny na zvážení informací z více oblastí. Ucelenější odpovědi znamenají větší důvěru ve výsledky a k řešení problémů. Rozsáhlejší datové sady umožňují objevovat nové souvislosti. Software je všude a produktivita softwarových inženýrů se radikálně zvýšila s příchodem nových specifikací, designu a programovacích paradigmat a jazyků.

Kyber-fyzické systémy (CPS) jsou složité systémy a zahrnují heterogenní softwarové a hardwarové komponenty, které na sebe vzájemně působí. Cílem jejich řízení ve smyslu ovládání je automatizace operací v různých oblastech, jako je automobilový průmysl, letecký průmysl, zdravotnictví nebo železnice. Stejně jako u každého softwarového systému se systémy CPS neustále vyvíjí tak, aby se vyrovnaly s novými požadavky zákazníků a technologickými změnami. Software CPS vyžadují přizpůsobit proces vývoje a provozu (DevOps) požadavkům praxe, a proto jejich vývoj je náročnější než vývoj konvenčních software [14-17].

Vývojáři softwaru CPS se spoléhají především na základní simulační modely [18,19] pro tuhá tělesa [20,21] a na simulační modely pro měkká tělesa [22,23]. Použití simulačních prostředí CPS umožňuje automatické generování a provádění testů [23,24]. Omezený rozpočet přidělený na testovací činnosti a prakticky nekonečný testovací prostor však představují výzvy pro adekvátní uplatňování chování CPS [24-27].

Jednou z recentních technologií je digitální dvojče, tedy digitální obraz reálného fyzického prvku: například model ve fázi návrhu výrobku, který můžeme postupně rozšiřovat v rámci životního cyklu výrobku nebo jakéhokoliv systému. Propojuje objekty a hledá vazby, jejich synergie a konflikty. Reálný objekt je propojen s virtuálním objektem a jednotlivé fyzické parametry jsou v jeho digitálním dvojčeti aktualizovány v čase. Právě časový prvek je základním rozdílem mezi digitálním dvojčetem a existujícími přístupy k modelování. Na digitální úrovni lze se systémem digitálních dvojčat experimentovat, ověřovat výstupy, simulovat chování a také aplikovat s umělou inteligencí ke zkoumání různých jevů, funkcí a kvalitativních vlastností. Technologie digitálních dvojčat může být aplikována v celém životním procesu složitých systémů, od jejich návrhu a ověření nadřazených funkcí přes provoz, změny, až po vypnutí nebo nahrazení jiným systémem [28].

V souvislosti s aplikacemi DevOps v kontextu CPS [29] analyzovali použití a výzvy digitálního dvojčete, aby umožnily přístupy DevOps pro kyberneticko-fyzické produkční systémy je neustále zlepšovat. Park a kol. [29] konkrétně identifikovali problémy související s:

- nesrovnalostmi mezi modely a jejich fyzickými protějšky,
- integrací mezi heterogenními modely kvůli složitosti CPS
- a bezpečnostními problémy způsobenými těsným propojením mezi digitálním dvojčetem a fyzickým prostředím.

Proto je třeba, abychom se nezaměřili jen na automatizaci výrobního procesu, ale abychom se zaměřili především na spojitou integraci (CI) a spojitý vývoj (CD) CPS, tj. na proces označovaný CI/CD .

Práce [7] zaměřuje pozornost na kybernetickou bezpečnost (přesněji kybernetické zabezpečení sledované entity), tj. na:
- hodnocení kybernetických rizik,
- bezpečnostní politiku a dodržování předpisů v oblasti kybernetické bezpečnosti,
- implementaci hardwaru a softwaru,
- plány obnovy,
- nástroje pro podporu dodržování předpisů,
- školení pracovníků
- a analýzu požadavků na konfiguraci.

Pro řízení rizik softwaru z pohledu bezpečnosti [30] je třeba:
- posoudit požadavky, tj. stanovit požadovanou úroveň ochrany systému a údajů,
- vybrat ovládací prvky, tj. identifikovat bezpečnostní postupy/politiky odpovídající požadovanému zabezpečení systému,
- zavést kontroly, tj. instalovat/používat/konfigurovat vhodná technická a/nebo procedurální řešení,
- vyhodnocovat kontroly, tj. identifikovat bezpečnostní nedostatky a vypracovat plán pro snížení zranitelností,
- provádět hodnocení rizik, tj. určit, zda organizace přijímá rizika spojená s provozem systému
- a řídit rizika, tj. udržovat systém (systémy) a software v žádoucím stavu na základě nepřetržitého sledování stavu zabezpečení.

Vzhledem k dynamickému vývoji světa je nutné dle [30-33] zajistit:
- neustálé zlepšování procesů,
- rozvoj politiky řízení informací a znalostí,
- správu a řízení big dat,
- automatizaci procesů
- a správu informací a vývoj nových postupů pro potřeby praxe.

Neustálé zlepšování procesů musí postupně odstraňovat neefektivní procesy, které způsobují problémy v praxi (jako jsou zmeškané termíny, nespokojení zákazníci, zbytečné náklady, vyhoření zaměstnanců a další problémy) a zajistit:
- rychlejší rozhodování,
- vyšší produktivitu, která vede k vyšší spolehlivosti,
- účinné přidělování zdrojů za účelem snížení nákladů,
- efektivní operace k zajištění pořádku a konzistence v plnění úkolů,
- zvýšenou automatizaci úkolů, aby se snížila únavná práce
- a vylepšit agilitu, která společnostem umožňuje snadno se orientovat v dynamickém podnikatelském prostředí.

4. DATA PRO CPS A PROJEKT COSMOS

Velké průmyslové podniky, malé podniky a akademičtí pracovníci v Evropské unii se spojili, aby vyvinuli vylepšené postupy DevOps pro vývoj softwaru kyber-fyzických systémů. Projekt COSMOS [1] financovaný Evropskou unií integruje sofistikovanější validaci a verifikaci, která zahrnuje:
- kombinaci statických analýz norem korelovaných s problémy a hlášeními chyb,
- automatizované generování testovacích případů,
- ověřování spolehlivosti opatření za provozu,
- testování hardwaru a zpětných vazeb v provozních zařízeních.

Projekt také využívá strojové učení, testování založené na modelech a generování testů založených na vyhledávání.

Je skutečností, že:
- velká část rostoucí složitosti systémů informačních a komunikačních technologií (ICT) je způsobena hodně distribuovanou a hodně heterogenní povahou těchto systémů,
- kyber-fyzické systémy mají stále více softwarových systémů.

Proto základní návrhy projektu COSMOS se zaměřují na propojení osvědčených postupů řešení DevOps s vývojovými procesy používanými v kontextu CPS, což umožňuje:
- rychlejší dodávky software pro CPS
- a výsledkem budou bezpečnější a důvěryhodnější systémy CPS.

COSMOS sdružuje vyvážené konsorcium velkých průmyslových podniků, malých a středních podniků a akademických pracovníků, kteří vyvíjí vylepšené kanály DevOps, které jsou zaměřené na vývoj softwaru CPS. Tato software mají zajistit sofistikovanější ověřování a potvrzování spolehlivosti řešení, a proto zahrnují:

- kombinace statických analýz norem, které korelují s problémy a zprávami o chybách,
- automatizované generování testovacích případů,
- ověřování za provozu zařízení,
- testování hardwaru ve smyčce (HiL)
- a zpětné vazby z provozních zařízení.

Přitom se používají přístupy založené na strojovém učení, testování založené na modelech a generování testů založených na vyhledávání slabých míst. Vyvíjí se také techniky pro stanovení priorit a plánování testování s cílem maximalizovat účinnost testovacích procesů a minimalizovat bezpečnostní hrozby. COSMOS využívá stávající prototypové technologie vyvinuté partnery a podporuje jejich vylepšování v průběhu celého projektu.

Projekt COSMOS využívá softwarově definované infrastruktury k alokaci zdrojů nezbytných pro splnění potřeb průmyslového testování. Vyvinuté postupy využívají cloudové platformy podle potřeby pro spouštění složitých testovacích procesů, dynamické škálování zdrojů infrastruktury a podle potřeby se zaměřují na optimalizační mechanismy, které tyto infrastruktury inteligentně využívají k minimalizaci celkového času a nákladů na testování a zároveň zajišťují, že testy jsou prováděny včas. COSMOS je schopen získávat vzorky z oblasti vývoje pro zlepšení efektivity testů (vyšší záběr testů, více zjištěných zranitelností atd.), které odráží prostředí reálného světa. Není to prováděno úpravou existujících norem, ale spíše úpravou konfigurace software, ve kterém je aplikace spuštěna.

Účastníci projektu COSMOS vyvíjí nástroje pro maximalizaci efektivity testů při minimalizaci času a nákladů na provádění testů. Efektivnější testování a ověřování zvyšuje spolehlivost softwaru a kybernetickou bezpečnost, protože v produkčních systémech je méně potenciálně zneužitelných chyb. COSMOS dosahuje lepší spolehlivost softwaru z důvodu použití sofistikované kombinace zlepšení efektivity testů prostřednictvím automatizovaného generování testů, technik strojového učení pro předvídání výsledků testů, uvážlivého zahrnutí testování hardwaru ve smyčce do testovacích procesů, začlenění zpětných vazeb existujících v reálu do testovacích procesů a statické analýzy norem.

S ohledem na zabezpečení CPS, COSMOS specificky vyvíjí řešení pro detekci bezpečnostních zranitelností v kyber-fyzických systémech prostřednictvím kombinace analýzy zdrojových norem a generování vstupních sekvencí, které mohou vyvolat bezpečnostní problémy. COSMOS také určuje modely odezvy, a to včetně modelů odezvy související se zabezpečením. Používá k tomu statické analýzy norem pro odezvu a softwarové základny založené na strojovém učení.

Publikované výsledky projektu [31] ukazují, že řešení problémů vychází z teoretického modelu CPS a je na vysoké teoretické úrovni, ale nebere v úvahu, že CPS, které se používají v praxi, mají dnes již nějakou strukturu a nějaká provozní pravidla, která jsou stanovena legislativou. Jejich rychlá změna není možná z provozních, ekonomických a časových důvodů. Proto je pro praktické cíle nutné najít postup pro jejich použití.

Analýza provedená v práci [31] ukazuje, že například pro železnici se vyplatí používat:

- manuální provádění statických analýz,
- automatické provádění testů,
- automatické provádění systémových testů a testů funkčnosti, které jsou jiné než přístupy vyvinuté v projektu COSMOS.

Je skutečností, že provozování železnice závisí na software pro systém řízení ovládání vlaků, tj. na systému označovaném „Train Control Management System (TCMS)“, který je založen na jistém programovacím jazyku, který je odlišný od programovacího jazyka používaného v projektu COSMOS. Proto pro aplikace vyvinuté v projektu COSMOS je nejprve třeba provést úpravu programovacího jazyka, na kterém má být software spuštěn. Železnice už má také zavedený proces pro spojitou integraci a vývoj CPS (CI/CD), který je v současné době ve stavu neustálého zlepšování. Proto má problémy při pokusu o zapojení nově vyvíjených software v projektu COSMOS, a to především kvůli složitosti domény železnice [17]. Normy pro železnici jsou založené na určitém modelu a přijatých postupech, které navrhovatelé software v projektu COSMOS bez specifických znalostí specifik železnice mohou interpretovat různě.

Systém řízení TCMS, podobně jako systém řízení letecké dopravy mají specifika hlavně z pohledu bezpečnosti [30]. Předmětný s\stém řízení představuje integrovaný systém řízení [30], do kterého nelze jednoduše vkládat kusy obecných software, které nerespektují oborová specifika.

5. METODIKA ZAJIŠTĚNÍ BEZPEČNOSTI ŽELEZNIC

Podle Maastrichtské smlouvy [34] je bezpečnost nejvyšší kvalitou každého objektu, tj. i CPS, což je ve sledovaném případě železnice. Železnice je vysoce složitý objekt CPS, který má velké množství specifických prvků a komponent složitě propojených. Na základě současného poznání [35] dle projektu železnice mají všechny komponenty a propojení své limity, které jsou nastaveny na určité podmínky tak, aby společně splňovaly zadaný cíl (tj. aby byly interoperabilní). Protože se svět dynamicky vyvíjí, tak se mění podmínky pro komponenty, jejich propojení i podmínky pro interoperabilitu. Při velkých změnách mohou být limity komponent, jejich propojení i limity interoperability, nastavené v projektu nedostatečné, a proto musí být z provozních, ekonomických i společenských důvodů zajištěna odezva, která zmírní dopady na lidi, železnici i území vyvolané změnami. To znamená, že bezpečnost železnice se mění v závislosti na vyvíjejících se podmínkách. Proto systém řízení železnice a jejich komponent musí být takový, že zajistí udržitelný provoz za všech podmínek.

Bezpečnost zahrnuje jak spolehlivost, tak funkčnost a s ohledem na vnitřní a vnější škodlivé jevy musí být její řídicí systémy zabezpečeny jak fyzicky, tak kyberneticky. Proto v souladu s požadavky [32] a s výsledky dalších prací musí mít železnice program řízení bezpečnosti železnice založený na řízení rizik, od návrhu, přes výstavbu [30] až po provoz [33], jakož i údržbu, obnovu, kompletaci a inovace. Vzhledem k důležitosti role kybernetické infrastruktury spojené s automatizovaným systémem řízení proto musí SMS monitorovat i kybernetickou bezpečnost a obsahovat CSMS (cybersecurity of safety management system) - obrázek 1 [35].

Obr. 1. Model řízení bezpečnosti železnic s automatizovaným řízením v čase. Procesy: 1- koncepce a řízení; 2 – správní postupy; 3 - technické procesy; 4 – vnější spolupráce; 5 - nouzová připravenost; 6 - dokumentace a vyšetřování nehod; 7 - Kybernetická bezpečnost (kybernetické zabezpečení). Zpětná vazba: 1-4 ve žlutých kroužcích [35].

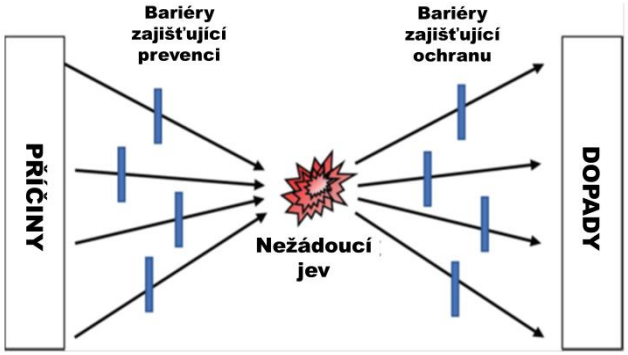
Hlavním cílem zabezpečení železniční infrastruktury při automatickém řízení je, aby pokyny pro systémy řízení provozu vlaků byly jasné a přesné, tj. nebyly ovlivněny jevy, které je zkreslují. Proto zabezpečovací systémy, které se dříve používaly na železnicích, byly uzavřené a patentované [36]. S vysokým stupněm automatizace se ukázalo, že je vhodné používat internet, což přineslo problémy, které se stále řeší.

Kybernetická bezpečnost není jen otázkou designu, protože limity a podmínky každého systému a každého zařízení se v průběhu času mění. To znamená, že problém kybernetického zabezpečení CPS pro výrobce CPS nekončí přijetím systému uživatelem. Z bezpečnostních důvodů musí být kybernetický stav každého kybernetického systému monitorován během provozu, dokud nebude systém vyřazen z provozu. Na základě výsledků monitorování musí být během provozu CPS prováděna údržba založená na rizicích [33]. Požadavky na údržbu založenou na rizicích závisí nejen na struktuře kyber-fyzických systémů, ale také velmi vážně na podmínkách, ve kterých jsou provozovány.

6. POSOUZENÍ VYUŽITÍ VÝSLEDKŮ PROGRAMU COSMOS PRO ŽELEZNICI

Železnice je nezbytnou součástí kritické infrastruktury každé země i celé Evropy, a proto je kladen důraz na integrální bezpečnost, která zahrnuje jak spolehlivost, tak funkčnost. Na základě výzkumu [32,33,35] je nutné zajistit integrální bezpečnost po celou dobu její životnosti vzhledem k dynamickému rozvoji světa a samotného železničního systému, tedy především v oblasti návrhu, provozu, údržby a modernizace. Vzhledem k proměnlivosti světa může být celková bezpečnost zajištěna pouze průběžným kvalifikovaným řízením rizik, jak ukazuje obrázek 1.

Při projektování je velmi důležité, jak projektant rozdělí reálná rizika pro železnici [35,37,38], viz schéma motýlka na obrázku 2. V projektu se aplikují preventivní opatření pro eliminování nebo snížení rizika a při provozu se snižují dopady rizik opatřeními odezvy. V druhém případě musí projektant v návrhu připravit kvalifikovaná opatření pro odezvu s cílem zmírnit dopady realizovaného rizika.

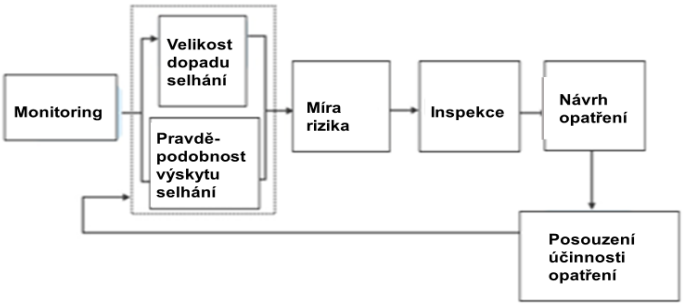


Obr. 2. Oddělení protiopatření mezi návrhem a odezvou; zpracováno dle [38].

Technika sestavení návrhu založeného na rizicích železničního systému je popsána v práci [35]. Principy provozu založené na riziku jsou popsány v [30]. Vzhledem k tomu, že všechny části železničního systému stárnou a zastarávají, je údržba v praxi velmi důležitá.

Strategie údržby založená na rizicích je založena na dvou hlavních fázích: posouzení rizik; a plánování údržby na základě rizika [33,39,40]. Pro každé identifikované riziko je třeba shromáždit údaje. To zahrnuje informace o riziku, jeho dopadech a důsledcích a o metodách, které lze použít ke zmírnění a předvídání rizika. Rámec údržby založený na rizicích je znázorněn na obrázku 3. Ve fázi hodnocení rizik se pravděpodobnost rizika i jeho důsledky kvantifikují v souvislosti s uvažovaným objektem.

Rámec údržby založený na rizicích se uplatňuje na každý systém v zařízení. Systém může být například vysokotlaká nádoba nebo brzdový či chladící systém. Tento systém bude mít sousední systémy, které jsou s ním propojené a vzájemně se ovlivňují. Nejprve jsou určeny pravděpodobné způsoby selhání systému. Poté se na každé riziko aplikuje typický rámec údržby založený na rizicích [33,39-43].



Obr. 3. Rámec údržby založený na rizicích.

Jedna z oblastí použití „umělé inteligence“ jsou fáze vývoje, verifikace a validace designu systému s ohledem na rizika. Jedná se o fáze vývoje podle V-cyklu [44], během kterých jsou testovány funkce systému a hledány možné zranitelnosti. K tomuto testování se používají nejrůznější metody. V závislosti na charakteru systému je potřeba vždy zvolit adekvátní metodiku testování. Čím komplexnější systém, tím je potřeba vícero typů metod, protože různé aspekty vyžadují různé metodiky.

Metamorfní testování je metoda pro testování síťových systémů a skládá se ze dvou fází. Během první fáze se testují funkce systému a během druhé se hledají zranitelnosti. Právě druhá fáze lze automatizovat za pomocí „umělé inteligence“ a za využití manuálního vstupu první fáze jako vstup pro tuto automatizaci.

Prvním krokem je vytvoření typologické mapy systémů, které říkáme metamorfní vztahy. Jedná se o definování vztahů mezi jednotlivými prvky a procesy systému. V případě komunikačních systémů může jít například o komunikační kanály a jejich vlastnosti, nebo odkud kam mají informace proudit.

Druhým krokem je testování funkčnosti. Je potřeba vložit do systému všechny typy očekávaných validních vstupů a posoudit správnost výstupu. Součástí správnosti vstupu může být adresa v systémů, kde je informace zadána. Nebo uživatelské jméno a heslo, které podmiňují zpracovávání takové informace.

Třetím krokem je pak modifikace / metamorfóza vstupů a hledání. Při této fázi hledáme vstup, který by mohl způsobit nežádoucí stav systému. Jelikož se jedná o opakované zadávaní vstupů, podobných těm schváleným, jde o ideální činnost pro automatizaci. Při automatizaci je ale důležité, aby „umělá inteligence“ postupovala efektivně.

Efektivitu „umělé inteligence“ můžeme definovat ve třech bodech. Musí znát podstatu schválených vstupů, musí být schopná pozměnit tyto vstupy pro hledání neznámých vstupů, musí poznat podobné vstupy a neopakovat tak stejný test vícekrát. Úspora náročnosti testování pak závisí na komplexnosti systému. V případě nejjednodušších systémů s jedním metamorfním vztahem je to 50%, tj. Polovina původního testování je prováděna stále manuálně a polovina je automatizovaná. Čím je ale systém složitější, tím je úspora metamorfního testování za pomocí „umělé inteligence“ vyšší.

7. ZÁVĚR

Vzhledem k tomu, že železniční systém je založen na celkové bezpečnosti, bude vždy nutné před uplatněním výsledků projektu COSMOS, který klade důraz především na spolehlivost a zabezpečení proti kybernetickým rizikům, nejprve provést inspekci a přijmout pouze ta software vytvořená v projektu COSMOS, která neohrožují celkovou bezpečnost.

Na základě principů inženýrství, které se zabývá riziky, navrhujeme využít vytvářený systém pro podporu rozhodování, pomocí kterého budeme porovnávat efektivitu, nároky na znalosti, finance, operátory a čas na instalaci [35] se softwarovými produkty vytvořenými projektem COSMOS a vybereme lepší systém pro železniční praxi.

Poděkování: Autoři děkují za podporu projektu COSMOS.

LITERATURA

[1] EU.*COSMOS. DevOps for Complex Cyber-physical Systems*. ID: 957254, EU H2020. Brussels: EU 2021.
[2] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury.* ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.
[3] LEITL, R. *Spolehlivost elektrotechnických systémů*. Praha: SNTL1990.
[4] BARUTH, A. *Applied Dynamics*. New York: CRC Press 2014.
[5] KLAS, A. Krok za krokem k výnosné automatizaci montážních linek. *MM průmyslové spektrum*, 2004, 28 p.
[6] MAIXNER, L. *Navrhování automatických výrobních systémů*. Praha: NTL 1980.
[7] QS. *System Reliability Toolkit-V. New Approaches and Practical Applications*. Utica: Quanterion Solutions Inc. 2015. https://www.quanterion .com/KnowledgeBase/ReliabilityToolkit.shtml
[8] ZLOCHOVÁ, M. Optimalizace výrobních buněk. *Úspěch - Produktivita a inovace v souvislostech.* Praha: UVB 2012.
[9] PROCHÁZKOVÁ, D., SRP, J. , PROCHÁZKA, J. Analysis of Cyber Networks in a System Concept. In: *Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics.*

Recent Advances in Systems, Control, Signal Processing and Informatics. ISBN 978-1-61804-204-0, Rhodes Island 2013, pp. 102-109.
[10] PROCHÁZKOVÁ. D. *Safety of Complex Technological Facilities.* ISBN 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244 p.
[11] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu.* ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. Doi: 10.14311%2FBK.978 80 01066096.
[12] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení.* Praha: ČVUT 2017, 364 p. Doi: 10.14311/BK.9788001061824.
[13] MAYER-SCHÖNBERGER, V., CUKIER, K. *Big Data. Překlad Jakub Goner. : Revoluce, která změní způsob, jak žijeme, pracujeme a myslíme.* ISBN 978-80-251-4119-9. *Brno: Computer Press 2014, 256 p.*
[14] HELLE, P., SCHAMAI, W., STROBEL, C. Testing of Autonomous Systems - Challenges and Current State-of-the-Art. *INCOSE International Symposium Proceedings* 2016, pp. 571–584.
[15] MALAVOLTA, I., LEWIS, G., SCHMERL, B., LAGO, P., GARLAN, D. How Do You Architect Your Robots? State of the Practice and Guidelines for ROS-Based Systems. In: *Proceedings of the ACM/IEEE 42nd International.* New York 2020, pp. 31-40.
[16] TEPJIT, S., HORVÁTH, I., RUSAK, Z. The State of Framework Development for Implementing Reasoning Mechanisms in Smart Cyber-Physical Systems: A Literature Review. *Journal of Computational Design and Engineering.* 6 (2019),4, pp. 527-541.
[17] TÖRNGREN, M., SELLGREN, U. *Complexity Challenges in Development of Cyber-Physical Systems.* Cham: Springer 2018.
[18] GONZÁLEZ, C. A., VARMAZYAR, M., NEJATI, S., BRIAND, C., ISASI. Y. Enabling Model Testing of Cyber-Physical Systems. In *Proceedings of the 21th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems 2018,* pp.176-186.
[19] SONTGES, S., ALTHOFF., M. Computing the Drivable Area of Autonomous Road Vehicles in Dynamic Road Scenes. *IEEE Trans. Intell. Transp. Syst*. 19 (2018), 6, pp. 1855-1866.
[20] LOQUERCIO, A., KAUFMANN, E., RANFTL, R., DOSOVITSKIY, A., KOLTUN, V., SCARAMUZZA, D. Deep drone racing: From Simulation to Reality with Domain Randomization. *IEEE Transactions on Robotics.* 36 (2019), 1, pp. 1-14.
[21] ZAPRIDOU, E., BARTOCCI, E., KATSAROS, P. Runtime Verification of Autonomous Driving Systems in CARLA. In: *Runtime Verification.* Cham: Springer International Publishing 2020.
[22] GAMBI, A., HUYNH, T., FRASER, G. Generating effective test cases for self-driving cars from police reports. In: *Proceedings of the ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering 2019*, pp. 257-267.
[23] RICCIO. V. , TONELLA. P. Model-based Exploration of the Frontier of Behaviours for Deep Learning System Testing. In P*roceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering.* (ESEC/FSE '20). Association for Computing Machinery 2020.
[24] NGUYEN,Y., HUBER, S., GAMBI, A. Automated Generation of Diversified Tests for Self-driving Cars from Existing Maps. In *2021 IEEE International Conference on Artificial Intelligence Testing (AITest*). IEEE 2021, pp. 128-135.
[25] FLORES-GARCÍA, E,. KIM, G-E., YANG, J., WIKTORSSON, M., DO NOH, S. Analyzing the Characteristics of Digital Twin and Discrete Event Simulation in Cyber Physical Systems. In: *Advances in Production Management Systems. Towards Smart and Digital Manufacturing (IFIP Advances in Information and Communication Technology*), 592 (2020), pp. 238–244.
[26] VIKHRAM, R.,RAJVIKRAM Y., ELAVARASAN, M., MANOHARAN, M., MIHET-POPA, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access 8151019–151064;* 2020.
[27] ABDESSALEM, R. B., PANICHELLA, A., NEJATI, S., BRIAND, L. C., STIFTER, T. Testing autonomous cars for feature interaction failures using many-objective search. In: *IEEE/ACM International Conference on Automated Software Engineering.*. IEEE 2018, pp. 143-154.
[28] SIEMENS. *Digital Twins/ Software Siemens 2022.* https ://www.plm.automation.siemens.com/global/en/our- story/glossary/digital-twin/24465
[29] PARK, H., EASWARAN, A., ANDALAM, S. Challenges in Digital Twin Development for Cyber-Physical Production Systems. In: *Cyber Physical Systems. Model-Based Design*. Cham: Springer International Publishing 2021, pp. 28-48.

[30] PROCHAZKOVA, D., PROCHAZKA, J. Generation of Risk-Based Design of Socio-Cyber-Physical Systems. *International Journal of Economics and Management Systems.* 6 (2021), pp. 261– 272. http:// www.iaras.org/iaras/journals/ij EMS
[31] ZAMPETTI, F., TAMBURRI, D., PANICHELLA, A., PANICHELLA, S., DI PENTA, M., GERARDO, C. Continuous Integration and Delivery practices for Cyber-Physical systems: An interview based study - 2022. Doi: 10.1016/j.jss.2022.111425,10.21256/zhaw-25591
[32] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for Developing SPI Programs Related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191 p.
[33] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRAB KA, 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
[34] EU. *Maastricht Treaty*. Brussels: EU 1992. C 191, 29.7.pp.1–112.
[35] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy.* Praha: ČVUT 2022,129 p. Doi:10.14311/BK.97880010 69950
[36] PROCHÁZKA, J., NOVOBILSKÝ, P., PROCHÁZKOVÁ, D., VALOUSEK, S. Cybersecurity Design for Railway Products. In: *Understanding and Managing Risk and Reliability for a Sustainable Future.* ISBN 978-981-18-5183-4. Singapore: Research Publishing 2022, pp. 304-311. Doi:10.3850/978-981-18-5183-4_R09-01-099-cd
[37] PROCHÁZKOVÁ, D. Risk-Based Design of Technical facilities. In: JUFOS 2021. ISBN 978-80-214-5963-2. Brno: VUT 2021, pp. 40-51.
[38] ZIO, E. Some Challenges and Opportunities in Reliability Engineering. *IEEE Transactions on Reliability*. 65 (2016), 4, pp. 769-1782.
[39] IAEA. *Maintenance, Surveillance and In-service Inspection in Nuclear Power Plant*. Vienna: IAEA 2002, 95 p.
[40] JARDINE, A. K. S., TSANG, A. H. C. *Maintenance, Replacement, and Reliability: Theory and Applications.* London: CRC Press 2013.
[41] KIRAN, S., PRAJEETH KUMAR, K. P., SREEJITH, B., MURALIHARAN, M. Reliability Evaluation and Risk Based Maintenance in a Process Plant. *Procedia Technology*. 24 (2016), pp. 576-583. www.sciencedirect.com
[42] KRISHNASAMY, L., KHAN, F., HADDARA, M. Development of a Risk-based Maintenance (RBM) Strategy for a Power-generating plant. *Journal of Loss Prevention in the Process Industries.* 18 (2005), 2, pp. 69-81.
[43] MONTGOMERY, R. L., SERRATELLA, C. Risk-Based Maintenance: New Vision for Asset Integrity Management. In: *ASME 2002 Pressure Vessels and Piping Conference*. ISBN 0-7918-4655-5. Vancouver: ASME 2002, pp. 151-165.
[44] CENELEC. *EN 50126-1 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).* Brussels 2017.

METODICKÝ POSTUP K ZAJIŠTĚNÍ BEZPEČNOSTI TECHNICKÝCH DĚL

METHODOLOGICAL PROCEDURE TO ENSURE THE SAFETY OF TECHNICAL FACILITIES

Dana Procházková

České vysoké učení technické, Fakulta strojní, Technická 4, 166 00 Praha 6, danuse.prochazkova@fs.cvut.cz

Abstrakt: Článek se zabývá významem pojmu "bezpečnost" a soustřeďuje se na jeho význam pro technická díla. Vysvětluje vztahy mezi pojmy spolehlivost, odolnost, kritičnost, riziko a bezpečnost. Charakterizuje řízení bezpečnosti procesů a systém řízení bezpečnosti technických děl. Popisuje metodiku pro zajištění bezpečnosti technických děl.

Klíčová slova: bezpečnost, řízení rizik, řízení bezpečnosti procesů, systém řízení bezpečnosti, metodika.

Abstract: The article deals with the sense of the term "safety" and focuses on its meaning for technical facilities. It explains the relationships among the concepts of reliability, resilience, criticality, risk and safety. It characterizes the process safety management and the safety management system of technical facilities. It describes the methodology for ensuring the safety of technical facilities.

Key words: safety, risk management, process safety management, safety management system, methodology.

1. ÚVOD

Na základě současných znalostí a zkušeností je skutečností, že kvalita života, zdraví a bezpečí každého člověka závisí na kvalitě lidského společenství, ke kterému náleží. Vzhledem k tomu, že podle EU [1] a OSN [2] je nejvyšší kvalitou každého objektu (tj. státu, lidské komunity, technického zařízení atd.) bezpečnost, je nejvyšší prioritou pro objekt celková (integrální) bezpečnost. To znamená, že nejde jen o částečnou bezpečnost, jako je vnitřní, vnější, environmentální, požární, ekonomická atd., ale o bezpečnost celku, která zahrnuje částečné bezpečnosti tak, aby stav celku byl optimální. Vzhledem k systémové povaze dnešního světa nelze budovat integrální bezpečnost bez ohledu na ostatní druhy bezpečnosti, protože jejich cíle jsou pro lidskou společnost také důležité. Kromě celkové bezpečnosti je u technických děl také velmi důležitá bezpečnost základních procesů, které zajišťují výrobky a služby pro lidskou společnost.

Základní funkcí státu od jeho vzniku bylo zajištění bezpečnosti chráněných aktiv (zájmů) státu a udržitelného rozvoje státu. Chráněná aktiva (zájmy) státu jsou aktiva státu, která jsou chráněna prioritně, tj.: životy, zdraví a bezpečí obyvatel; majetek; životní prostředí; veřejné blaho; znalosti; kritické technologie a infrastruktury. Aby bylo zajištěno bezpečí a rozvoj veřejných aktiv i státu, musí stát dobře hospodařit se zdroji, majetkem a lidmi za normálních, nouzových a kritických podmínek [3].

Bezpečnost státu je ve své podstatě soubor lidských opatření a činností, které zajišťují bezpečí a udržitelný rozvoj státu a jeho veřejných aktiv; tj. omezují podmínky pro realizaci nebezpečí. Za tímto účelem by se správa státu neměla zabývat pouze přežitím, mocí, sociálním souladem a prevencí škod, ale měla by řešit metodicko-koncepční problémy a zajistit, aby:

- bezpečnost by byla posuzována v systémovém kontextu, tj. nejen ve spojení s předem definovanými riziky,
- koncepce bezpečnosti nebyla zatížena ideologickými a politickými klišé,
- řešení problémů bylo založeno na výsledcích teorie rozhodování,
- vztah mezi rizikem a bezpečností by byl správně chápán. Podstata problému spočívá v odpovědi na otázku: Jak jsou identifikována rizika a jejich dopady? Odpověď zní: Jsou určeny věrohodnými scénáři. Neexistuje však žádný postup, jak by měl být takový scénář vytvořen. Scénář je obvykle založen na minulých událostech a jevech a nebere v úvahu lidská porušení a existenci možných překvapení způsobených dynamickým vývojem světa a lidské společnosti,
- bral v úvahu dynamický vývoj světa, který způsobuje změny v povaze stávajících rizik a přináší nová rizika.

Stát hraje úlohu, kterou lze popsat z hlediska řízení rizik [3,4], protože přerozděluje určité druhy rizik prostřednictvím rozhodování o systému sociálního zabezpečení / veřejném blahu a zdravotní péči. Je třeba zvážit rizika a správně je řídit na všech úrovních veřejné správy, aby se zabránilo selháním v poskytování veřejných služeb.

Rizika vstupují do veřejné domény, pokud splňují některý z následujících atributů:

1. Jedná se o externality, které tržní mechanismy nemohou řešit.
2. V souvislosti s legislativou jsou občanům vnucovány škodlivé dopady technologií a špatná rozhodnutí veřejné správy.
3. Ohrožena je významná část veřejnosti, která nesouhlasí s koncepcí správy určitých aktiv.
4. Politická rozhodnutí bez ohledu na bezpečnost a rozvoj občanů vedou k jevům, při nichž se rizika realizují.
5. Nežádoucí jevy, které způsobují nepřijatelná rizika, jsou rozloženy tak, že ignorují politickou spravedlnost.

Orgány veřejné správy by proto měly analyzovat rizika jak z hlediska dopadů na společnost, tak z hlediska dopadů na systém řízení veřejné správy, neboť řada příkladů v minulosti ukázala, že rozhodování veřejné správy zhoršilo dopady nouzové situace [5-18]. Kroky procesu řízení rizik prováděné orgány veřejné správy se liší od běžného postupu řízení rizik [3] pouze v tom, že by měla být věnována značná pozornost formulaci souvislostí a sledování rizik ze strategického a procesního hlediska, tj.:

1. Schopnost orgánů veřejné správy a dalších zúčastněných stran dosáhnout strategických cílů v oblasti bezpečnosti, ochrany, mobility a environmentálních podmínek (zdravotní a environmentální rizika) by měla být posuzována ve strategickém kontextu.
2. Schopnost orgánů veřejné správy řešit problémy by měla být posuzována v organizačním kontextu.
3. V souvislosti s řízením rizik by měly být posuzovány prahové hodnoty rizika, maximální úrovně dopadů a správné priority pro rozhodování.

Vzhledem k dynamickému vývoji světa je nezbytné, aby veřejná správa, správci všech organizací státu (tj. veřejných institucí i soukromých subjektů) a jednotlivci přizpůsobili soubor lidských opatření a činností zajišťujících bezpečí a udržitelný rozvoj státu a jeho veřejných aktiv současným podmínkám. To znamená, že permanentní řízení rizik se musí provádět na všech úrovních organizací ve prospěch integrální bezpečnosti.

Předložený článek zkoumá problematiku bezpečnosti veřejných aktiv státu, které patří mezi technická díla. Jejich bezpečnost závisí nejen na nich samotných, ale také na kvalitě jejich vztahu k veřejné správě. Veřejná správa je potřebuje, protože poskytují produkty a služby občanům a státu, který tak plní řadu svých základních funkcí. Naopak technická zařízení potřebují veřejnou správu, protože ta nastavuje a kontroluje podmínky jejich činnosti.

2. BEZPEČNOST A KRITIČNOST TECHNICKÝCH ZAŘÍZENÍ

Technologie je aplikace znalostí k dosažení praktických cílů specifikovaným a reprodukovatelným způsobem. Jedná se o systémové využití znalostí pro praktické účely. Zatímco technologie přispívají k hospodářskému rozvoji a lidské prosperitě, mohou mít také nepřijatelné dopady, jako je znečištění nebo vyčerpávání zdrojů, nebo způsobit sociální škody , jako je technologická nezaměstnanost způsobená automatizací.

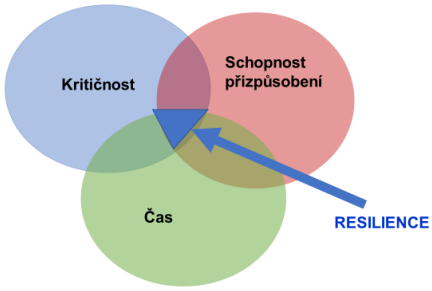
Inženýrství je proces, kterým je technologie vyvíjena a provozována. To často vyžaduje řešení problémů za přísných omezení, protože v sázce je bezpečnost lidí a dalších veřejných statků. Řízení bezpečnosti technických zařízení je proto zásadní.

Řízení bezpečnosti technických prací, které jsou komplexními systémy typu "systémů -SoS", lze definovat jako integrované plánování, návrh, optimalizaci, provoz a řízení výrobků, procesů a služeb ve prospěch lidí [3,4-20]. Pokud jde o konkurenceschopnost a hospodárnost, musí být rovněž zajištěna jejich výkonnost. To závisí na jejich odolnosti, která určuje, jak technické zařízení reaguje na škodlivé jevy všeho druhu. Z teorie řízení systému podle [20] vyplývá, že odolnost systému souvisí s robustností, redundancí, vynalézavostí a rychlostí spuštění správné reakce, obrázek 1.

Pro zvýšení bezpečnosti a resilience technických děl je nutné z hlediska zajištění jejich kritických prvků a celku použít velikosti pohrom s dobou návratnosti větší než 100 let (současné normy uvažují projektové pohromy na úrovni 100 let [20,24]). Dále záleží na tom, že při projektování zajišťuje pouze ochrana prvků a objektů pouze pro vyjmenované pohromy, tj. s dalšími možnými a nepojmenovanými pohromami se neuvažuje – správné je použít koncept „All-Hazard Approach“ [20].

Obr. 1. Souvislosti resilience (houževnatosti) systému s robustností, redundancí, vynalézavostí a rychlostí [24].

Vzhledem k tomu, že technická díla poskytují lidstvu životně důležité funkce, je třeba dbát na zajištění kontinuity provozu, pro které je resilience důležitá. Idea resilience je zobrazena jako průsečík tří kruhů, obrázek 2. Resilience znamená neustálé zvyšování bezpečnosti i zabezpečení při řešení potenciálních konfliktů, které vznikají v praxi.



Obr. 2. Kritické parametry, které jsou důležité pro resilienci [24].

Resilience je potenciál systému, který spočívá ve specifickém uspořádání systému, které udržuje funkce a zpětné vazby systému v kondici, která udržuje schopnost systému reorganizovat se na základě změn vyvolaných poruchami. Z toho vyplývá, že řízení udržitelnosti systému musí být založeno na řízení resilience, které má dva cíle:

1. Zabránit tomu, aby se systém dostal do nepřijatelného stavu v důsledku vnějších poruch a vnější zátěže.
2. Uchovat prvky aktivující systémovou reorganizaci a obnovu v důsledku masivních změn.

Další důležitou vlastností technických zařízení je kritičnost [20], která je funkcí resilience a nezbytnosti (důležitosti) pro bezpečnost systému. Na kritičnost lze pohlížet ze dvou hledisek, a to z hlediska technického (poruchovost prvků systému u, tj. technického díla) a sociálního (dopady nefunkčnosti poskytování služeb technickým dílem obyvatelstvu). Oba aspekty jsou důležité z hlediska národní bezpečnosti. Z hlediska bezpečnosti provozu technických děl je důležitý první aspekt; jeho hodnota je stanovena projektem technického díla.

3. DRUHY BEZPEČNOSTI TECHNICKÝCH ZAŘÍZENÍ

S ohledem na současné znalosti a zkušenosti je v současné době sledována bezpečnost procesů a celková (integrální) bezpečnost technických děl.

Bezpečnost procesů je soubor opatření a činností, který zajišťuje bezpečný provoz, tj. bezpečný průběh procesů, např. v případě chemických procesů se zaměřují na prevenci požárů, výbuchů a úniků nebezpečných látek do životního prostředí [21]. Specifická disciplína řízení bezpečnosti procesů (PSM – process safety management) se vyvíjí posledních 40 let a jejím cílem je zajistit bezpečné procesy, které probíhají v technologiích, jde o řízení principů a systémů pro identifikaci možných ohrožení, pochopení a zvládnutí procesů vedoucích k realizaci rizik. Jedná se o složitý postup, který vyžaduje vícerozměrný přístup, který kombinuje technologie a jejich řízení [20].

Řízení bezpečnosti procesů je spojeno s kulturou bezpečnosti a pro hodnocení bezpečnosti se často používá kontrolní seznam [22].

Řízení bezpečnosti procesů je široce používáno v továrnách a dalších automatizovaných prostředích k zajištění efektivity výroby. Technologie řízení bezpečnosti procesů je obecně navržena tak, aby monitorovala senzory a nastavovala důležité veličiny podle naměřených hodnot. Tato technologie umožňuje relativně malé skupině lidí řídit složité operace a pomáhá zajistit, aby bylo trvale dosaženo požadovaného výsledku.

Bezpečnost systému je soubor opatření a činností, který zajišťuje bezpečné technické dílo a jeho bezpečné okolí. Předmětná disciplína vznikla na základě systémového přístupu ve strojírenských oborech. Integrální (celková, objektová) bezpečnost má své kořeny v inženýrství bezpečnosti průmyslu , které sahá až do 19. století a které po 2. světové válce aplikovalo disciplíny: systémové inženýrství a systémovou analýzu k řešení nových a složitých inženýrských problémů.

Bezpečnost systému ve sledovaném pojetí spočívá v aplikaci technických a manažerských dovedností při identifikaci, analýze, hodnocení a řízení škodlivých jevů a souvisejících rizik pomocí systémového přístupu [4-24]. Z praktických důvodů musí být přístupy používané e sledované oblasti účinné a cenově dostupné. Orientace na bezpečnost musí být součástí systému řízení podniku a zároveň musí respektovat omezení, která vyplývají z vnějšího světa.

Předmětná disciplína definuje:
- technické zařízení jako systém, což je kombinace lidí, postupů a zařízení, které jsou integrovány k provádění specifického provozního úkolu nebo funkce v určitém prostředí,
- koncept bezpečnosti systému jako aplikaci speciálních technických a organizačních dovedností s cílem systematicky předcházet škodám a ztrátám na majetku s nimi spojených identifikací ohrožení a řízením rizik po celou dobu životnosti každého díla nebo objektu vytvořeného a implementovaného člověkem.

OECD postupem času vyvinula samostatné koncepce pro jaderný a chemický průmysl [19]. Tento koncept je v práci [23] doplněn kybernetickým zabezpečením technického díla vzhledem k rostoucí roli automatizace v současné době.

Bezpečnost systému aplikovaná na technická díla využívá teorii systémů a systémové inženýrství k prevenci předvídatelných nehod a k minimalizaci následků nepředvídatelných nehod. V moderním pojetí se obecně zajímá o všechny ztráty a škody, a to nejen o smrtelné nehody nebo zranění a škody na majetku, ale také o nesplnění poslání (mise, účelu) nebo poškození životního prostředí. Klíčovým bodem disciplíny je považovat ztráty za natolik závažné, aby se na jejich prevenci věnoval dostatek času, úsilí a zdrojů. Výše investic věnovaných na prevenci nehod a/nebo jejich dopadů do značné míry závisí na sociálních, politických a ekonomických faktorech. Proto u technologií, které mohou mít vážné důsledky, je požadavek předběžné opatrnosti uložen právními předpisy, aby byla zajištěna ochrana veřejných aktiv [24].

Hlavním zájmem bezpečnosti technických děl je kvalifikované řízení rizik, tj.: identifikace možných ohrožení; stanovení a vyhodnocení rizik; a eliminace a/nebo řízení rizik prostřednictvím analýzy projektu a/nebo organizačních postupů. Program bezpečnosti technických děl musí stanovit přesně vymezený postup metodické kontroly hledisek souvisejících s bezpečností a hodnotit projekt technického díla ve smyslu identifikace možných zdrojů rizik a předepsání časových a nákladově efektivních nápravných zásahů. Cílem programu pro technická díla je zajistit:
- bezpečnost technického díla, která odpovídá jeho poslání, která je vložena inherentně do projektu,
- identifikaci, posuzování, odstraňování a/nebo řízení rizik na přijatelnou úroveň rizik pro všechna rizika spojená se systémem, subsystémem a jednotlivými částmi,
- řízení rizik od hrozeb, která nelze eliminovat; tj. rizika musí být zajištěna tak, aby byl ochráněn personál, zařízení a majetek,
- aby použití nových materiálů a/nebo výrobků a zkušebních metod představovalo pouze minimální riziko,
- potřeba nápravných opatření potřebných ke zlepšení bezpečnosti dočasným začleněním bezpečnostních faktorů byla při budování systému minimalizována,
- aby historické údaje o bezpečnosti získané z podobných bezpečnostních programů se braly úvahu a použily se tam, kde je to vhodné.

Průmyslová odvětví buď přizpůsobila programy bezpečnosti systémů od armády nebo NASA, nebo nezávisle vyvinula své vlastní programy založené na zkušenostech získaných z výstavby jaderných elektráren, z výroby složitých, nebezpečných a drahých zařízení. Čekání na nehody a následné odstranění příčin se stalo neekonomickým a někdy dokonce nepřijatelným způsobem modifikace a zlepšování systémů.

Budování mnoha dnešních složitých systémů vyžaduje integraci částí (subsystémů a komponent) vyrobených různými nezávislými dodavateli a organizacemi. I když každý dodavatel zachovává požadovanou kvalitu svých dílů, kombinace subsystémů přináší nové chyby a nová nebezpečí, která nejsou viditelná, pokud se na ně pohlíží jako na samostatné díly.

Zvažování rizik spojených s kombinací systémů a subsystémů se v praxi označuje jako vytváření inherentní bezpečnosti. V mnoha průmyslových odvětvích bylo potvrzeno, že začleněním inherentní bezpečnosti do zařízení nebo výrobků se mohou snížit jejich celkové náklady na životní cyklus a že dosažení přijatelné úrovně bezpečnosti vyžaduje pokročilé moderní přístupy k bezpečnosti systémů [24].

Činnosti související s bezpečností systému začínají v nejranějších fázích vývoje koncepce systému a pokračují přes všechny činnosti návrhu, výroby, testování, provozu a odstavení. Zásadním aspektem, který odlišuje přístup bezpečnost systému od jiných přístupů používaných v oblasti bezpečnosti, je primární důraz na včasnou identifikaci a klasifikaci rizik, aby bylo možné přijmout nápravná opatření k jejich odstranění nebo minimalizaci před konečným rozhodnutím o projektu.

Přestože je bezpečnost systémů poměrně novou a stále se vyvíjející disciplínou, má své základní myšlenky, které jsou zachovány ve všech jejích projevech a odlišují ji od jiných přístupů k bezpečnosti a řízení rizik. Principy řízení bezpečnosti systému v současné koncepci jsou:
- bezpečnost je vytvářena krok za krokem od začátku návrhu systému a není přidávána do vytvořeného systému,
- bezpečnost se týká systému jako celku a nejen dílčích systémů a komponent,
- bezpečnost bere ohrožení a související nebezpečí ve větší šíři než jen jako chyby personálu,
- vytváření bezpečnosti klade důraz spíše na analýzu než na zkušenosti získané později a standardy vyvinuté později,
- kvalitativní přístupy jsou upřednostňovány před kvantitativními,
- rozpoznává se důležitost změn a konfliktů cílů v projektu systému, což přesahuje inženýrství systémů.

Nejdůležitějším aspektem bezpečnosti systému z hlediska prevence nehod jsou postupy řízení bezpečnosti. Efektivní řízení bezpečnosti spočívá ve stanovení politik a definování cílů bezpečnosti, tj. v:
- plánování úloh a postupů,
- vymezení odpovědností a určení kompetencí,
- dokumentace a průběžné sledování hrozeb a z nich vyplývajících nebezpečí, včetně kontrol,
- údržba informačního systému pro řízení bezpečnosti, včetně zpětné vazby a formulářů hlášení poruch/nehod apod.

Bezpečnost systému je zodpovědný za zajištění bezpečnosti systému jako celku, včetně analýzy rozhraní mezi komponentami. Činnosti v oblasti bezpečnosti komponent, jako je bezpečnost odpalovací rampy raket, mohou být součástí obecné odpovědnosti za bezpečnost systému nebo mohou být součástí inženýrství komponent ve velkých a složitých projektech. Pro definované druhy nebezpečí, jako je požár, jaderná bezpečnost nebo výbušné prostředí, může být požadována další členění odpovědnosti za bezpečnost.

V jakékoli gradaci členění úsilí o zajištění bezpečnosti systému jsou systémoví inženýři zodpovědní za integraci jednotlivých bezpečnostních činností a informací. Bezpečnost systému je obvykle spojena s odpovídajícími inženýrskými a/nebo vědeckými disciplínami, jako je spolehlivostní inženýrství, zajištění kvality, lidský faktor atd. Jaké procesy a úkoly týkající se bezpečnosti systému budou prováděny v konkrétním projektu, závisí na jeho velikosti a úrovni rizika navrženého systému [24].

Bezpečnost a spolehlivost systému spolu úzce souvisí [20,25]. V praxi je bezpečné zařízení nebo bezpečný systém spolehlivý, ale spolehlivé zařízení nebo spolehlivý systém nemusí být bezpečné. Inženýrství spolehlivosti přednostně řeší chyby a snižuje jejich četnost. Spolehlivost je definována jako charakteristika daného objektu vyjádřená pravděpodobností, že objekt bude vykonávat specifikovaným způsobem funkce, které jsou od něj požadovány během určitého časového intervalu a za specifikovaných nebo předpovězených podmínek. Reprezentativní techniky inženýrství spolehlivosti zaměřené na minimalizaci chyb komponent (komponent) a tím i složitých selhání systému způsobených chybami komponent jsou: paralelní redundance; zálohování zařízení; bezpečnostní rezervy; snižování počtu přetížení; a omezení doby použití.

Ukázalo se, že tyto techniky jsou účinné při zvyšování spolehlivosti, ale nemusí nutně zvyšovat efektivitu a mohou ji dokonce za určitých okolností snížit (např. začlenění více záloh do systémů může vytvořit prostředí pro nežádoucí vazby a afinity mezi komponentami, které za určitých podmínek způsobují selhání). Proto analýzy rizik spojené s bezpečností systému sledují interakce a nezaměřují se pouze na technické chyby nebo nejistoty.

Inženýři zabývající se spolehlivostí často považují spolehlivost a bezpečnost za synonyma. To platí pouze v některých zvláštních případech. Obecně platí, že bezpečnost má o něco širší význam. Spolehlivost a bezpečnost mají obvykle mnoho společných vlastností. K mnoha selháním však dochází, aniž by došlo k selhání součásti. Naopak, mnohokrát všechny složky nehod fungovaly podle očekávání a bezchybně [24]. Může se také stát, že komponenty mohou selhat (selhat) a nezpůsobit havárii. Je skutečností, že poruchy a nehody mohou být způsobeny provozem zařízení mimo povolené rozsahy hodnot ukazatelů nebo časové limity, na nichž byly založeny analýzy spolehlivosti. To znamená, že systém může mít vysokou spolehlivost a přesto havarovat. Zobecněné analýzy pravděpodobností a spolehlivosti navíc nelze přímo aplikovat na specifické nebo místní podmínky. A co je nejdůležitější, havárie a nehody často nejsou výsledkem jednoduché kombinace chyb / selhání součástí [24].

Bezpečnost je vlastnost, která vystupuje na úrovni systému, když jsou komponenty provozovány společně. Události vedoucí k nehodě mohou být složitou kombinací chyb zařízení, nesprávné údržby, problémů s informačním a řídicím systémem, lidského zásahu a konstrukčních chyb. Analýzy spolehlivosti se zaměřují pouze na pravděpodobnosti nehod a nehod souvisejících s chybami; nezkoumají potenciální poškození, které může být způsobeno správnou funkcí (provozem) jednotlivých komponent. Proto není možné, aby inženýrství spolehlivosti nahradilo inženýrství zacílené na bezpečnost systému, ale může ji doplnit. To však musí být provedeno s jasným vědomím, že konečným cílem je zvýšit odolnost systému vůči nebezpečí výskytu náhodných chyb. Vždy je lepší, když je zařízení/systém navržen tak, aby jednotlivé náhodné chyby nemohly způsobit nehodu.

Při používání technik odhadu spolehlivosti pro posouzení bezpečnosti je třeba postupovat velmi opatrně. Pokud havárie či nehody nejsou nevyhnutelně způsobeny jevy, které lze vyjádřit pravděpodobností výskytu, nelze na ně obecně vztáhnout míru pravděpodobnosti výskytu rizika. Odhady pravděpodobnosti výskytu měří pravděpodobnost výskytu náhodných chyb, nikoli pravděpodobnost výskytu rizik nebo nehod. Praxe ukazuje, že když je během analýz systému nalezena chyba projektu, je mnohem efektivnější ji opravit, než přesvědčovat někoho pomocí vypočtených pravděpodobností, že chyba nikdy nezpůsobí havárii. Vysoké hodnoty pravděpodobnosti spolehlivého chování nezaručují bezpečnost a z praxe je známo, že bezpečnost často nevyžaduje ultra vysokou spolehlivost [24].

Nejčastěji hlavní nevýhodou pravděpodobnostních modelů není to, co obsahují, ale to, co neobsahují. Nízké hodnoty pravděpodobnosti výskytu nespolehlivého chování jednoduše naznačují, že systém neselže zamýšleným způsobem, ale neříkají nic o skutečnosti, že systém může selhat s mnohem vyšší pravděpodobností způsobem, který nebyl uvažován [24]. Odlišení rizika spojeného se vznikem nehody od chyb je zásadní pro pochopení rozdílu mezi bezpečností a spolehlivostí.

Z praktických důvodů musí být přístupy a programy pro zajištění bezpečnosti systému efektivní a cenově dostupné. Návratnost nákladů na program pro zajištění bezpečnosti systému je dosažena tehdy, když se zabrání haváriím. Účinnost programu na zajištění bezpečnosti systému je velmi obtížné prokázat, protože měření něčeho, co se nestalo, je obtížné. Jedním z nepřímých způsobů, jak měřit efektivitu předmětného programu, i když ne zcela uspokojivé kvůli nedostatku porovnávaných faktorů, je porovnat provoz systémů, které měly předmětný program s těmi, které neměly a havarovaly. Dalším způsobem, jak určit účinnost programu pro zajištění bezpečnosti systému, je hlášení nebezpečí, jejichž realizace byla odvrácena zásahem pracovníků předtím, než došlo k nehodě, anebo byla jinak zjištěna. Třetím způsobem odhadu účinnosti programů pro zajištění bezpečnosti systému je vyšetřování případů, kdy nebyla respektována doporučení pro zajištění bezpečnosti systému a došlo k nehodám.

4. POSTUPY PRO ZAJIŠTĚNÍ BEZPEČNOSTI TECHNICKÝCH DĚL

Na základě současných poznatků shrnutých v pracích [5-20,23,24] zahrnuje systém řízení bezpečnosti technických děl organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro stanovení a uplatňování prevence pohrom nebo alespoň zmírnění jejich nepřijatelných dopadů v technickém díle a okolním území. Zpravidla zahrnuje řadu otázek, mimo jiné organizaci, personál, identifikaci a hodnocení hrozeb a z nich vyplývajících rizik, organizační operace, řízení organizačních změn, havarijní a krizové plánování, monitorování bezpečnosti, audity a přezkumy [23]. Na základě[poslední citované práce je systém řízení bezpečnosti (safety management system - SMS) technického díla integrovaným řízením 7 procesů:

1. Proces návrhu a realizace koncepce a řízení, který je dále rozdělen do dílčích procesů, aby byly zajištěny: celková koncepce bezpečnosti; dílčí cíle bezpečnosti; řízení/správa bezpečnosti; systém řízení bezpečnosti; zaměstnanci (podproces se dále dělí do následujících oddílů: řízení lidských zdrojů, školení a vzdělávání, interní komunikace/povědomí a pracovní prostředí); a přezkoumání a hodnocení plnění cílů bezpečnosti.

2. Proces provádění administrativních postupů, který se dále dělí na dílčí procesy, aby byly zajištěny: identifikace ohrožení od možných pohrom hodnocení rizik; vedení dokumentace; administrativní postupy (včetně systémů pracovního povolení); řízení změn; bezpečnost ve spolupráci s dodavateli; a dohled nad bezpečností výrobků.
3. Proces technických záležitostí, který je dále rozdělen do dílčích procesů pro: výzkum a vývoj; projektování a montáž; inherentní bezpečnost procesu; průmyslové normy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů.
4. Proces externí spolupráce, který se dále dělí na: spolupráci se správními orgány; spolupráci s veřejností a dalšími zúčastněnými stranami (včetně akademických pracovišť); a spolupráci s jinými podniky.
5. Proces havarijní připravenosti a odezvy na havárie a nehody, který se dále dělí na dílčí procesy pro: plánování připravenosti na odezvu uvnitř technického díla; usnadnění plánování připravenosti na odezvu vně technického díla (které spadá do odpovědnosti veřejné správy);a koordinaci, jakož i činnosti resortních organizací při zajišťování havarijní připravenosti a odezvy.
6. Proces zpracování hlášení a vyšetřování havárií/skoronehod, který se dále dělí na podprocesy pro: zpracování zpráv o haváriích, nehodách, skoronehodách a dalších významných zkušenostech; vyšetřování nežádoucích jevů; a r odezvu na havárie a nehody a následná opatření (včetně uplatňování získaných zkušeností a sdílení informací).
7. Proces fyzické a kybernetické bezpečnosti technického zařízení, který se dále dělí na podprocesy pro zajištění: fyzické bezpečnosti; a kybernetické bezpečnost proti hackerům a teroristům.

Systém řízení bezpečnosti (SMS) technického díla je založen na koncepci prevence pohrom nebo alespoň jejich závažných dopadů [19,23,24], která zahrnuje povinnost zavést a udržovat systém řízení, ve kterém jsou zohledněny následující problémy:

- role a povinnosti osob zapojených do zvládání závažných ohrožení od pohrom všeho druhu na všech organizačních úrovních technického díla a opatření v oblasti odborné přípravy v souladu se zjištěnými potřebami odborné přípravy,
- plány pro systematické zjišťování závažných ohrožení od pohrom a z nich vyplývajících rizik spojených s normálními a abnormálními podmínkami, a pro vyhodnocování jejich pravděpodobnosti a závažnosti (velikosti),
- plány a postupy pro zajištění bezpečnosti všech konstrukčních částí a funkcí v technickém díle a v jeho okolí, včetně údržby objektů a vybavení,
- plány realizace změn v technickém díle, jeho objektech i zařízení a území,
- plány na určení předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testování a posouzení pohotovostních plánů pro odezvu na tyto nouzové situace,
- plány pro průběžná hodnocení souladu s cíli uvedenými v koncepci bezpečnosti a v SMS a mechanismy pro vyšetřování a provádění nápravných opatření v případě nedosažení stanovených cílů,
- plány pro pravidelná systematická hodnocení koncepce bezpečnosti, účinnosti a vhodnosti systému řízení bezpečnosti (SMS) a kritéria pro hodnocení úrovně bezpečnosti špičkovým týmem pracovníků technického díla.

Bezpečnost je záležitostí všech zúčastněných, tj. manažerů, zaměstnanců a náhodně přítomných. V této souvislosti hovoříme o tzv. ***zlatých pravidlech všech zúčastněných***[24], kterými jsou:

- dle svých možností předcházet pohromám nebo alespoň jejich nepřijatelným dopadům pomocí preventivních opatření, zajistit připravenost na řešení nepřijatelných dopadů na chráněná aktiva (zájmy) technického díla a účinnou odezvu technického díla,
- komunikovat a spolupracovat s ostatními subjekty zapojenými do všech aspektů prevence, připravenosti a odezvy technického díla,
- znát ohrožení vyplývající z pohrom a možná rizika v technickém díle a jeho okolí,
- zavádět a respektovat "kulturu bezpečnosti", která je vždy respektována a prosazována všemi zúčastněnými stranami,
- zavádět systémy řízení bezpečnosti, sledovat a v případě potřeby upravovat jejich činnosti,
- uplatňovat zásady inherentní bezpečnosti při navrhování, projektování a provozu technického díla a jeho vybavení,
- pečlivě řídit změny v technickém díle,
- být připraveni vyrovnat se s jakýmikoli škodlivými jevy, které se mohou vyskytnout,
- pomáhat ostatním zúčastněným stranám při plnění jejich úloh a povinností,

- provádět neustálé zvyšování bezpečnosti,
- pracovat v souladu s kulturou bezpečnosti, bezpečnými postupy a výcvikem,
- usilovat o to, aby byly aktuální informace a informace a poskytovaly zpětnou vazbu vedoucím pracovníkům,
- usilovat o rozvoj, posilování a neustálé zlepšování koncepce bezpečnosti, nařízení a směrnic,
- vést a motivovat všechny ostatní zúčastněné k tomu, aby plnily své role a povinnosti,
- znát rizika uvnitř sféry vlastní odpovědnosti, vhodně plánovat opatření pro jejich řádné řízení,
- používat vhodnou a koherentní politiku plánování a následných činností,
- být si vědom rizik v technickém díle a vědět, co dělat, pokud budou realizována,
- podílet se na havarijním plánování a odezvě na havárie.

Kultura bezpečnosti znamená, že osoba ve všech svých rolích (manažer, zaměstnanec, občan nebo oběť pohromy) dodržuje zásady bezpečnosti, tj. chová se tak, aby nezpůsobovala realizaci možných rizik a když se stane účastníkem realizace rizik, přispívá k účinné odezvě, stabilizaci chráněných zájmů a jejich obnově a zahájení jejich dalšího rozvoje. Účinná kultura bezpečnosti je základním prvkem bezpečnosti. Odráží koncept bezpečnosti a je založena na hodnotách, názorech a činnostech vrcholových manažerů organizace a jejich komunikaci se všemi zúčastněnými stranami. Je to jasný závazek aktivně se podílet na řešení otázek spojených s bezpečností a prosazuje, aby všechny zúčastněné strany jednaly bezpečně a dodržovaly příslušné zákony, standardy a normy. Pravidla kultury bezpečnosti musí být začleněna do všech činností v technickém díle. Nejsou založena na soustředění se na potrestání viníků/pachatelů chyb, ale na poučení se z chyb a zavádění nápravných opatření tak, aby se chyby nemohly opakovat nebo alespoň aby se výrazně snížit jejich výskyt.

Nástrojem pro zajištění bezpečného technického díla, tj. takového technického díla, ve kterém existuje účinná kultura bezpečnosti, je program pro zvyšování bezpečnosti technického díla [24]. Postup pro vytvoření programu pro zvyšování bezpečnosti technického díla podle [19] se skládá z následujících kroků:

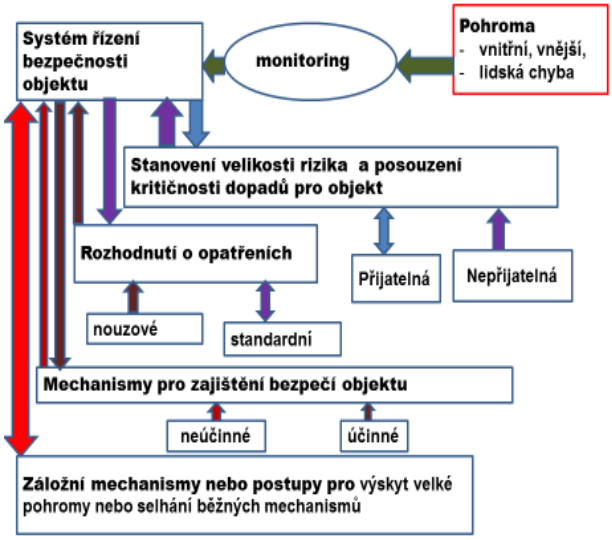
1. Definovat úkoly (dílčí cíle) a strategické cíle technického díla s ohledem na bezpečnost.
2. Pro každý úsek technického díla (spojeného s výše uvedenými procesy a dílčími procesy) zvolit vhodné cílové a průběžné ukazatele pro posuzování úrovní bezpečnosti nebo vypracovat zvláštní kontrolní seznamy.
3. Vytvořit slovník pro potřeby řízení integrální bezpečnosti technického díla.
4. Sladit standardy, metody dobré praxe a místní postupy.
5. Stanovit seznam cílových ukazatelů nebo mezních hodnot pro kontrolní seznamy podle podmínek v daném technickém díle.
6. Stanovit seznam průběžných ukazatelů nebo průběžných mezních hodnot pro kontrolní seznamy podle podmínek v daném technickém díle.
7. Stanovit způsob hodnocení cílových ukazatelů (tj. hodnotový systém) nebo kontrolních seznamů podle podmínek v daném technickém díle.
8. Stanovit způsob hodnocení průběžných ukazatelů (tj. hodnotový systém) nebo kontrolních seznamů podle podmínek v daném technickém díle.
9. Stanovit metodu/stupnici pro měření souboru ukazatelů (tj. souboru hodnot) nebo sadu kontrolních seznamů (systém pro podporu rozhodování [24]) a mezní limity podle podmínek v daném technickém díle.

Obrázky 3 a 4 ukazují představu o řízení bezpečnosti entity na základě výše uvedených poznatků o řízení rizik [20]. První je jednodušší a druhý ukazuje způsob rozhodování zabudovaný do systému řízení bezpečnosti technického díla.

5. ZÁVĚR

Inženýrství orientované na bezpečnost cíleně provádí úkoly řízení bezpečnosti, tj. úkoly řízení rizik ve prospěch bezpečnosti a vývoje lidského systému. V technickém slangu hovoříme o vytvoření inherentní bezpečnosti technického díla proti projektovým pohromám pomocí řízení bezpečnosti. Při uplatňování zásady předběžné opatrnosti zajišťujeme zvýšení odolnosti vůči nepřijatelným dopadům nadprojektových pohrom, jejichž výskyt je tak nepravděpodobný, že je nepředvídatelný. Do praxe se v technologiích na základě zmíněných cílů zavádí principy jako „selži bezpečně“, „prováděj jen určené funkce, tj. když nemůžeš splnit cíl, tak nic nedělej“… [20].

Obr. 3. Milníky, které rozhodují o bezpečném nebo nebezpečném chování technického díla v případě nebezpečné situace.



Obr. 4. Představa o způsobu řízení bezpečnosti technického díla zabudovaná do systému řízení bezpečnosti.

Předmětné inženýrství je založeno na řízení bezpečnosti, které je založeno na specifickém řízení rizik [20], které se vyznačuje zejména následujícími vlastnostmi:

- umísťování - projektování - konstrukce - návrh s minimalizací rizik, tzv.: risk-based design, risk-based operation, risk-based maintenance atd.,
- provoz se začleněným systémem včasného varování a postupy pro řízení přijatelné úrovně rizik,
- zvládání abnormálních, nouzových a kritických podmínek během provozu a odstávky.

Specifičnost sledovaného řízení rizik spočívá v tom, že se jedná o řízení rizik [4]:

- od všech možných pohrom najednou, přičemž příslušný seznam pohrom je určen přístupem All-Hazard-Approach [26, 27] (tj. zvažováním všech možných pohrom bez ohledu na to, zda jejich zdroje leží uvnitř nebo vně systému)
- a hledá se optimální řešení pro příslušné možné pohromy a přitom se uplatňují zásady předběžné opatrnosti, které zahrnuje udržitelný rozvoj.

Inženýrství zacílené na bezpečnost [20] při stanovení rizika používá principy:

- riziko je určováno během celého životního cyklu technického díla, tj. během výběru lokality, projektování, výstavby, provozu a vyřazení z provozu, a případně i při uvedení území do původního stavu,

- stanovení rizik se zaměřuje na požadavky uživatelů a úroveň poskytovaných služeb,
- rizika jsou určována podle kritičnosti dopadů na procesy, poskytované služby a aktiva stanovená veřejným zájmem,
- nepřijatelná rizika jsou zmírňována pomocí nástrojů řízení rizik, tj. pomocí technických a organizačních opatření, standardizací provozních postupů nebo automatizovanými kontrolami.

Předmětné inženýrství je z odborného hlediska proces, který vyhledává všechny možné podmínky, které by ohrožovaly úspěšné fungování monitorovaného technického díla ve všech fázích jeho životnosti, a identifikuje možnosti jejich řízení prevencí, připraveností, reakcí a obnovou.

LITERATURA

[1] EU. *Maastricht Treaty*. C 191, 29.7.pp.1–112. Maastricht: EU 1992

[2] UN. *Human Development Report*. New York 1994, www.un.org

[3] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace.* ISBN 978-80-01-04844-3. Praha : ČVUT 2011, 483 p.

[4] PROCHÁZKOVÁ, D. *Analýza, řízení a vypořádání rizik spojených s technickými díly.* Praha: ČVUT 2018, 222 p. Doi:10.14311%2FBK.9788001064801

[5] BRIŠ, R., GUEDES SOARES, C. & MARTORELL, S., eds. *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362 p.

[6] ALE, B., PAPAZOGLOU, I., ZIO, E., eds. *Reliability, Risk and Safety*. ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448 p.

[7] BERENGUER, C., GRALL, A., GUEDES SOARES, C., eds. *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035 p.

[8] IAPSAM, eds. *Probabilistic Safety Assessment and Management Conference. International. 11th 2012. (and Annual European Safety and Reliability Conference*). ISBN: 978-1-62276-436-5. Helsinki: IPSAM &ESRA 2012, 6889 p.

[9] STEENBERGEN, R., VAN GELDER, P., MIRAGLIA, S., TON VROUWENVELDER, A., eds. *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387 p.

[10] NOWAKOWSKI, T., MLYŇCZAK, M., JO-DEJKO-PIETRUCZUK, A., WERBIŇSKA-WOJCIECHOWSKA, S., eds . *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453 p.

[11] PODOFILLINI, L., SUDRET, B., STOJA-DINOVIC, B., ZIO, E., KRÖGER, W., eds. *Safety and Reliability of Complex Engineered Systems.* ISBN 978-1-138-02879-1. London: CRC Press 2015, 4560 p.

[12] WALLS, L., REVIE, M., BEDFORD, T., eds. *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL* ISBN 978-1-315-37498-7. London: CRC Press 2016, 2942 p.

[13] CEPIN, M., BRIS, R., eds. *Safety and Reliability – Theory and Applications*. ISBN: 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.

[14] 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.

[15] BEER, M., ZIO, E., eds. *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*. ISBN 978-981-11-2724-3. Singapore: ESRA, Research Publishing 2019, 4315 p., e:enquiries @rpsonline.com.sg

[16] BARALDI, P., DI MAIO, F., ZIO, E., eds. *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15).* ISBN 978 -981-14-8593-0. Singapore: ESRA, Research Publishing 2020, 5067 p., enquiries@rpsonline.com.sg

[17] CASTANIER, B., CEPIN, M., BIGAUD, D., BERENGUER, C., eds. *Proceedings of the 31st European Safety and Reliability Conference* . ISBN 978-981-18-2016-8. Singapore: ESRA, Research Publishing 2021, 3473 p., enquiries@rpsonline.com.sg

[18] LEVA, M.C., PATELLI, E., PODOFILLINI, L., WILSON, S., eds. *Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)*. ISBN 978-981-18-5183-4. Singapore: ESRA, Rese- arch Publishing 2022, 3413 p., enquiries@rpsonline.com.sg

[19] OECD. Guidance on Safety Performance Indicators. Guidance for Industry, Public Autho-rities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response. Paris: OECD 2002, 191 p.

[20] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení.* ISBN 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364 p. Doi:10.14311%2FBK.9788001061824
[21] EU. *Seveso III Directive (2012/18/ EU).* Brussels: EU 2012.
[22] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessee: US DOE 1996, 180 p.
[23] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. Praha: ČVUT 2022, 129 p. Doi:10.14311/BK.978 80010 69950
[24] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OU-HRABKA, 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.978800 1066751
[25] RAUSAND, M. *Reliability of* Safety-Critical *Systems: Theory and Applications*. John Wiley & Sons 2014, 421 p.
[26] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.
[27] EU. *FOCUS Project*. Brussels: EU 2012, http://www.focusproject.eu/documents /14976/-5d7 63378-1198-4dc9-86ff-c46959712f8a

METODIKA PRO APLIKACI ŘÍZENÍ BEZPEČNOSTI PROCESU BĚHEM EXPERIMENTU

METHODOLOGY FOR THE APPLICATION OF PROCESS SAFETY MANAGEMENT DURING THE EXPERIMENT

Dana Procházková

České vysoké učení technické v Praze, Technická 4, 166 00 Praha 6, Česká republika, danuse.prochazkova@fs.cvut.cz

Abstrakt: Každý experiment, který řeší praktické problémy, je proces, který probíhá za určitých podmínek, které významně ovlivňují jeho výsledky. Výsledky experimentu jsou dále ovlivněny kvalitou: vstupů; technického a kybernetického vybavení; způsobem řízení; a znalostmi, zkušenostmi a dovednostmi personálu. Proto musí být experimenty podporující průmyslovou praxi prováděny pomocí metodiky, která zajišťuje, že výsledky jsou vždy požadované kvality. Řízení bezpečnosti procesu, které je založeno na řízení rizik spojených s procesem, se osvědčilo v praxi a v mnoha případech jsou jeho principy zakotveny i v legislativě některých vyspělých zemí. Článek navrhuje metodiku aplikace procesu řízení bezpečnosti během provádění experiment a její hlavní část, tj. prototypový kontrolní seznam pro hodnocení dílčích rizik i integrálního rizika experimentu.

Klíčová slova: Experimenty; limity a podmínky; rizika; řízení bezpečnosti procesu; metodika; kontrolní seznam.

Abstract: Any experiment that solves practical problems is a process that takes place under certain conditions that significantly affect its results. The results of the experiment are further influenced by the quality of: inputs; technical and cybernetic equipment; management method; and the knowledge, experience and skills of the staff. Therefore, experiments supporting the industrial practice must be carried out using a methodology that ensures that the results are always of the required quality. Process safety management, which is based on the management of risks associated with the process, has proven itself in practice and in many cases its principles are enshrined in the legislation of some developed countries. The article proposes the methodology of application of the process safety management during the execution of experiment and its main part, i.e. a prototype checklist for the evaluation of partial risks and integral risks of the experiment.

Key words: Experiments; limits and conditions; risks; process safety management; methodology; checklist.

1. ÚVOD

Práce vychází z předpokladu, že inženýr řeší problémy praxe spojené s určitým objektem nebo zařízením za určitých specifických podmínek tak, aby řešení každého problému dosahovalo požadovaných výsledků po celou dobu životnosti objektu nebo zařízení a zároveň neohrožovalo objekt nebo zařízení nebo jeho okolí. Přitom využívá stávající znalosti a zkušenosti a zajišťuje, aby řízení zdrojů, sil a prostředků bylo hospodárné a podporovalo koexistenci základních systémů, které lidé potřebují pro svůj život, tj. koexistenci environmentálního, sociálního a technologického systému. K dosažení tohoto cíle využívá znalosti, dovednosti, zkušenosti a schopnosti vytvořit koncept řešení problémů a realizovat jej v daných podmínkách tak, aby objekt nebo jiný subjekt byl bezpečný, tj. spolehlivý a funkční po celou dobu své životnosti a za kritických podmínek neohrožoval sebe ani své okolí.

Podle poznatků a zkušeností shrnutých v [1] je pro řešení jakéhokoliv problému nejprve nutné problém poznat a porozumět mu, což lze provést pouze na základě:

- znalostí založených na sběru dat pozorováním a experimentováním a na formulování a testování hypotéz
- a aplikace správných metod, tj. metod, které jsou opakovatelné, transparentní, mají jasně definované veličiny, jednotky a terminologii.

Především je nutné: shrnout stávající znalosti, abychom věděli, co je již známo a zabránili "znovuobjevení"; a důsledně uplatňovat principy logického myšlení a kvalifikovaných metod, které jsou základem pro vytváření kvalitních inženýrských řešení. Poté je nutné provést:

- rekognoskaci prostředí, ve kterém je problém řešen, protože reálné prostředí není homogenní ani izotropní a ovlivňuje výsledky řešení problému,

- sběr dat pozorováním a monitorováním, protože prostředí se dynamicky vyvíjí, což podstatně ovlivňuje jeho vlastnosti, a tím i chování objektů, které jsou pro člověka životně důležité
- a experimenty, protože ty jsou základním kamenem empirického přístupu k získávání znalostí o okolním světě.

Experimenty se používají v přírodních, technických a společenských vědách od historických dob pro dva cíle: řešit praktické problémy; a potvrdit nebo vyvrátit výsledky vyplývající z teoretických předpokladů. Aby byly tyto cíle splněny, musí být výsledky experimentů kvalitní, tj.: musí: být správné; mít vztah k řešenému problému; a mít odhad náhodných a epistemických nejistot. To znamená, že k dosažení musí být použity kvalitní metody, které zajišťují stabilní a spolehlivé výsledky a mají dobrou rozlišovací schopnost [1]. Podle dokumentu [4] je nejvyšším faktorem kvality entity (tj. objektu, systému, procesu atd.) bezpečnost, a proto je na ni v současné době soustředěna pozornost [5,7-9,23-38].

Každý experiment je proces. Hodnocení mnoha výsledků experimentů, prováděných v univerzitních laboratořích, ukázalo velký rozptyl jejich výsledků při opakování experimentů, např. [2,3]. Vzhledem k tomu, že praxe takové výsledky nepotřebuje, je nutné použít metodiku experimentu, která zajistí kvalitní výsledky. V článku je popsáno, jak implementovat řízení bezpečnosti procesu (Process Safety Management) během provádění experimentů v technických oborech.

2. INŽENÝRSKÉ ŘEŠENÍ PROBLÉMŮ

Inženýrství je široká disciplína, která řeší problémy od jejich pochopení, přes návrh řešení až po realizaci v daných podmínkách. Je hnací silou lidského rozvoje, protože se také zabývá problémy, které je obtížné přesně vyřešit. K dosažení cíle využívá kreativitu lidských jedinců a přístupy označované jako dobrá praxe. V současné době je založeno na systémovém přístupu a využívá specifické disciplíny, které jsou charakterizovány v pracích [5-7] k zajištění současných cílů, kterými jsou bezpečný podnik, bezpečná komunita, bezpečný region apod. Podle prací [6,8,9] je inženýrská odbornost chápána jako výraz schopnosti řešit problém, tj.: aplikovat znalosti matematiky, vědy a techniky; navrhovat a realizovat experimenty; analyzovat a interpretovat data; navrhovat komponenty nebo celý systém podle požadavků a v rámci realistických omezení identifikovat, formulovat a řešit technické problémy; efektivně komunikovat; chápat dopady technických řešení v širším kontextu; používat nejmodernější nástroje a metody v inženýrské praxi; dodržovat profesní odpovědnost a etiku; a vést interdisciplinární tým.

Je třeba vnímat, že existuje rozdíl mezi akademiky a inženýry při řešení problémů. Akademici obvykle hledají obecná řešení nebo dílčí řešení v závislosti na kontextu spojeném s různými definicemi chování systémů a jejich okolí. Inženýr se zajímá o řešení úloh ve specifických podmínkách daných: charakteristikou konkrétního místa; právními předpisy, včetně norem a standardů; dostupnými zdroji, zejména finančními, technickými a lidskými (úroveň kvalifikace disponibilního personálu); strukturou dotyčných systémů, tj. jejich prvky, vazbami a toky mezi prvky, které tvoří aktiva systémů, která jsou důležitá pro řízení bezpečnosti systému.

Cílem inženýrských oborů je řešit problém za určitých daných podmínek tak, aby řešení bylo funkční a mělo požadovanou kvalitu v daných podmínkách po stanovenou dobu. Primární a naprosto základní úkol, který musí být vyřešen, aby bylo dosaženo kvalifikovaného řešení konkrétního problému, souvisí s následujícími aspekty, které je třeba vzít v úvahu při vytváření koncepce řešení konkrétního problému. Jedná se o určení: cílů a kontextu řešení, tj. určit, zda bude problém řešen jako jednooborový nebo multidisciplinární nebo multidisciplinární a průřezový; a na jaké odborné úrovni se to bude řešit, tj. jako specifické pro danou lokalitu, region nebo obecně.

Je skutečností, že cíle řešení jedné a téže úlohy mohou být nastaveny odlišně, např.:

- zvažuje se: jediné aktivum; dvě nebo více vzájemně se podporujících aktiv; a dva nebo více aktiv, z nichž některá se vzájemně podporují a některá jsou ve vzájemném konfliktu – např.: dobré životní prostředí podporuje kvalitu života a rozvoj člověka; naopak je známo mnoho konfliktů mezi životním prostředím a technologií, mezi člověkem a technologií (viz specifické oblasti studia, jako je člověk-stroj, člověk-počítač atd.)
- zvažují se různá kritická místa úloh podle znalostí a zkušeností.

Je to proto, že mnoho praktických úloh nemá obecné řešení vzhledem k tomu, že chování systémů a jejich okolí je proměnlivé, variabilita není lineární, dochází k náhlým změnám atd., což znamená, že neexistuje ani dostupné analytické řešení, ani jedno konkrétní univerzálně platné řešení [5,7-9,23,24]. Základní kroky řešení problému jsou následující: pochopení problému; poznání problému; analýza příčin problému; návrh a realizace opatření k odstranění příčin problému s ohledem na stanovený cíl; test účinnosti opatření; provádění opatření k odstranění příčin problému; zpráva o výsledcích řešení problému; a určení budoucích nápravných opatření a kroků v případě velkých odchylek od požadované situace. Pro praktické řešení problému je: nutné problému porozumět; nutné

určit, co a jak lze řešit a zda vynaložené náklady (čas, mzdy, příprava, administrativní změny) na řešení problému odpovídají možným úsporám nebo míře rizika; důležité stanovit cílový stav, protože na něm závisí kritéria nebo ukazatele monitoringu sledování kvality řešení problému.

Poznat problém znamená posoudit problém z různých perspektiv; například účinky změn provozních parametrů strojů, přípravků, vlivu lidského faktoru, vlhkosti, teploty atd. Ideální je sledování vlivů provádět systematicky, aby bylo možné dohledat vlivy náhodných a definovatelných příčin variability procesů. Specifičnost inženýrských metod spočívá v tom, že není možné oddělit charakteristiky jevů, před nimiž musí být daný objekt chráněn, vlastnosti materiálů, území, konstrukcí a zařízení, která tvoří objekt, provozní podmínky a limity, detekci narušení objektů při překročení stanovených limitů a nápravná opatření podporující bezpečnost objektu a jeho okolí. Cílem je však zajistit kvalitní řešení v daných podmínkách, a proto je nutné kombinovat přesné výsledky s výsledky správné inženýrské praxe, což znamená především použití pouze ověřených postupů a ověřených dat.

Proces je sled jevů nebo činností v prostoru a čase, ve kterém lze rozlišit vstupy a výstupy. Uvnitř každého procesu obvykle existuje mnoho paralelních, ale odlišných podprocesů. Každý podproces je spojen s konkrétním prvkem prostoru nebo skupinou prvků ve sledovaném prostoru. Procesní model je zobrazení určitého procesu zaměřeného na konkrétní cíl. Vzhledem k tomu, že cíle úloh v praxi nejsou stejné, existuje u jednoho objektu více procesních modelů pro jeden proces. Jedná se o popis procesu na úrovni typu (grafické znázornění obchodních procesů nebo pracovních postupů) [39]. V našem případě jsou cíle procesního modelu normativní, tj.: definuje se, jak by požadované procesy měly/mohly/mohly být prováděny; a stanovují se pravidla, směrnice a vzorce chování, jejichž dodržování vede k požadovanému výkonu procesu.

Procesní model podporovaný kvalitním IT je matematický nástroj, který umožňuje popsat současný stav, navrhnout nové nebo optimalizovat stávající procesy, odhalit zbytečné procesy nebo neefektivní procesy, modelovat a vyhodnocovat možný dopad změn před jejich implementací. Procesní modely jsou vysoce sofistikované nástroje z hlediska formalizované procesní analýzy. Je si však třeba uvědomit, že pouhá grafická prezentace může být zavádějící a může znamenat nepřijatelné zjednodušení posuzovaného systému, a proto je třeba vytvořit modely pro různé počáteční a okrajové podmínky, které odrážejí rozdíly v počátečních stavech a stavech okolní. V praxi existují různé procesní modely, např. pro technologie, procesy, organizaci nebo řízení [10,39]. Při výběru procesního modelu je třeba vzít v úvahu, že řešení každého problému a jeho úroveň závisí na podmínkách, ve kterých problém je řešen.

3. SHRNUTÍ POZNATKŮ O ŘÍZENÍ BEZPEČNOSTI PROCESU

Řízení bezpečnosti procesu (anglická zkratka *PSM*) má ve světě různé verze. Představuje složitý postup a vyžaduje vícerozměrný přístup, který spojuje technologie a jejich řízení [11]. Je propojeno s kulturou bezpečnosti a pro hodnocení bezpečnosti se často používá kontrolní seznam [12]. V Evropské unii je řízení bezpečnosti procesů obvykle spojeno se skladováním nebezpečných chemických látek a s manipulací s nimi [13] s cílem omezit rizika. Ve Spojeném království se nařízení o řízení ohrožení závažných havárií (COMAH) z roku 2015 vztahuje na PSM [14]. Nařízení se se zabývá specifickými normami pro všeobecný a stavební průmysl.

Řízení bezpečnosti procesů je složité a vyžaduje multidimenzionální přístup, který propojuje technologie a řízení řešení problémů. Každý program pro řízení bezpečnosti procesu má obsahovat 14 základních prvků [15-22]. Jejich stručný přehled je:

1. Informace o bezpečnosti procesu.
2. Analýza ohrožení a určení rizik procesu.
3. Provozní postupy.
4. Povolení k práci s ohněm nebo jinými zdroji vznícení.
5. Připravenost a odezva na nouzové situace.
6. Mechanická integrita zařízení.
7. Bezpečnostní přezkum před uvedením do provozu.
8. Řízené školení a výcvik ve všech bezpečnostních postupech.
9. Řízení změn – změnu provést až po přezkumu, že nedojde ke zvýšení rizik.
10. Vyšetřování incidentů s near-misses.

11. Řízení bezpečnosti dodavatelů a systémy řízení bezpečnosti procesů.
12. Audity dodržování předpisů s cílem zajistit soulad postupů a procesů.
13. Zapojení zaměstnanců do dodržování bezpečných postupů.
14. Důkladná dokumentace materiálů a procesů, a to i těch, které jsou obchodním tajemstvím, aby byla zajištěna bezpečnost a ochrana zdraví zaměstnanců.

Stojí za zmínku, že PSM se zaměřuje na události, které se v minulosti vyskytovaly velmi zřídka. Možná k nim vůbec nedošlo. Pokud k nim však dojde, jsou často katastrofální. I když může být složité a nákladné porozumět těmto událostem s nízkou pravděpodobností, výsledky, které vzniknou, když k nim dojde, jsou velmi vysoce závažné.

4. BEZPEČNOST A SPOLEHLIVOST VÝSLEDKŮ EXPERIMENTŮ V TECHNICKÝCH OBORECH

Každý experiment v sledované oblasti má určitý cíl, např. zjistit: popis chování nějakého objektu za stanovených podmínek; kritický / mezní stav, při kterém objekt mění vlastnosti; výrobní postup nebo techniku výroby skutečného produktu atd. V dalším textu se soustředíme na posledně zmíněný problém.

Praxe vyžaduje bezpečné, tedy spolehlivé a funkční výstupy. Proto při každém experimentu potřebujeme k vyřešení úkolu vysoce kvalitní faktická data. Abychom je získali měřením, potřebujeme kvalitní metodu měření veličin v průběhu experimentu, které jsou následně zpracovány vhodnou matematickou metodou. Aby byly získané údaje důvěryhodné, musí být proces měření: dostatečně flexibilní; transparentní; opakovatelný; přesné v tom smyslu, že zajišťuje stejné výsledky při opakování; a správné v tom smyslu, že se hodnotí oba typy nejistot, náhodná i znalostní .

Pro splnění výše uvedených požadavků je nutné mít bezpečný měřicí přístroj, bezpečný postup měření a provádět měření v bezpečně známém prostředí [1]. Měřicí přístroj se skládá z řady více či méně složitých prvků, součástí a systémů, které jsou uspořádány v určité struktuře, která musí být bezpečná. Koncem roku 1980 se hovořilo o spirále kvality při tvorbě technických systémů. Dnes používáme místo pojmu „kvalita“ pojem "bezpečnost" [4,11]. Bezpečnost každého technického zařízení je určena mnoha faktory. Ve fázi návrhu se jedná o stanovení správných specifikací, které musí respektovat vlastnosti místa, kde je technické zařízení umístěno. Dále se jedná o opatření zabudovaná do zařízení , která usnadní řízení bezpečnosti provozu za normálních, abnormálních a kritických podmínek různého druhu [23]. V souladu se současnými znalostmi by měla být zajištěna:

- aplikace stávajících norem a standardů, protože bez standardů a legislativy by odborníci i odborná veřejnost byli odsouzeni k opakování chyb minulosti
- a doplnění úprav na základě vyhodnocení možných rizik, která mají původ ve změnách v čase a stárnutí materiálů, které jsou příčinou znalostních nejistot [11,23].

Každé experimentální zařízení je jedinečným experimentálním zařízením. Proto je nutné předcházet problémům a defektům metodami řízení rizik. Z hlediska současných poznatků je třeba pro návrh a provoz experimentálních zařízení použit principy: návrh založený na rizicích (risk-based design) [23]; a provoz založený na rizicích (risk-based operation) [24].

5. POSTUP PRO SESTAVENÍ METODIKY PRO IMPLEMENTACI PSM DO REALIZACE EXPERIMENTŮ

Metodika je chápana jako ucelený soubor poznatků a principů poznání pro řešení problémů v určité oblasti . Velkého významu nabývá u málo strukturovaných úloh, u kterých umožňuje pružně řešit různé úrovně problémů. Zcela obecně platí, že když chceme vyřešit určitý netriviální problém, musíme provést jistá opatření a činnosti v duševní i praktické oblasti a umět správně rozhodovat při výběru možných alternativ řešení, a k tomu kromě vlastních znalostí a schopností potřebujeme fakta, tj. relevantní data a relevantní metody, kterými zpracujeme podklady, na jejichž základě můžeme správně rozhodovat. Datové soubory pro daný účel musí být sestaveny tak, aby umožnily získat žádoucí výsledky, tj. musí mít oceněny nejistoty a neurčitosti v místě a čase. Jinak analýzy, hodnocení či výpočty nebudou ani správné, ani konzistentní a rozhodování budou prováděna formou případ od případu bez jednotného metodického rámce, což odporuje odborným postupům a koncepčním přístupům vyspělých zemí. Aplikace PSM je způsob, jak zajistit výše uvedené požadavky.

V souladu s veřejným zájmem a vývojem lidské společnosti je vyžadováno bezpečné provádění experimentu. To vyžaduje aplikovat bezpečné provozní postupy. Postupy musí zahrnovat provozní limity a kroky potřebné k

nápravě nebo zabránění odchylkám od mezních hodnot. V souladu se znalostmi a zkušenostmi shrnutými v [24] musí být experimentátor schopen rozpoznat odchylku, která ovlivňuje bezpečnost, a vědět, co dělat, aby udržel kontrolu nad průběhem experimentu. Musí znát důsledky odchylek, jaká opatření je třeba podniknout a jak používat vhodné bezpečnostní vybavení. Provozní postupy pro experiment musí zohledňovat otázky bezpečnosti a ochrany zdraví.

Vzhledem k tomu, že každý experiment je proces, tak v souladu s cíli PSM v případě experimentu je vyžadováno trvalé úsilí zacílené na předcházení katastrofickým haváriím a na dosažení bezpečných výsledků. Analogicky k postupům popsaným v [15-22] je třeba aplikovat principy, metody a postupy řízení zacílené na prevenci a řízení rizik během přípravy, návrhu, průběhu a hodnocení výsledků experimentu. K tomu je potřeba mít úplné a přesné informace o: experimentální technologii; experimentálním zařízení; fyzikálních vlastnostech použitých materiálů; vnějších a vnitřních podmínkách, ve kterých se experiment provádí; a o nebezpečných charakteristikách jevů, ke kterým může docházet během experimentu. Proto musí být tyto faktory pro bezpečný průběh experimentu přezkoumány. Při auditu je třeba vzít v úvahu: provozní limity přístrojů a jejich propojení; důsledky odchýlení se od těchto mezních hodnot; a opatření pro zotavení z odchylek. Postupy musí být zaměřeny na běžné, abnormální a nouzové podmínky, které mohou nastat během experimentu, aby se připravila reakce experimentátorů na jakoukoli událost, která může rozumně nastat.

Jelikož podmínky, za kterých je experiment prováděn, ovlivňují výsledky experimentu, je při přípravě metodiky pro praxi důležité nejen pracovní postup, ale také definice intervalu podmínek, za kterých mají výsledky experimentu požadovanou kvalitu. Proto se musíme zabývat riziky spojenými s experimentem, tj. s: vlastnostmi místního prostředí, ve kterém se experiment provádí; zařízením používaným pro experiment; materiály použitými při experimentu; přípravou a výstavbou zařízení pro experiment; inspekcí zařízení pro experiment; pokyny pro provádění experimentu; pokyny pro zdraví a bezpečnost experimentátora během přípravy a provádění experimentu; reakcí na incidenty v průběhu experimentu; dokumentací údajů z experimentu; tvorbou a zpracováním datového souboru z experimentu; vyhodnocením a posouzením dat z experimentu a posouzením jejich přijatelnosti; dokumentací výsledků experimentu; a vytvořením doporučení pro praxi (to také znamená stanovit limity a podmínky provádění experimentu, které zaručují požadovanou kvalitu výsledků). Proto, aby bylo dosaženo vysoce kvalitních výsledků, musí být provedeno řízení rizik ve prospěch bezpečnosti. V souladu s [23,24] to znamená používat: zásady návrhu založeného na rizicích a provozu založeného na rizicích; a mít plán řízení rizik, tj. soubor protiopatření pro zmírnění rizika v případě výskytu problémů při experimentu.

Analogicky k postupům popsaným v [15-24] je třeba vzít v úvahu výše uvedených 14 hlavních prvků a adaptovat je na experiment. Tyto prvky by měly být dobře známy bezpečnostnímu manažerovi experimentu a ostatní pracující v místnosti by si jich měli být také vědomi. Jedná se o tyto prvky: bezpečnostní informace spojené s experimentem; audit vnějších podmínek, ve kterých je experiment prováděn; analýza rizik experimentu; operační postupy experimentu; školení experimentátora; spolupráce experimentátora se spolupracovníky; mechanická integrita experimentálních zařízení; vysoce nebezpečné práce během provádění experimentu; řízení změn při provádění experimentu v případě problémů; vyšetřování incidentů spojených s experimentem; audity souladu s předpisy; účast jiných osob na provádění experimentu; přezkum bezpečnosti experimentu před spuštěním; a havarijní plánování a reakce na havárie realizovaná plánem řízení rizik [23,24]. Obdobně jako [15-24] je kontrolní seznam vhodným nástrojem pro kontrolu plnění těchto požadavků.

V souladu s postupem [6,26] je třeba při sestavování kontrolních seznamů dodržet následující kroky: specifikovat položky, které by měly být sledovány; vytvořit pořadí položek na základě jejich závažnosti pro sledovanou oblast; identifikovat kritické položky, které jsou zdrojem rizika; sestavit otázky kontrolního seznamu; a určit, jak má být kontrolní seznam posuzován.

6. METODIKA APLIKACE ŘÍZENÍ BEZPEČNOSTI PROCESU BĚHEM EXPERIMENTU

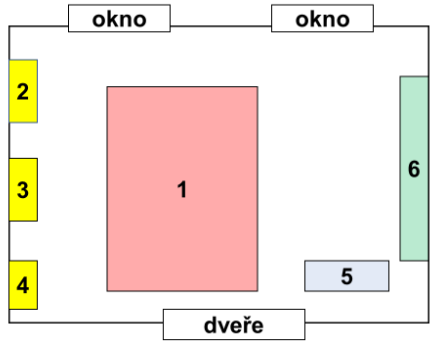
Na základě výše uvedených skutečností navrhujeme metodiku pro provádění řízení bezpečnosti procesu během experimentů takto:

- shromáždit dostupné informace související s experimentem,
- zkonstruovat procesní model experimentu,
- shromáždit: vhodné nástroje a materiály; normy a postupy pro navrhování, výrobu a provoz experimentálních přístrojů,
- vytvořit pravidla OSHA pro konstrukci experimentálního zařízení a průběh experimentu,
- ověřit znalosti, dovednosti a zručnost experimentátorů v oblasti navrhování, konstrukce a provozu,
- provést sestavení experimentálního zařízení,

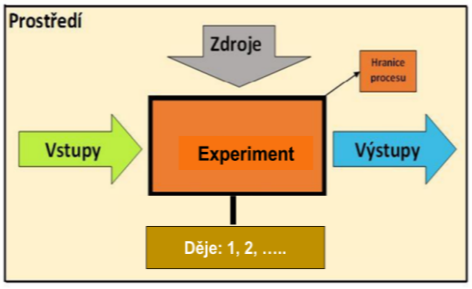
- provést bezpečnostní audit mechanické integrity experimentálního zařízení, tj. vzít v úvahu nejen bezpečnost komponentů, ale i bezpečnost jejich propojení (protože propojení jsou velmi často kritickými částmi zařízení [24]),
- vyhodnotit vnější ohrožení v místnosti, ve které se experiment provede,
- vyhodnotit vnitřní rizika spojená s experimentálním zařízením a jevy, které se mohou vyskytnout během provádění experimentu,
- vytvořit zásady kultury bezpečnosti [24] pro provádění experimentu, které zahrnují plán řízení rizik,
- zahájit experiment a realizovat řízení rizik ve prospěch bezpečnosti během provádění experimentu,
- dokumentovat průběh experimentu,
- po ukončení experimentu shromáždit data a provést zpracování dat získaných z údajů naměřených při experimentu.

Aby všechny uvedené požadavky byly snadno přístupné experimentátorům, tak je vhodné konvertovat je do kontrolního seznamu.

Příklad schématu podmínek prostředí místnosti, ve které se experiment provádí, je znázorněn na obrázku 1. Příklad procesního modelu experimentu je znázorněn na obrázku 2. Prototypový kontrolní seznam pro posouzení, zda řízení bezpečnosti procesů během experimentu má dostatečnou kvalitu, je uveden v tabulce 1; jedná se o kontrolní seznam pro hodnocení rizik. V reálném případě musí uvedené dokumenty odpovídat skutečným podmínkám.



Obr. 1. Dispozice místnosti s experimentálním vybavením. 1 – experimentální zařízení; 2 – zdroj plynu; 3 – zdroj vody; 4 – elektrický rozvaděč; 5 – velín, tj. řídící stanice pro experiment (řízení experiment, regulace teploty, vlhkosti a větrání v místnosti); 6 – zabezpečovací zařízení (požární signalizace, hasicí zařízení, osobní ochranné prostředky, provozní předpisy, bezpečnostní listy pro použité technické plyny).



Obr.2. Procesní model experimentu.

Tabulka 1. Prototypový kontrolní seznam pro posouzení rizik, které ovlivňují průběh a výsledek experimentu; A - ano, N - ne.

Otázka	A	N
Příprava experimentu		
Jsou shromážděny všechny informace spojené s experimentem?		
Je konstruován procesní model pro experiment?		
Je zajištěna spolehlivá funkce klimatizace (teplota, vlhkost, větrání) v místnosti?		
Je stav rozvaděče elektřiny v souladu s normami pro bezpečný provoz?		
Je stav zdroje plynu v souladu s normami pro bezpečný provoz?		

Jsou napájecí kabely v souladu s normami pro bezpečný provoz?		
Je potrubí pro rozvod technických plynů v souladu s normami pro bezpečný provoz?		
Jsou vodovodní potrubí v souladu s bezpečnými provozními normami?		
Je elektrická požární signalizace v provozu?		
Jsou v hale funkční hasicí systémy (i pro případ požáru z elektroinstalace)?		
Splňuje velín normy pro bezpečný provoz?		
Má řídicí systém velínu integrovaný systém řízení bezpečnosti v souladu s normami pro bezpečný provoz?		
Obsahuje systém řízení bezpečnosti velínu postupy pro bezpečný provoz měřicího zařízení nejen za běžných (projektových) podmínek, ale také za abnormálních a kritických podmínek?		
Jsou vyhodnocena vnitřní rizika spojená s experimentálním zařízením a jevy, které se vyskytují během provádění experimentu?		
Je vypracován plán reakce na možné vnitřní a vnější nežádoucí jevy?		
Má personál místnosti znalosti a kompetence v souladu s normami pro bezpečný provoz velínu a experimentálního vybavení?		
Dodržuje personál místnosti postupy pro bezpečný provoz v souladu s provozním řádem místnosti a experimentálního zařízením pro bezpečný provoz?		
Jsou shromážděny: vhodné nástroje a materiály; normy a postupy pro navrhování, konstrukci a provoz experimentálního přístrojového vybavení?		
Jsou stanoveny zásady kultury bezpečnosti pro provádění experimentu, které zahrnují plán řízení rizik?		
Je zpracován program experimentu pro velín?		
.....jiné položky specifické pro web a experiment		
Komponenty experimentálního zařízení (s – počet komponent experimentálního zařízení)		
Jsou k dispozici všechny komponenty experimentálního zařízení?		
Je komponenta A1 v souladu s normami pro bezpečný provoz?		
Je komponenta A2 v souladu s normami pro bezpečný provoz?		
.....		
Je komponenta As v souladu s normami pro bezpečný provoz?		
Postup projektování a výstavby a ověřování kvality měřicích zařízení (m – počet procesů pro spojování součástí)		
Je při konstrukci měřicího zařízení použita vhodná zásada inherentní bezpečnosti?		
Jsou při návrhu použity systémy pasivní bezpečnosti?		
Jsou při návrhu použity systémy aktivní bezpečnosti?		
Jsou propojení komponenty B1 s ostatními komponentami v souladu s normami pro bezpečný provoz?		
Jsou propojení komponenty B2 s ostatními komponentami v souladu s normami pro bezpečný provoz?		
.....		
Jsou propojení komponenty Bm s ostatními komponentami v souladu s normami pro bezpečný provoz?		
Je konstrukce experimentálního zařízení prováděna v souladu s normami pro bezpečný provoz?		
Je program experimentu vložen do velínu?		
Audit		
Je správný program experimentu vložen do velínu?		
Jsou komponenty a jejich propojení provedeny podle norem?		
Je proveden bezpečnostní audit mechanické integrity experimentálního zařízení, tj. Je brána v úvahu nejen bezpečnost komponentů, ale i jejich propojení (propojení jsou velmi často kritickou součástí zařízení)?		
Bylo ověřeno, že komponenty a celá konstrukce zařízení jsou dostatečně robustní, aby odolaly superkritickým podmínkám způsobeným výbuchem?		
Bylo ověřeno, že komponenty a celá konstrukce zařízení jsou dostatečně robustní, aby odolaly superkritickým podmínkám způsobeným požárem?		
Bylo ověřeno, že komponenty a celá konstrukce zařízení jsou dostatečně robustní, aby odolaly superkritickým podmínkám způsobeným úderem?		

Bylo ověřeno, že komponenty a celá konstrukce zařízení jsou dostatečně robustní, aby odolaly superkritickým podmínkám způsobeným vysokou teplotou?		
Bylo ověřeno, že komponenty a celá konstrukce zařízení jsou dostatečně robustní, aby odolaly nadkritickým podmínkám způsobeným výpadkem elektrického proudu?		
Bylo ověřeno, že komponenty a celá konstrukce zařízení jsou dostatečně robustní, aby odolaly superkritickým podmínkám způsobeným vodou?		
.....jiné položky specifické pro web a experiment		
Experiment		
Je velín zapnut?		
Jsou všechny měřicí přístroje zapnuté?		
Jsou zapnuty všechny potřebné zdroje (elektřina, plyn, voda)?		
Jsou všechna ochranná zařízení pro BOZP zapnutá?		
Je správný vzorek ze správného materiálu vložen do experimentálního zařízení?		
Provádí se sledování všech důležitých fází (etap procesu) experimentu?		
Je záznamové zařízení v provozu?		
Je výsledný vzorek vyjmut z experimentálního zařízení po ukončení experimentu?		
Jsou použité zdroje po skončení experimentu vypnuty?		
Jsou měřicí přístroje po skončení experimentu vypnuty?		
Jsou všechna ochranná zařízení pro BOZP po skončení experimentu vypnuta?		
Je řídicí stanice po skončení experimentu vypnutá?		
Je místnost po skončení experimentu vyčištěna a zamčena?		
Zpracování dat z experimentu		
Jsou údaje získané z experimentu převedeny na data ve formátu, který umožňuje další zpracování?		
Posuzuje se přesnost a správnost dat?		
Je zpracován protokol o experimentu a jeho výsledcích?		
Je sepsána zpráva pro potřeby dalších experimentů a praxe?		

Na základě dosavadních znalostí a zkušeností shromážděných např. V [5,23,24] ovlivňují chyby v položkách uvedených v kontrolním seznamu a zejména jejich kombinace kvalitu výsledků experimentu. Pro zajištění vysoké kvality experimentu musí být posouzena jak rizika spojená s jednotlivými položkami, které jsou uvedeny v kontrolním seznamu, tak integrální riziko [5,23,24]. Hodnocení dílčích rizik se provádí tak, aby posuzované otázce byla přiřazena hodnota 0 v případě záporné odpovědi nebo 1 v případě kladné odpovědi. Výjimečně lze hodnotu mezi 0 a 1 přiřadit i v případě částečně splněných podmínek [5]. Nejprve je třeba stanovit počet rizikových položek v daném případě pro posouzení vybrané části nebo všech rizik, tj. $\boldsymbol{N}$ je celkový součet otázek, $\boldsymbol{n}$ je počet odpovědí NE. Úroveň rizika v posuzovaném případě $\boldsymbol{r}$ se rovná $\boldsymbol{n}$/N jako procentuální hodnota, kde $\boldsymbol{N}$ je 100 %. Jeho hodnocení se provádí podle stupnice používané v technických normách od roku 1980, tabulka 2 [24].

Tabulka 2. Hodnotová stupnice pro stanovení úrovně rizika $\boldsymbol{r = n/N}$.

Míra rizika	**Hodnoty *r* v %**
Extrémně vysoká – 5	Více než 95 %
Velmi vysoká – 4	70 - 95 %
Vysoká – 3	45 - 70 %
Střední – 2	25 – 45 %
Nízká – 1	5 – 25 %
Zanedbatelné – 0	Nižší než 5 %

Na základě poznatků shrnutých v [23,24] platí, že pokud je riziko:

- přijatelné, tak není třeba přijímat další opatření, protože úroveň bezpečnosti (kvalita experimentu) je na přijatelné úrovni. Pokud je toto potvrzeno dostatečným počtem opakovaných experimentů, je metodika experimentu vhodná pro praxi,
- podmíněně přijatelné, je třeba provést technická opatření (parametry prostředí, materiál, technický princip, postup výstavby, bariéry proti vlivu kritických jevů, zálohy komponent apod.), pokud je to technicky a

finančně možné, a tím snížit míru obou rizik, dílčího i integrálního, a pokud to není technicky a finančně možné, umožnit provedení odezvy prostřednictvím dodatečného technického vybavení a organizačních opatření, která umožní zlepšit výkon měřicího zařízení a zajistit přijatelnou úroveň bezpečnosti zařízení. Pro potřeby praxe je nutné opakovanými experimenty nalézt takové podmínky a limity pro provádění experimentu, ve kterých je vždy přijatelná míra rizika, tj. úroveň bezpečnosti (kvality) experimentu odpovídá potřebám praxe. Pouze pokud je to potvrzeno dostatečným počtem opakovaných experimentů, je upravená metodika experimentu vhodná pro praxi (tj. v praxi musí být dodržen soulad limit a podmínek určených experimenty, aby požadovaná kvalita výstupu byla dosažena),

- nepřijatelné, je nutné zavést základní technická opatření v oblasti materiálu, technických zásad, konstrukčních postupů, bariér proti vlivu kritických jevů, záloh komponent) s cílem snížit míru všech rizik: dílčích i integrovaného. Pro praxi je metodika v předložené formě nepřijatelná a musí být provedena zásadní změna experimentálního postupu.

Publikované články [41,42] ukazují úspěšnou aplikaci této metodiky.

7. ZÁVĚR

Předložená práce se zabývá experimenty v laboratořích, které řeší praktické problémy. Současné poznatky a zkušenosti ukazují, že výsledky každého experimentu jsou ovlivněny jak vnějšími, tak vnitřními podmínkami, za kterých je experiment prováděn. Velkou roli dále hraje kvalita: vstupů, technického a kybernetického vybavení; způsobu řízení; znalostí, zkušeností a dovedností personálu. Proto musí být experimenty, jejichž výsledkem má být základ provozního předpisu pro průmyslovou praxi, prováděny za použití metodiky, která zajišťuje dobrou kvalitu výsledků. Řízení bezpečnosti procesu, které je založeno na řízení rizik spojených s procesem, se osvědčilo v praxi. Proto výše předkládáme postup, jak aplikovat jeho principy při provádění experimentů, jejichž cílem je připravit výrobní postup pro průmysl.

Z technických a ekonomických důvodů potřebuje průmyslová praxe pouze spolehlivé postupy s vysokou kvalitou, tj. bezpečné postupy. Článek ukazuje metodiku řízení bezpečnosti procesu při provádění experimentů a její hlavní část, tj. prototypový kontrolní seznam pro hodnocení dílčích rizik i integrálního rizika experimentu. Pro potřeby průmyslové praxe je nutné opakovanými experimenty nalézt takové podmínky a limity pro provádění experimentu, při kterých je míra rizika vždy přijatelná, tj. úroveň bezpečnosti (kvalita experimentu) odpovídá potřebám praxe.

LITERATURA

[1] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Data a metodika jejich zpracování pro potřeby inženýrských disciplín.* ISBN 978-80-01-05792-6. Praha: ČVUT 2015, 186 p.

[2] CIHLÁŘ, M., MAREČEK, M. *Vady MSL smyčky*. Řež: Centrum výzkumu Řež – Archiv 2020.

[3] TLASKAL, F. Vliv předúpravy povrchu pro technologie práškového lakování. *Bakalářská práce*. Fakulta strojního inženýrství. Praha: CVUT 2022, 99 p.

[4] EU. *Maastricht Treaty*. C 191, 29.7.pp.1–112. Maastricht: EU 1992

[5] PROCHÁZKOVÁ, D. *Analýza, řízení a vypořádání rizik spojených s technickými díly*. Praha: ČVUT 2018, 222 p. Doi:10.14311%2FBK.9788001064801

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

[7] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace.* ISBN 978-80-01-04844-3. Praha: ČVUT 2011, 483 p.

[8] ROLAND, H. E., MORIARITY, B. *System Safety Engineering and Management.* ISBN 0-471-6186-0. J. Willey 1990, 321 p.

[9] ANDERSON, R. *Security Engineering- A Guide to Building Dependable Distributed Systems.* ISBN 978-0-470-068552-6. J. Willey 2008, 1001 p.

[10] COLETTE R. *A Multi-Model View of Process Modelling. Requirements Engineering*. 4 (1994), 4.

[11] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení.* ISBN 978-80-01-06180-0. Praha: ČVUT 2017, 364 p. Doi:10.14311%2FBK.9788001061824

[12] US DOE (1996). *DOE -HDBK-110196. Handbook. No 20585*- Tennessse: US DOE, 180 p.

[13] EU (2012). *Seveso III Directive (2012/18/EU).* Brussels: EU 2012.

[14] www.hse.gov.uk

[15] www.osha.gov

[16] CMA. *Process Safety Management (Control of Acute Hazards).* Washington, DC: CMA 1985.

[17] AIChE. *Plant Guidelines for Technical Management of Chemical Process Safety*. New York: AIChE 1992.
[18] AIChE. *Guidelines for Implementing Process Safety Management Systems.* New York: AIChE 1994.
[19] AIChE. *Guideline for Engineering Design for Process Safety.* New York: AIChE 1993.
[20] AIChE. *Guidelines for Preventing Human' Error in Process Safety.* New York: AIChE 1994.
[21] AIChE. *Guidelines for Auditing Process Safety Management Systems.* New York: AIChE 1993.
[22] AIChE. *Guidelines for Process Safety Management Documentation.* AIChE, New York1995.
[23] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. Doi:10.14311%2FBK.9788001066096
[24] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Řízení rizik procesů spojených s provozem technického díla během jeho životnost.* ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. Doi:10.14311%2FBK.9788001066751
[25] BRIŠ, R., GUEDES SOARES, C. & MARTORELL, S., eds. *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362 p.
[26] ALE, B., PAPAZOGLOU, I., ZIO, E., eds. *Reliability, Risk and Safety*. ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448 p.
[27] BÉRENGUER, C., GRALL, A., GUEDES SOARES, C., eds. *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035 p.
[28] IAPSAM, eds. *Probabilistic Safety Assessment and Management Conference. International. 11th 2012. (and Annual European Safety and Reliability Conference*). ISBN: 978-1-62276-436-5. Helsinki: IPSAM & ESRA 2012, 6889 p.
[29] STEENBERGEN, R., VAN GELDER, P., MIRAGLIA, S., TON VROUWENVELDER, A., eds. *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387 p.
[30] NOWAKOWSKI, T., MLYŇCZAK, M., JODEJKO-PIETRUCZUK, A., WERBIŇSKA-WOJ-CIECHOWSKA, S., eds . *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453 p.
[31] PODOFILLINI, L., SUDRET, B., STOJADINOVIC, B., ZIO, E., KRÖGER, W., eds. *Safety and Reliability of Complex Engineered Systems.* ISBN 978-1-138-02879-1. London: CRC Press 2015, 4560 p.
[32] WALLS, L., REVIE, M., BEDFORD, T., eds. *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL* ISBN 978-1-315-37498-7. London: CRC Press 2016, 2942 p.
[33] CEPIN, M., BRIS, R., eds. *Safety and Reliability – Theory and Applications*. ISBN: 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.
[34] 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.
[35] BEER, M., ZIO, E., eds. *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*. ISBN 978-981-11-2724-3. Singapore: ESRA, Research Publishing 2019, 4315 p., e:enquiries @rps online.com.sg
[36] BARALDI, P., DI MAIO, F., ZIO, E., eds. Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15). ISBN 978 -981-14-8593-0. Singapore: ESRA, Research Publishing 2020, 5067 p., enquiries@rps online.com.sg
[37] CASTANIER, B., CEPIN, M., BIGAUD, D., BERENGUER, C., eds. *Proceedings of the 31st European Safety and Reliability Conference* . ISBN 978-981-18-2016-8. Singapore: ESRA, Research Publishing 2021, 3473 p., enquiries@rpsonline.com.sg
[38] LEVA, M.C., PATELLI, E., PODOFILLINI, L., WILSON, S., eds. *Proceedings of the 32nd European Safety And Reliability Conference (ESREL 2022)*. ISBN 978-981-18-5183-4. Singapore: ESRA, Research Pu-blishing 2022, 3413 p., enquiries@rpsonline.com.sg
[39] KROGSTIE, J., SINDRE, G., JORGENSEN, H. Process Models Representing Knowledge for Action: a Revised Quality Framework. *European Journal of Information Systems*. 15 (2006), 1, pp 91-102. Doi:10.1057/palgrave.ejis.3000598. S2CID 16574846
[40] PROCHÁZKOVÁ, D., ŠESTÁK, B. *Kontrolní seznamy. Nástroj rizikového inženýrství*. ISBN 80-7251-225-0, Praha: PA ČR 2006, 319 p.
[41] KUCHAR, J., KREIBICH, V., PROCHAZKOVA, D., BACHUROVA, N. Mitigating the Risks of Energetic Facilities by Cleaning Internal Surfaces. In: *Proceedinggs the 32 ESREL Conference*. Singapore: Research Publishing(s) Pte Ltd. editorial@rpsonline.com.sg 2023. ISBN 978-981-18-8071-1, pp.113-1121, Doi:10.3850/978-981-18-8071-1_driver

[42] KUCHAR, J., KREIBICH, V., PROCHAZKOVA, D., BACHUROVA, TLASKAL, F. Mitigation of Risks of Corrosion and Delamination by Surface Pre-Treatment. In: *Proceedinggs the 32 ESREL Conference.* Singapore: Research Publishing(s) Pte Ltd. editorial@rpsonline.com.sg 2023. ISBN 978-981-18-8071-1, pp. 355-363, Doi:10.3850/978-981-18-8071-1_driver

VYBRANÉ KONTROLNÍ SEZNAMY PRO ŘÍZENÍ RIZIK STROJNÍCH A ELEKTRICKÝCH ZAŘÍZENÍ

SELECTED CHECKLISTS FOR RISK MANAGEMENT OF MACHINERY AND ELECTRICAL EQUIPMENTS

Dana Procházková

ČVUT v Praze, fakulta strojní, Technická 4, 166 07 Praha, danuse.prochazkova@fs.cvut.cz

Abstrakt: Řízení rizik je základem inženýrství, které je zacílené na bezpečnost (i spolehlivost, zabezpečení, výkonnost) entit. Pro předmětné řízení lze použít řadu nástrojů, které závisí na složitosti struktury entity a cíli řízení. Nejjednodušší a často používaný nástroj pro řízení rizik je kontrolní seznam spojený se stupnicí jeho hodnocení, která dobře vystihuje cíl řízení. V článku jsou ukázány příklady typů kontrolních seznamů pro různé cíle řízení rizik u strojních a elektrických zařízení a stupnice pro stanovení míry rizika.

Klíčová slova: Riziko; bezpečnost; řízení rizika; kontrolní seznam; stupnice pro hodnocení rizika.

Abstract: Risk management is the ground of engineering that is aimed at safety (also reliability, security, performance) of entities. A number of tools can be used for the management in question, depending on the complexity of the entity structure and the objective of the management. The simplest and frequently used risk management tool is a checklist linked to a rating scale that reflects the management objective well. The paper shows examples of checklists types for different risk management objectives for machinery and electrical equipment and the scale for determining the risk rate.

Key words: Risk; safety; risk management; checklist; risk rating scale.

1. ÚVOD

Pro existenci a rozvoj lidí a lidské společnosti je nutné zajistit podmínky pro život. Svět se dynamicky vyvíjí a to ovlivňuje jak lidi a lidskou společnost, tak přírodu a všechny entity, které lidstvo vytvořilo pro zvýšení kvality svého života. Proto od počátku civilizace inženýrství a jeho disciplíny aplikují technické a vědecké poznatky, využívají zákony přírody i lidské prostředky k vytváření nových entit, tj. materiálů, strojů, zařízení, systémů a procesů, které usnadňují a zlepšují život lidí.

Inženýrství zahrnuje mnoho specializací, které se věnují problémům spojeným s vývojem a užíváním určitého druhu výrobku nebo objektu, s využíváním určité technologie pro zajištění základních služeb podporujících bezpečí a rozvoj lidské společnosti. Je širokou disciplínou, která řeší problémy od jejich pochopení, přes návrh řešení až po realizaci v daných podmínkách. Inženýrské disciplíny jsou hnací silou lidského vývoje, protože se zabývají i problémy, které je obtížné přesně řešit a k dosažení cíle používají kreativitu lidských jedinců a přístupy označované jako dobrá praxe. V současné době se používá inženýrství zacílené na bezpečnost, spolehlivost, zabezpečení a výkonnost [1].

V článku sledujeme pojetí bezpečnosti, které je ve vyspělých zemích prosazované od 90. let. Je kodifikované deklarací a smlouvou OSN v r. 1994 [2] a v Evropské unii je kodifikované Maastrichtskou smlouvou z roku 1992 [3]. Dle něho je:

- riziko mírou ztrát a škod na objektu, zařízení, území, procesu, technickém zařízení i technickém díle, které může způsobit / způsobí škodlivý jev z pohledu lidské společnosti,
- bezpečnost 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; je základním znakem kvality sledované entity.

Inženýrství zacílené na bezpečnost představuje soubor znalostí a dovedností, které řeší určitý problém, tj. uspokojují požadavky, kterými jsou užitečnost, disponibilita a bezpečnost, a to na základě principů systémových disciplín. Jeho základním nástrojem je řízení rizik [4].

Dle současného poznání je riziko inherentní vlastností současného světa a je proměnné v čase i prostoru [1,4]. Proto bezpečnost každé entity lze zajistit jen permanentním řízením rizik [1,4]. Protože riziko lze zmírnit nejen technickými, ale i organizačními opatřeními, tak doplňkovou veličinou k bezpečnosti je kritičnost.

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, státu [6]. Označuje položku potřebnou, ale zároveň velmi zranitelnou. 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, ani s pojmem krizový, což politici a další často používají.

V Evropské unii se používá řízení typu „Total Quality Management (TQM)“ od r.1989 [7]. Technická zařízení i objekty jsou považovány za systémy systémů – SoS (otevřený soubor otevřených systémů) [3,4] a při jejich charakteristice se používají specifické pojmy: koherentnost; kompatibilita; operabilita; interoperabilita; integrita bezpečnosti; provozní spolehlivost; odolnost; atd. [3,4,8].

2. BEZPEČNOST STROJNÍCH A ELEKTRICKÝCH ZAŘÍZENÍ

V práci dále sledujeme složitá strojní a technická zařízení, která zkráceně označujeme entity a která mají strukturu popsanou modelem systém systémů (SoS), tj. otevřený soubor otevřených a vzájemně provázaných systémů, přičemž povaha systému systémů je socio-kyber-fyzická (technická) [1]. Znalosti o entitách a jejich příslušenství jsou sestaveny z poznatků uvedených v pracích [1,8-32]. Lze je shrnout následovně:

1. Životní cyklus každé sledované entity zahrnuje fáze, kterými jsou návrh, projekt, umístění, výstavba, konstrukce a uvedení do provozu, provoz a ukončení provozu. Jde o proces složitý a velmi rozmanitý, protože jde o propojení mnoha různých činností, které jsou místně specifické, jelikož závisí také na parametrech prostředí, do kterého je daná entita vložena. Proto je potřeba ve všech uvedených fázích pracovat s riziky, jejichž realizace by mohla významně narušit podmínky nutné pro život lidí, a lidská společnost by v daném případě nemusela mít schopnost vzniklá rizika vypořádat.
2. Z hlediska výběru, návrhu a realizace optimální verze entity v každém konkrétním případě hraje roli:
   - dosažená úroveň bezpečí entity a jejího okolí,
   - technická proveditelnost opatření pro zajištění bezpečné entity s tím, že se bere do úvahy vhodnost opatření pro daný systém, tj. entitu a její okolí,
   - materiálová náročnost i energetická náročnost entity,
   - rychlost realizace entity,
   - ovladatelnost zařízení a procesů entity,
   - životnost entity,
   - nároky provozu entity na kvalifikovaný personál,
   - nároky provozu entity na údržbu,
   - nároky entity na dopravu a informační zajištění, tj. komunikační sítě,
   - nároky entity na finance při výstavbě a provozu,
   - nároky entity na zajištění celkové bezpečnosti včetně technického a kybernetického zabezpečení,
   - nároky na personál entity z hlediska odpovědnosti za bezpečnost,
   - nároky entity na řízení / organizaci,
   - nároky entity na nouzové služby při provozu,
   - nároky veřejné správy na řízení bezpečnosti v okolí entity.
3. Bezpečnost, zabezpečení, spolehlivost a výkonnost entity jsou důležité vlastnosti v praxi. Všechny se zajišťují řízením rizik, ale výsledky řízení rizik v jednotlivých případech nejsou stejné, protože jejich cíle nejsou stejné. Integrální (celková) bezpečnost entity chápaná z pohledu bezpečnosti a rozvoje lidské společnosti je vlastnost, která zahrnuje ostatní vlastnosti, protože sleduje i rizika spojená s žádoucími i nežádoucími propojeními v dílčích systémech vyvolaných dynamickým chováním entity a jejího okolí.
4. Základní požadavky na bezpečnost provozu entity jsou:
   - materiály, ze kterých jsou entita a její příslušenství vyrobeny musí respektovat vlastnosti způsobu provozu a prostředí, ve kterém se plánuje provoz,

- projekt a konstrukce entity a jejího příslušenství musí respektovat způsob provozu a prostředí, ve kterém se plánuje provoz,
- projekt a konstrukce entity musí respektovat způsob provozu a prostředí, ve kterém se plánuje provoz,
- entita a její příslušenství musí obsahovat principy inherentní bezpečnosti a spolehlivé zálohování kritických položek (např. odlehčovací ventily, senzory sledující hodnoty důležitých parametrů),
- projekt a konstrukce založení entity musí respektovat způsob provozu a prostředí, ve kterém se plánuje provoz,
- při provozu entity musí být splněny požadavky na bezpečnost v oblastech: technické; organizační; právní; finanční; i ochrany osob a životního prostředí,
- při údržbě entity musí být splněny požadavky na bezpečnost v oblastech: technické; organizační; právní; finanční; i ochrany osob a životního prostředí,
- dokumentace, která:
  - obsahuje: mezní limity pro provoz entity, schémata a návody, protokoly o zkouškách, zdroje rizik, výsledky analýzy rizik, podmínky, při kterých entita nesmí být používána, upozornění na možná nebezpečí, požadavky na vzdělání obsluhy,
  - stanovuje způsob a podmínky provozu, způsob a harmonogram provádění údržby, požadavky na vzdělání obsluhy, ochranu obsluhy (ochranné pomůcky a prostředky) a okolního prostředí,
  - postupy odezvy na poruchy, selhání a havárie,
  - způsoby a postupy ochrany obsluhy a okolního prostředí.

Z pohledu ochrany kritické infrastruktury [9,10] u kritických entit je důležitá ***robustnost entit***, aby byla zajištěna spolehlivost po dlouhou dobu. Robustnost objektu je vlastnost, která je vložena do projektu entity pomocí parametrů použitých materiálů a postupů konstrukce a její úroveň závisí na způsobu údržby [1,8-32].

Specifická pozornost musí být věnována bezpečnosti entit, a to hlavně těm, ve kterých jsou nebezpečné látky [8,12]. Jde o ***zabezpečení entit,*** které zabrání úniku nebezpečných látek do prostření, výbuchu a požáru.

Vzhledem k tomu, že lidská společnost nemá nikdy dostatek zdrojů, sil a prostředků k ochraně všeho, se dále zabýváme jen kritickými entitami.

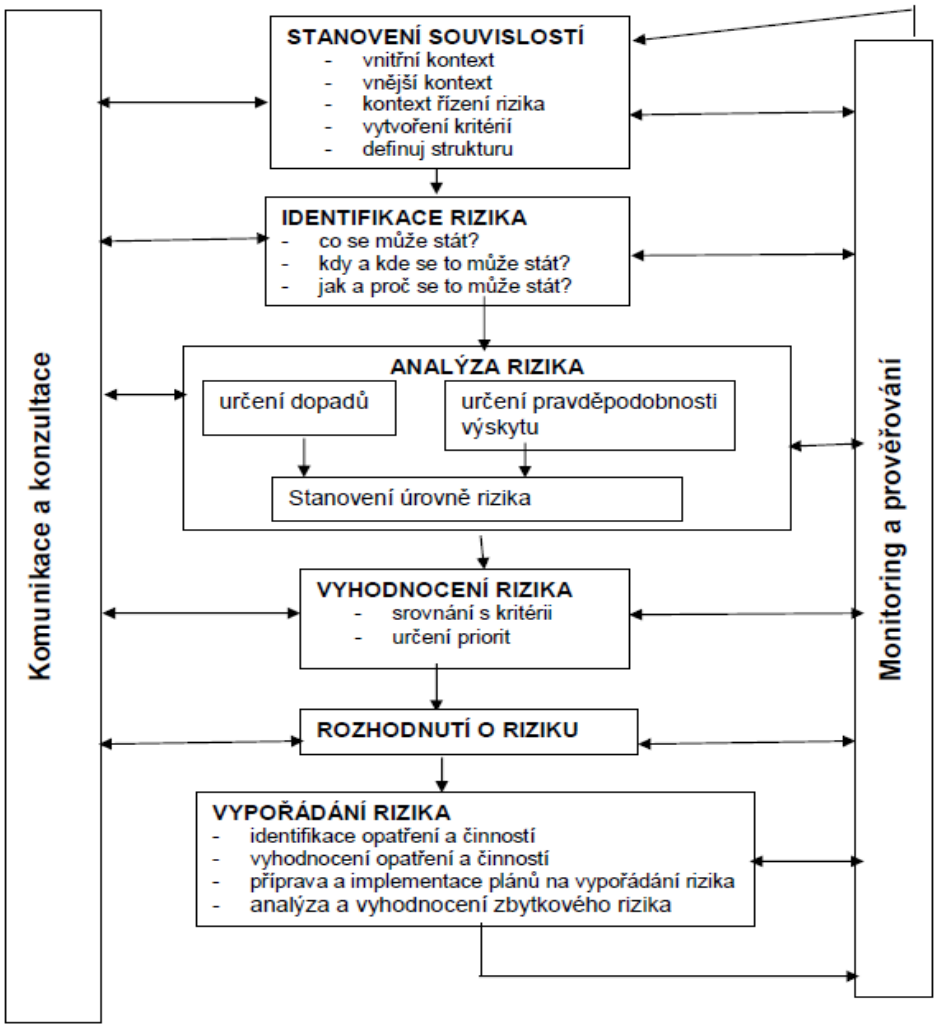
3. ŘÍZENÍ RIZIK

Kritické entity jsou složité systémy, které se skládají z velkého množství částí, které je třeba chápat jako otevřené a vzájemně provázané systémy, jak ukazuje kapitola 2. Při řízení rizik ve prospěch bezpečnosti entit (tj. celkové – integrální), které jsou složitými systémy [1,4,8-32], se musí sledovat organizační struktury, postupy a pravidla, které ovlivňují výkon a kvalitu práce lidí (výrobky či služby, údržbu, renovace i změny). Významnými faktory [1,4,8] jsou:
- odpovědnost,
- rozumná autonomie,
- adaptabilita,
- celistvost
- a smysluplnost úkolů .

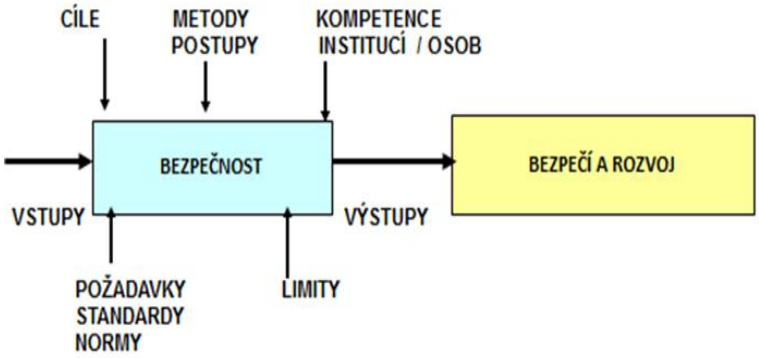
Řízení rizik požadují normy ISO 9000, ISO 31 000, ISO 31 010 atd. Model řízení rizik dle norem ISO 31 000 a ISO 31 010 je na obrázku 1.

Řízení rizik ve prospěch bezpečnosti entit (objektů, zařízení, systémů, procesů) řeší otázky:
- materiálu,
- technologií,
- projektování,¨
- konstrukce,
- výstavby,
- provozu,
- personálu,
- organizace plnění úkolů,
- vzdělávání,
- financí a práva

tak, aby zajistilo žádoucí procesy, které mu přinášejí zisk, zajišťují soulad se státem a konkurenceschopnost, a zároveň potlačilo procesy, které mu přinášejí škody a ztráty [1,4,8-32]. Model řízení je uveden na obrázku 2.



Obr. 1. Schéma pro řízení rizika dle norem ISO; podrobný popis je např. v práci [4].



Obr. 2. Model řízení rizik entity ve prospěch bezpečnosti.

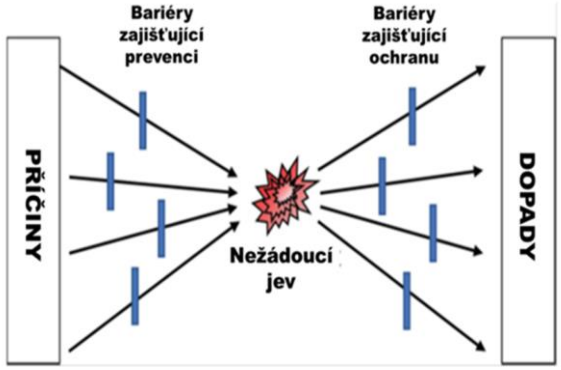
Vidíme, že při řízení rizik (vstupy - data o rizicích) hrají role:

- cíle (tj. požadovaná úroveň bezpečnosti),

- metody a postupy k dosažení cílů,
- kompetence institucí a osob,
- požadavky norem a standardů
- a limity (znalostní, finanční, materiálové a popř. i jiné).

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 (ALARA / ALARP) rizika. *Používáme:* ISO normy založené na projektovém řízení typu TQM (Total Quality Management) [7], tj. ISO 9000, 14000, 18000 a 30 000 30 010 aj.; ***postup pro řízení rizik*** [4], který zahrnuje:

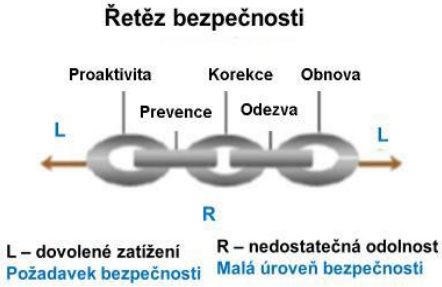
- identifikaci rizik dle principu All-Hazard-Approach [33,34],
- určení rizik a jejich klasifikace na: seznam vyhodnocených rizik; seznam rizik vyžadujících nejvyšší pozornost; a seznam neaktuálních/vyřešených rizik [4,7,8],
- rozdělení rizik vyžadujících pozornost při provozu [12] dle postupu na obrázku 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 opatření, která umožňují kvalitní odezvu.



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.

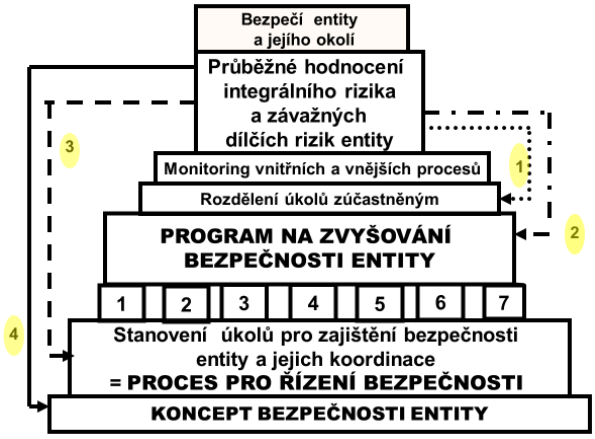
Specifické řízení rizik ve prospěch bezpečnosti [1,4,8-32,35] používá tzv. řetěz bezpečnosti, zobrazený na obrázku 4 a vyznačuje se zejména následujícími rozhodovacími procesy o objektech či zařízeních při jejich:

- umísťování – projektování - výstavbě a konstrukci - návrhu s minimalizaci rizik; známé jsou především specifické postupy označované jako risk-based-design [12,13],
- provozování se začleněním systému včasného varování a procedur pro řízení přijatelné úrovně rizik; známé jsou především specifické postupy označované jako risk-based-operation [8,14], který obsahuje nejen postupy pro normální provoz, ale i postupy na: zvládání abnormálních, nouzových a kritických stavů při jejich provozu i odstavení; dále pak postupy označované jako: risk-based maintenance; risk-based inspection; a risk based reconstruction / modernization [35].



Obr. 4. Činnosti pro zajištění bezpečnosti sledovaného systému.

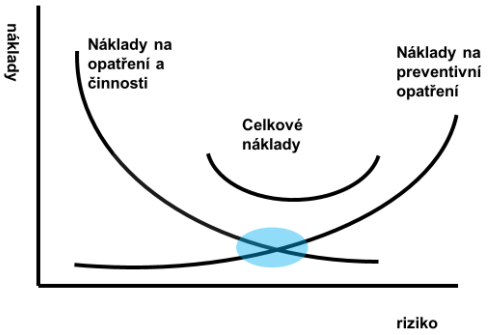
To znamená, že opatření a činnosti se provádí podle míry rizika. Nástroje používané pro řízení rizik závisí na složitosti sledované entity a jsou charakterizovány v pracích [4,36]. Řízení rizik entity v čase je uvedeno na obrázku 5 [35].



Obr. 5. Procesní model řízení bezpečnosti entity v čase. Procesy: 1- koncepce a řízení; 2 - administrativní postupy;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 [35].

Z obrázku 5 je zřejmé, že zásadní pro zajištění bezpečnosti v čase je permanentní analýza a hodnocení rizik, které přináší znalosti, což potvrzují poznatky uvedené v práci [37] a z důvodu stále rostoucí automatizace, která přináší řadu neurčitostí je třeba aplikovat metody, které mají schopnost neurčitosti zvažovat, např. fuzzy logika [38].

Je faktem, že inženýrský projekt s velkou bezpečností je nákladný a že touha každého investora či provozovatele po co nejmenších nákladech na entitu vede ke snížení bezpečnosti, tj. k zúžení intervalu podmínek, které entita zvládne. Obrázek 6 ukazuje, že ve skutečnosti je třeba porovnávat náklady na snížení rizika a náklady na nutná opatření, tj. jde o aplikaci metody CBA [36] s vyhověním požadavkům na bezpečnost.



Obr. 6. Interval celkových nákladů, ve kterém je zajištěna bezpečnost; zpracováno dle [39]; oblast optimálních nákladů je vyznačena modře.

4. DATA – ZDROJE RIZIK ENTIT

Analýza prací [1,4,8,11,12,13,15-34, 40] ukazuje, že bezpečnost entit narušují:

1. Chyby v řízení a ovládání entity.
2. Vnitřní zdroje rizik entity prvku spojené s jejím projektem, konstrukcí, jejími propojeními a provozem.
3. Chyby personálu obsluhy entity.
4. Vnější zdroje rizik entity spojené s živelními pohromami.

5. Vnější zdroje rizik entit spojené se selháním okolních entit a procesů (vazby a toky) – např. selhání dodávek elektřiny, vody, chladiva, dodávek materiálu atd.
6. Vnější zdroje rizik entity spojené s chováním veřejné správy (daně, poplatky, pobídky apod.), konkurencí, trhem apod.,
7. Útoky na entitu.
8. Kybernetické zdroje rizik spojené se sítěmi spojenými s entitou.
9. Válka.
10. Chybný dozor veřejné správy.

To znamená, že na základě analýzy konkrétních místních podmínek a konkrétní struktury a složitosti entity jde v naší zemi např. o:
- živelní pohromy (povodeň, zemětřesení, sesuv podloží, blesk, vichřice, tornádo, požár v území, pád letadla, nadměrné srážky, požár či výbuch v okolí aj.),
- agresivní vnější prostředí,
- selhání či havárie infrastruktur nutných pro provoz entity,
- nevhodné umístění entity,
- chyby v projektu a v konstrukci entity a jejího uložení (např. materiál, ze kterého je entita zhotovena není dostatečně odolný vůči působení přepravovaného média; špatné svary; nevhodná těsnění; nevhodné armatury; nevhodné senzory; špatné podpory entity dovolující průhyby a vibrace, nevhodné senzory nebo špatně umístěné senzory atd.),
- nevhodné nebo neexistující provozní předpisy,
- špatná údržba,
- vnitřní technické problémy: koroze; zanášení propojujících potrubí; extrémní teploty; opotřebovaná těsnění; atd.),
- nedodržení limit pro provoz entity,
- chyby při opravách a modernizacích,
- chyby obsluhy,
- chybné řízení provozu entity,
- nedostatečná dokumentace a chybné řízení bezpečnosti ve všech oblastech,
- nedostatečně stanovené odpovědnosti v provozu entity,
- zanedbání předpisů pro zajištění bezpečnosti,
- nedostatečný dozor veřejné správy,
- hackerský útok
- teroristický útok.

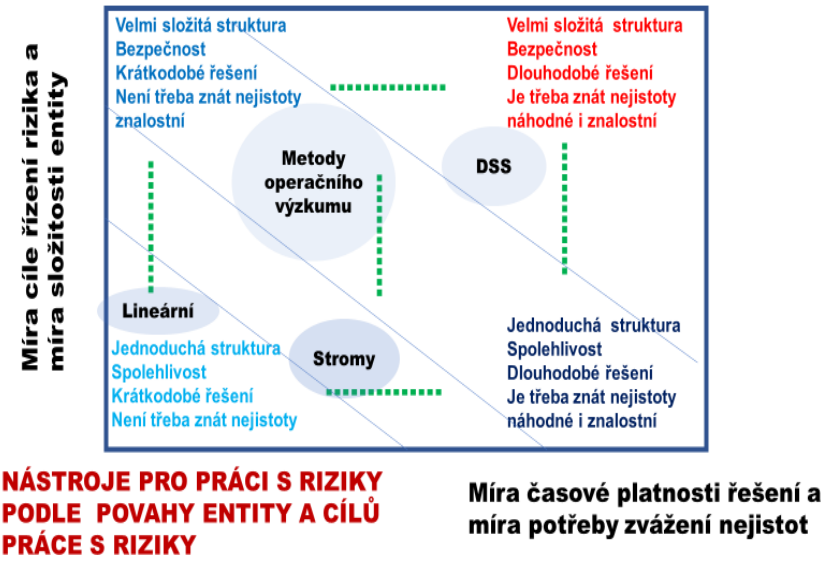
5. METODA KONTROLNÍ SEZNAM

Každý nástroj pro řízení rizik ve prospěch bezpečnosti [41] je:
- více či méně obsažný,
- sleduje určité položky dané podle potřeby,¨
- je zaměřen na určitý cíl,
- určen pro určitou osobu, která má odpovědnost za cíl.

Je zřejmé, že čím složitější je nástroj, tím větší jsou nároky na data, znalost složitých, čas zpracování a také finance. Zobrazení rozložení nástrojů řízení rizik ve prospěch bezpečnosti v závislosti na cílech a složitosti entity, která je předmětem řízení rizik ve prospěch bezpečnosti [41] je na obrázku 7. Vidíme, že čím složitější je zařízení a čím vyšší je cíl (od krátkodobé spolehlivosti jednoduchého systému až po integrální bezpečnost složitého systému), tím složitější, na data náročnější a na čas zpracování náročnější je třeba použít.

Proto pro konkrétní úkoly praxe je nutno použít takový nástroj, který dá správné výsledky a je nejméně náročný na data a čas zpracování

Pro běžnou praxi jsou vhodné kontrolní seznamy [4,41,42]. Kontrolní seznam (checklist), tj. postup založený na systematické kontrole plnění předem stanovených podmínek a opatření. Jde o soubor navzájem nezávislých otázek, který popisuje hodnocenou problematiku, přičemž je potřeba vhodně sestavit formulace a logické pořadí otázek. Otázky v kontrolním seznamu musí být logicky uspořádané, nesmí se opakovat a odpovědi na ně musí být



Obr. 7. Rozložení nástrojů řízení rizik ve prospěch bezpečnosti v závislosti na cílech a složitosti entity.

stejným směrem [4,42]. Sestavení kontrolního seznamu vyžaduje experta s nejvyšší odborností na posuzovanou problematiku, v případě multioborového problému tým expertů z jednotlivých oborů. Naproti tomu aplikace kontrolního seznamu již vyžaduje pouze základní znalosti v oboru a schopnost rozpoznání odchylek od popisovaného stavu.

Uživatel kontrolního seznamu postupuje otázku po otázce a odpovídá na ně podle předem určené hodnotové stupnice, ať už logické (ano/ne), nebo číselné. Popřípadě provede měření sledované veličiny. Výsledkem hodnocení je pak statistická hodnota, určená podle daného postupu. Kontrolní seznamy jsou vhodné pro posuzování rutinních systémů, kde pouze sledujeme odchylky od běžného stavu a není potřeba invence.

Jednoduchý kontrolní seznam obsahuje dotazy na sledované zásadní aspekty spojené s původci rizik pro sledovanou entitu. Popisný kontrolní seznam obsahuje dotazy, které testují postup pro měření parametrů. Škálovací kontrolní seznam obsahuje dotazy, které testují popis prahových hodnot, trvání dopadů a jejich vratnosti či nevratnosti s využitím škálovací metody. Dotazovací kontrolní seznam obsahuje dotazy, které testují pochopení sledovaného procesu. Kontrolní seznam pro posuzování kvality obsahuje dotazy, které testují kvalitu hodnocení (dotazuje se na škály a váhy).Rozhodovací matice, která vznikne, když se dají do vzájemné souvislosti dva kontrolní seznamy.

Výsledkem kontrolního seznamu bývá zpravidla numerická hodnota, která je rovna buď počtu odpovědí ano/ne, součtu udělených bodů, nebo měrnému průměru známek. Jednotlivé otázky nemusí mýt stejnou váhu v měrném průměru. Celá škála možných výsledků je pak rozdělena na několik úseků, kde každému úsek je přiděleno označení závažnosti situace, popřípadě ještě odkaz na následující kroky. Stejně jako soubor otázek a jejich hodnocení i kalibrace výsledné škály je potřeba provést odborně.

Na základě poznatků shrnutých v pracích [4,42] a zkušeností autorky z praxe, kontrolní seznam pomáhá eliminovat lidské chyby, protože vede pracovníky tak, že provedou všechny požadované úkony v požadovaném pořadí a kvalitě a že vyhodnotí všechny požadované parametry. Tím zvyšuje kvalitu požadované činnosti, což zvyšuje bezpečnost.

Dle současného poznání [4,8,12,36,42,43], je důležité jak správné pořadí otázek (provádí se dle procesního modelu entity), tak hodnocení otázek kontrolního seznamu a pravidla pro:

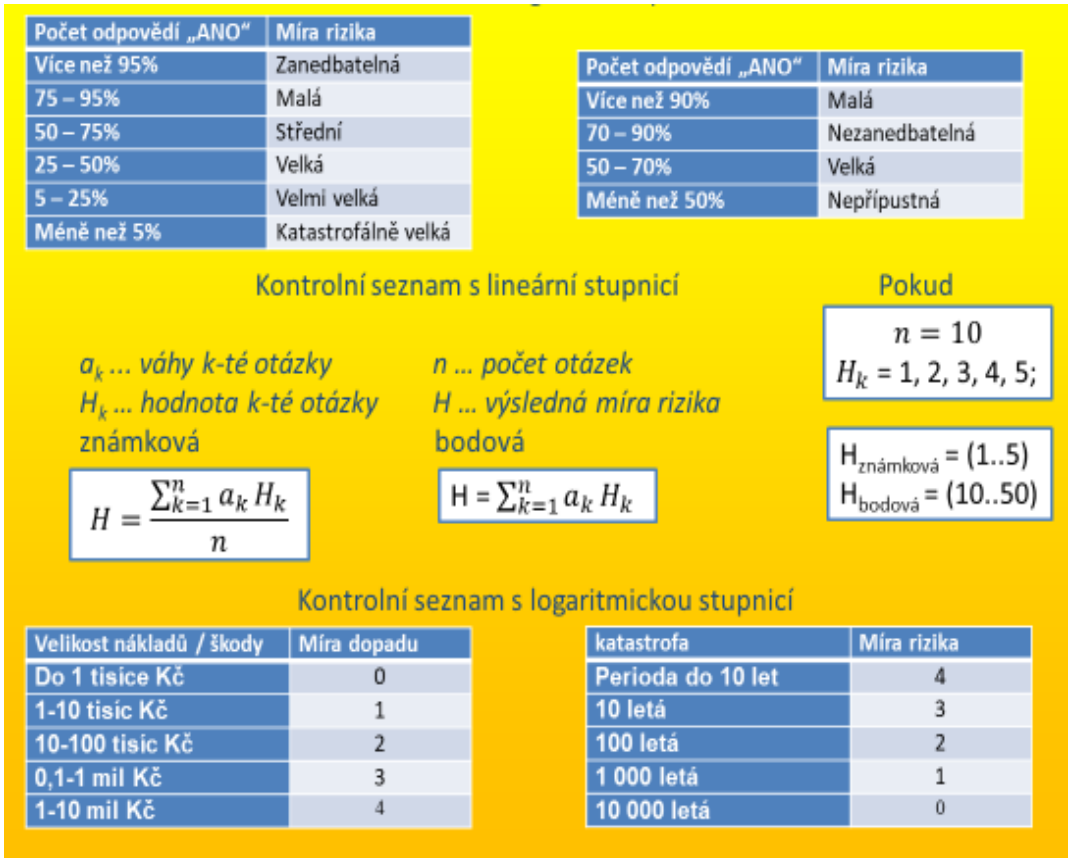
- jeho aplikaci,
- postupy pro nevyhovující situace,
- způsoby hodnocení jednotlivých otázek i celého kontrolního seznamu, protože dle poznatků shrnutých v práci [8] příčiny selhání a havárií způsobené jedním zdrojem rizika jsou jen cca 20% a zbytek je spojen s kumulací menších zdrojů rizik, které samotné by selhání či havárii samy nezpůsobily, v krátkém časovém intervalu.

Pro hodnocení jednotlivých otázek se dle [4,36,42] používají stupnice:

- jednoduché - ANO či NE,

- stupnice: 0-3, 1-5, 1-10, 1-100.

Pro vyhodnocení celého kontrolního seznamu se používá celá řada stupnic – OECD, FEMA, Swiss Re atd. [41]. Nejčastěji používané hodnotové stupnice jsou uvedeny na obrázku 8.V České republice se v technické oblasti od poloviny 80. let používá stupnice uvedená v tabulce 1.



Obr. 8. Nejčastěji používané hodnotové stupnice u kontrolních seznamů.

Tabulka 1. Způsob hodnocení celého kontrolního seznamu; N je počet odpovědí NE v %.

Míra rizika	**Hodnoty N v %**
Extrémně vysoká – 5	Více než 95 %
Velmi vysoká – 4	70 - 95 %
Vysoká – 3	45 - 70 %
Střední – 2	25 – 45 %
Nízká – 1	5 – 25 %
Zanedbatelná – 0	Méně než 5 %

V některých případech se používají kontrolní seznamy, ve kterých jsou otázky různě barevné; když je červená, tak se musí problém okamžitě řešit (např. pokyny pro piloty Gripenů) [44].

Velmi často se používají kontrolní seznamy jako základ systémů pro podporu rozhodování (decision support system - DSS) [3,4,8,12,36,42,45]. V těchto případech se posuzují nesouměřitelné položky – velikost dopadů rizika na:

- životy a zdraví lidí,
- majetek,
- životní prostředí,
- škody na technologii,¨

- náklady na odezvu a obnovu,
- ekonomické škody vyvolané nefunkčností entity (např. nedostatek výrobků); i dlouhodobé dopady nefunkčnosti kritických zařízení na životní úroveň obyvatel (např. nezaměstnanost, kriminalita, občanské nepokoje).

Pro hodnocení v těchto případech musí být vždy sestavena stupnice pro zajištění na souměřitelnosti odpovědí na otázky (dopady rizik technických, právních, lidských atd. musí mít stejnou velikost); příklady jsou v [8,12]. Výsledkem je pak dle principu maximálního užitku [45] ta varianta, která má nejnižší integrální riziko.

6. PŘÍKLADY

Dále jsou uvedeny příklady kontrolních seznamů, vytvořené dle těch, které byly sestavené a již použité v praxi [44,46]; vzhledem ke smluvním ujednáním nejsou uvedeny entity, pro které byly sestaveny a odzkoušeny v praxi.. Z uvedených příkladů, tabulky 2-12, je zřejmé, že konkrétní náplň kontrolních seznamů vždy závisí na cíli, ke kterému slouží.

Tabulka 2. Kontrolní seznam pro posuzování kritičnosti technického díla.

Otázka	**Odpověď**	
	ANO	**NE**
Konají se v daném technickém díle kritické činnosti?		
Je prováděno hodnocení rizik pravidelně a po každé větší nehodě?		
Jsou v daném technickém díle kritická nebo hodnotná zařízení?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně umístěná?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně vyrobena?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně instalována?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně provozována?		
Jsou všechna propojení mezi kritickými nebo hodnotnými zařízeními v daném technickém díle správně a bezpečně naprojektována, provedena a provozována?		
Jsou správně zabezpečeny kybernetické sítě technického díla?		
Mají všechna kritická nebo hodnotná zařízení v daném technickém díle zálohy?		
Je technické dílo fyzicky zabezpečeno?		
Jsou jasně stanoveny odpovědnosti za provoz technického díla?		
Jsou jasně stanoveny odpovědnosti za provoz kritických nebo hodnotných zařízení v daném technickém díle?		
Je dokumentace technického díla a všech kritických nebo hodnotných zařízení úplná a správná?		
Je prováděna proaktivní preventivní údržba všech kritických nebo hodnotných zařízení technického díla?		
Je zaveden integrovaný systém řízení bezpečnosti technického díla?		
CELKEM		

Tabulka 3. Kontrolní seznam pro posuzování požární bezpečnosti technického díla.

Otázka	**Odpověď**	
	ANO	**NE**
Je požární útvar technického díla dobře obeznámen se zařízeními, jejich umístěním a se specifickými ohroženími v technickém díle?		
Je požární poplachový systém technického díla certifikován tak, jak je požadováno?		
Je požární poplachový systém technického díla testován alespoň jednou ročně?		
Používá-li požární poplachový systém technického díla vnitřní stoupací potrubí a ventily, jsou pravidelně kontrolovány?		
Používá-li požární poplachový systém technického díla venkovní neveřejné požární hydranty, jsou alespoň jednou ročně odzkoušeny a je dle plánu prováděna rutinní preventivní údržba?		
Jsou požární dveře a požární uzávěry v technickém díle v dobrém provozním stavu?		

Jsou požární dveře a požární uzávěry v technickém díle nezatarasené (tj. volné) a jsou chráněné proti zatarasení včetně jejich protiváh (vyvážení)?		
Jsou automatické řídící ventily vodního sprinklerového systému, tlaku vzduchu a tlaku vody v technickém díle kontrolovány týdně / periodicky tak, jak je požadováno?		
Je údržba automatických sprinklerových systémů v technickém díle přidělena odpovědným osobám nebo je svěřena kontraktorovi?		
V případě, že údržba automatických sprinklerových systémů v technickém díle je přidělena kontraktorovi, je tento řádně poučen, aby se choval tak, aby nezpůsobil nehodu?		
Jsou hlavice sprinklerů v technickém díle chráněny kovovými kryty když jsou vystaveny fyzickému poškození?		
Je v technickém díle řádně udržován prostor pod sprinklerovými hlavicemi?		
Jsou přenosné hasicí přístroje v technickém díle k dispozici v adekvátním množství a v odpovídajících typech?		
Jsou hasicí přístroje v technickém díle připevněny ve snadno dosažitelné poloze?		
Jsou hasicí přístroje v technickém díle pravidelně plněny a označeny visačkou o inspekci?		
Jsou zaměstnanci technického díla pravidelně instruováni o použití hasicích přístrojů a o postupech požární ochrany?		
Jsou prováděla pravidelná cvičení akceschopnosti požární techniky technického díla?		
Odpovídá požární technika i personál požadavkům, které vyžaduje požární ochrana technického díla?		
CELKEM		

Tabulka 4. Kontrolní seznam pro posuzování bezpečnosti přenosných žebříků.

Otázka	**Odpověď**	
	ANO	**NE**
Jsou všechny žebříky udržovány v dobrém stavu, jsou spoje mezi příčlemi a upevnění žebřin, všechna zařízení a součásti bezpečně připevněna a jsou pohyblivé části volné bez odporu a drhnutí?		
Je každý žebřík vybaven protiskluzovou bezpečnostní plochou?		
Je každá nášlapná plocha nebo příčka kovového žebříku opatřena protiskluzovou bezpečnostní plochou?		
Nejsou příčky žebříku a schůdky znečištěny oleji nebo mazivy?		
Je zakázáno umísťovat žebřík před otevírající se dveře, s výjimkou dveří, jejichž otevírání je blokováno, zamčeno nebo zajištěno?		
Je zakázáno umísťovat žebříky na kabiny, sudy nebo jiné nestabilní podklady, aby bylo dosaženo potřebné (další) výšky?		
Jsou zaměstnanci technického díla poučeni o tom, aby při výstupu a sestupu po žebříku byli obráceni čelem k žebříku?		
Je zaměstnancům technického díla zakázáno používat žebříky, pokud jsou zlomené, když jim scházejí příčle, jsou zlomené žebřiny (bočnice) nebo pokud jsou poškozeny jakékoliv jiné části?		
Jsou zaměstnanci technického díla poučeni o tom, aby nepoužívali poslední (nejvrchnější) stupeň standardního žebříku k vykročení?		
Používají-li se příčkové žebříky k dosažení mimoúrovňových (zvýšených) ploch (poloh), střech apod., přesahuje žebřík vždy nejméně o 90 cm nad mimoúrovňovou plochu?		
Je požadováno, aby u používaných přenosných příčkových nebo lištových žebříků byl spodek umístěn tak, aby nemohlo dojít k uklouznutí nebo je připoután (přivázán) či jinak přidržován?		
Jsou přenosné kovové žebříky zřetelně (čitelně) označeny značkami „VÝSTRAHA – Nepoužívat v blízkosti elektrických zařízení“ nebo ekvivalentní formulací?		
Je zaměstnancům technického díla zakázáno používat žebříky pro jiné než stanovené účely?		
Jsou zaměstnanci technického díla poučeni o tom jak se seřizuje rozměr žebříků před jeho použitím (ne tedy při stání na žebříku samotném či z pozice nad ním)?		
Jsou kovové žebříky pravidelně kontrolovány s ohledem zjištění jejich poškození?		
Jsou příčle žebříků stejnoměrně umístěny ve vzdálenosti 30 cm od středu ke středu.		
CELKEM		

Tabulka 5. Kontrolní seznam pro posuzování bezpečnosti ručního nářadí a zařízení.

Otázka	**Odpověď**	
	ANO	**NE**
Jsou všechny nástroje a zařízení používané zaměstnanci na pracovišti v dobrém stavu?		
Jsou ruční nástroje / nářadí jako dláta, děrovače apod., které se použitím mohou opotřebovat, opravovány nebo nahrazovány dle potřeby?		
Jsou zlomené nebo porušené násady kladiv, seker a podobných zařízení okamžitě vyměněny?		
Jsou ztupená nebo zakřivená nářadí pravidelně nahrazována?		
Jsou používána vhodná držátka na pilnících nebo podobných nástrojích / nářadích?		
Jsou zaměstnanci technického díla upozorněni na nebezpečí vyplývající z vadného nebo nesprávného používání ručního nářadí / nástrojů?		
Jsou používány bezpečnostní brýle, obličejové štíty apod. při práci s ručním nářadím nebo zařízením, které může produkovat polétavé materiály nebo se může zlomit?		
Jsou zvedáky periodicky kontrolovány, aby se zajistily jejich bezvadné provozní podmínky?		
Jsou násady nářadí zaklíněny pevně do hlavic u všeho nářadí?		
Jsou řezné hrany u nářadí udržovány tak, aby se nářadí pohybovalo hladce bez kvedlání nebo poskakování?		
Jsou nástroje / nářadí skladovány na suchém a bezpečném místě tak, aby nemohly být zneužity?		
Je používána ochrana očí a obličeje při opracovávání neforemných předmětů, které nelze řádně upevnit?		
CELKEM		

Tabulka 6. Kontrolní seznam pro posuzování bezpečnosti přenosných (elektricky poháněných) nářadí a zařízení.

Otázka	**Odpověď**	
	ANO	**NE**
Jsou brusky, pily a podobná zařízení v odpovídajícím bezpečném provedení?		
Jsou nářadí poháněná elektřinou používána se správnou ochranou a příslušenstvím doporučeným výrobcem?		
Jsou přenosné kotoučové pily vybaveny ochranami nad a pod břitem?		
Jsou ochrany kotoučových pil kontrolovány s cílem zajistit, aby nemohly být zaklíněny tak, že by to umožnilo, že nižší část břitu by byla nechráněna?		
Jsou rotující nebo pohybující části zařízení chráněny tak, aby zabránily fyzickému kontaktu?		
Jsou všechna provozovaná nářadí a zařízení poháněná elektrickým proudem (šňůrově připojená) vhodně uzemněná nebo mají schválenou dvojitou izolaci?		
Je zajištěna efektivní ochrana nad pásy, řemenicemi, kladkami, řetězy, ozubenými koly na takových zařízeních, jako jsou míchačky, kompresory apod.?		
Jsou přenosné ventilátory vybaveny plnou ochranou nebo mřížkou s otvory 1.3 cm nebo méně?		
Je používané zvedací zařízení vhodné pro zvedání těžkých předmětů a jsou jeho zvedací poměry a charakteristiky vhodné pro daný úkol?		
Jsou přerušovače obvodu pro případ zemního zkratu umístěny na všech dočasných elektrických obvodech s 15 a 20 A, které byly používané po dobu konstrukce?		
Jsou pneumatické a hydraulické hadice na elektricky napájených nářadích kontrolovány pravidelně s ohledem na poškození a škody?		
CELKEM		

Tabulka 7. Kontrolní seznam pro posuzování bezpečnosti strojů.

Otázka	**Odpověď**	
	ANO	**NE**
Je v technickém díle k dispozici školicí program, který zajišťuje vzdělání zaměstnanců ohledně bezpečných metod spojených s provozem strojů?		

Existuje v technickém díle adekvátní dohled, který zajišťuje, že zaměstnanci dodržují postupy pro bezpečný provoz strojů?		
Existuje v technickém díle pravidelný program inspekcí bezpečnosti strojů a zařízení?		
Jsou v technickém díle všechny stroje a zařízení udržovány v čistém stavu a jsou řádně udržovány?		
Je v technickém díle provedeno dostatečné vyklizení kolem a mezi stroji takové, které zajišťuje bezpečný provoz, seřizování a servis, nakládání s materiálem a odstraňování odpadu?		
Jsou v technickém díle zařízení a stroje bezpečně umístěny a je-li nutné i ukotveny tak, aby se zabránilo jejich převržení nebo jinému pohybu, který by mohl vyvolat pracovní úraz?		
Je v technickém díle na každém stroji síťový (silnoproudý) vypínač v dosahu polohy provozovatele takového stroje?		
Lze v technickém díle na každém stroji vypnout přívod elektrického proudu (elektrický výkon, příkon) pro případ údržby, opravy nebo z důvodu bezpečí?		
Jsou v technickém díle nosné kovové části, které nejsou pod proudem u strojů poháněných elektřinou spojeny a uzemněny?		
Jsou v technickém díle nožní spínače chráněny nebo uspořádány tak, že je zabráněno neúmyslnému uvedení do činnosti osobou nebo padajícími předměty?		
Jsou v technickém díle ručně ovládané ventily a spínače, řídící provoz zařízení a strojů, jasně identifikovatelné a snadno přístupné?		
Jsou v technickém díle všechny nouzové vypínače nabarveny červenou barvou?		
Jsou v technickém díle všechny řemenice (převody) a pásy, které jsou do 210 cm nad podlahou nebo nad provozní plošinou, řádně chráněny?		
Jsou v technickém díle všechny pohybující se řetězy a ozubená soukolí (pohony motoru) řádně chráněny?		
Jsou v technickém díle na strojích, které jsou chlazeny, namontovány kryty tak, aby chladivo nestříkalo na zaměstnance?		
Jsou v technickém díle k dispozici metody, které chrání provozujícího / obsluhu a jiné zaměstnance v okolí strojů od ohrožení vytvářených v místě provozu, v místech štípání (řezání), u rotujících částí, polétavých třísek a jisker?		
Jsou v technickém díle ochrany strojů zabezpečeny a jsou nainstalovány tak, aby nemohly vyvolat ohrožení při používání?		
Jestliže se v technickém díle používá ruční nářadí k přísunu nebo oddálení materiálu, jsou chráněny ruce obsluhy / provozujícího?		
Je v technickém díle zajištěno, že otáčecí bubny (válce), sudy a kontejnery jsou chráněny uzávěrem, který je uzamčen hnacím mechanismem tak, aby nemohlo dojít k pootočení dokud je uzávěr na svém místě?		
Mají v technickém díle hřídele a vřetena soustruhů spolehlivé a zabezpečené podpěry (nosiče) a nemůže u nich dojít k samovolnému spuštění?		
Jsou v technickém díle instalována opatření, která zabrání, aby se stroje automaticky spustily (nastartovaly), když je proud obnovován po selhání dodávky nebo vypnutí proudu?		
Jsou v technickém díle stroje konstruovány tak, aby u nich nedocházelo k nadměrné vibraci, je-li připevněno nářadí velkého rozměru a pracuje-li na plný výkon?		
Je-li v technickém díle stroj čištěn stlačeným vzduchem, je kontrolován tlak vzduchu a jsou používány osobní ochranná zařízení nebo jiná ochrana k ochraně obsluhy a dalších pracujících proti poškození oči a těla?		
Jsou v technickém díle lopatky ventilátoru chráněny krytem s otvory ne většími než 1.2 cm, pracují-li do 210 cm nad podlahou?		
Jsou v technickém díle pily pro rozřezávání vybaveny zařízením proti zpětnému rázu a rozpěrkou?		
Jsou v technickém díle ramenové kotoučové pily uspořádány tak, aby se řezací hlava snadno vrátila zpět na desku, je-li uvolněna?		
CELKEM		

Tabulka 8. Kontrolní seznam pro posuzování bezpečnosti svařování, řezání a pájení.

Otázka	**Odpověď**	
	ANO	**NE**
Mohou v technickém díle pouze autorizované a proškolené osoby používat zařízení pro svařování, řezání a pájení?		
Má každý pracovník technického díla provozující svařování, řezání a pájení kopii odpovídajících provozních postupů a musí je dodržovat?		
Jsou v technickém díle ocelové lahve na stlačený plyn pravidelně přezkušovány s ohledem na možné poruchy, projevy koroze nebo úniku?		
Je v technickém díle věnována odpovídající pozornost při manipulování a skladování tlakových lahví, bezpečnostním ventilům, pojistným (přepouštěcím) ventilům atd. s cílem zabránit jejich poškození?		
Jsou v technickém díle přijata preventivní opatření k zabránění vzniku směsi vzduchu nebo kyslíku s hořlavými plyny a následnému hoření, kromě hořáku nebo pájecí lampy?		
Používají se v technickém díle pouze certifikované (schválené) aparatury (pájecí lampy, regulátory, redukční ventily, zdroje / generátory acetylenu, rozdělovače – rozdělovací kusy)?		
Jsou v technickém díle tlakové lahve umísťovány tak, aby nebyly v dosahu tepelných zdrojů?		
Jsou v technickém díle tlakové lahve umísťovány v dostatečné vzdálenosti od výtahů, schodů nebo ochozů (přechodových lávek)?		
Je v technickém díle zakázáno používat tlakové lahve pro valení nebo podpírání?		
Jsou v technickém díle prázdné tlakové lahve odpovídajícím způsobem označeny a jsou uzavřeny jejich ventily?		
Jsou v technickém díle řádně rozmístěny značky s názvem: NEBEZPEČÍ – ZÁKAZ KOUŘENÍ, ZÁKAZ POUŽÍVÁNÍ ZÁPALEK NEBO OTEVŘENÉHO OHNĚ nebo jejich ekvivalenty?		
Je v technickém díle zajištěno, aby se tlakové lahve a jejich ventily, spoje, regulátory, hadice a aparatury nedostaly do styku s oleji nebo jinými mastnými látkami?		
Dbá se v technickém díle na to, aby bylo u tlakových lahví zabráněno jejich pádu nebo nárazu?		
Je v technickém díle zajištěno, aby v případech, kdy se nepoužijí speciální nákladní automobily, byly regulační ventily sejmuty a aby byla nasazeny ochranné kloboučky ventilů před transportem tlakových lahví?		
Mají v technickém díle válce, které nejsou připevněné a jsou bez kol, klíče, násady (držátka) nebo nepřizpůsobené (francouzské) klíče na zastavovacích (těsnicích, zarážecích) ventilech, když jsou v provozu?		
Jsou v technickém díle zkapalněné plyny skladovány a transportovány v nádobách s koncovými ventily, na nichž je umístěn ventilový kryt?		
Jsou v technickém díle přijata opatření, aby nikdy nepraskl ventil ocelové lahve s palivem poblíž zdrojů, které mohou způsobit zapálení?		
Je v technickém díle zajištěno, aby před tím, než se odstraní regulátor, došlo k uzavření ventilu a k vypuštění plynu z regulátoru?		
Používá se v technickém díle červené označení k identifikaci hadice s acetylenem (nebo jiného paliva), zelené pro hadici s kyslíkem a černé pro inertní plyn nebo hadici se vzduchem?		
Používají se v technickém díle tlakové redukční regulátory pouze pro plyny a tlaky, pro které jsou určené?		
Je v technickém díle napětí otevřeného obvodu (bez zatížení) u svařovacích a řezacích strojů pokud možno co nejnižší a nepřekračuje doporučené limity?		
Používají se v technickém díle ve vlhkém prostředí automatické ovladače pro redukci napětí při zatížení?		
Kontroluje se v technickém díle pravidelně uzemnění rámu strojů a bezpečnostní zemnění přenosných strojů?		
Jsou v technickém díle elektrody oddáleny (vyjmuty) z držáků, když se nepoužívají?		
Vyžaduje se v technickém díle, aby byl elektrický proud ke svařovací soupravě zastaven, když souprava není v provozu?		
Je v technickém díle k dispozici hasicí přístroj pro okamžité použití?		
Je v technickém díle zakázáno, aby si svářeč ovinul nebo obkroužil kabel svařovací elektrody kolem svého těla?		

Jsou v technickém díle vlhké stroje řádně vysušeny a před použitím otestovány?		
Jsou v technickém díle pracovní a kabelové přívody k elektrodám kontrolovány často s ohledem na zjištění jejich opotřebení a poškození a jsou znovu přešněrovány (provlečeny), je-li to potřeba?		
Jsou v technickém díle prostředky pro propojování kabelů dostatečně dlouhé a přiměřeně izolované?		
Je v technickém díle zajištěno, aby když předmět na svařování nemůže být přemístěn a když nemůže být odstraněno požární ohrožení, že se musí používat štíty k omezení tepla, jisker a strusky?		
Jsou v technickém díle požární hlásiče určení k dohledu při svařování nebo řezání umístěny na místech, kde by mohl vzniknout závažný požár?		
Jsou v technickém díle hořlavé podlahy zvlhčovány, pokryty vlhkým pískem nebo ochráněny požárně odolnými štíty (kryty)?		
Když podlahy v technickém díle jsou zespoda promočené, je zajištěno, aby osoby byly ochráněny před možným elektrickým šokem?		
Když se v technickém díle provádí svařování na kovových stěnách, jsou přijata opatření k ochraně hořlavých látek na druhé straně stěn?		
Jsou v technickém díle před zahájením prací s teplem (v horkých provozech) bubny, barely a jiné cisterny vyčištěny tak dokonale, aby na nich nezůstal žádný zbytek látek, který by mohl explodovat, iniciovat nebo vyprodukovat toxické páry?		
Vyžaduje se v technickém díle, aby přilby pro ochranu očí, ruční štíty a ochranné brýle vyhovovaly příslušným standardům?		
Jsou zaměstnanci technického díla, kteří jsou vystaveni nebezpečí při svařování, řezání nebo pájení, chráněni osobními ochrannými zařízeními a oděvy?		
Kontroluje se v technickém díle, že je adekvátní větrání v prostoru, kde se provádí svěřování nebo řezání?		
Když se v technickém díle pracuje ve stísněných prostorách, provádí se monitorování prostředí a jsou k dispozici prostředky k rychlému přesunu svářečů v případě nouzové situace?		
CELKEM		

Tabulka 9. Kontrolní seznam pro posuzování bezpečnosti elektrických zařízení.

Otázka	**Odpověď**	
	ANO	**NE**
Byla v technickém díle dosažena shoda s příslušnými platnými standardy pro všechny smluvní práce na elektrických zařízeních?		
Jsou všichni zaměstnanci technického díla povinni hlásit, pokud možno co nejdříve, jakékoliv viditelné ohrožení života nebo majetku pozorované v souvislosti s elektrickými zařízeními nebo elektrickými vedeními?		
Jsou zaměstnanci technického díla proškoleni o tom, aby prováděli předběžné kontroly a / nebo vhodné testy pro zjištění podmínek existujících před zahájením práce na elektrických zařízeních nebo elektrických vedeních?		
Když se v technickém díle seřizují, udržují nebo nastavují elektrická zařízení nebo elektrická vedení, jsou potřebné spínače zapnuty, vypnuty a oštítkovány, kdykoliv je to možné?		
Jsou v technickém díle přenosná elektrická nářadí a zařízení uzemněna nebo jsou opatřena dvojitou izolací?		
Jsou v technickém díle elektrické spotřebiče takové jako vakuové čističe, leštiče, svařovací soupravy atd., uzemněny?		
Mají v technickém díle provozované prodlužovací šňůry zemnicí vodič?		
Jsou v technickém díle zakázány vícezástrčkové rozdvojky?		
Mají v technickém díle všechny přechodné (dočasné) obvody AC (střídavého proudu) s 15 nebo 20 A 120 V nainstalovány přerušovače proudu při selhání zemnění v místech, kde se provádí výstavba, demolice, přestavby, změny nebo výkopy?		
Jsou v technickém díle všechny přechodné (dočasné) obvody chráněny vhodnými vypínači nebo zástrčkami na spojích s permanentním vedením?		
Nachází se v technickém díle elektrické instalace v prostorách s nebezpečím prachu nebo par? Jestliže ano, splňují požadavky příslušného standardu pro nebezpečná místa?		

Jsou v technickém díle exponovaná vedení a šňůry s odřenou nebo poškozenou izolací opravovány nebo nahrazeny okamžitě?		
Je v technickém díle zajištěno, aby pružné (ohebné) šňůry a kabely nebyly slepeny nebo nastaveny?		
Jsou-li v technickém díle svorky nebo jiné zabezpečující prostředky nainstalované na ohebných šňůrách nebo na kabelových zástrčkách, elektrických zásuvkách, nářadí, zařízení atd. a plní obal kabelu bezpečně funkci?		
Jsou v technickém díle všechny šňůry, kabely a proudová spojení neporušené a zabezpečené?		
Jsou v technickém díle ve vlhkých nebo sychravých místech použita jen elektrická nářadí vhodná nebo jsou chráněna jinak?		
Je v technickém díle určeno umístění elektrických vedení a kabelů (nadzemních, podzemních, podpodlažních, postranních atd.) před zahájením výkopů, vrtů nebo podobných prací?		
Je v technickém díle zakázáno používat kovové vyměřovací pásky, lanka, montážní nebo podobná zařízení s kovovými ovíjecími vlákny tam, kde by mohly přijít do styku s energetickými částmi zařízení nebo vodičových obvodů?		
Je v technickém díle zakázáno používat kovové žebříky v prostorách, ve kterých žebřík nebo osoba ho používající by mohla přijít do styku s energetickými částmi nebo zařízeními, upínacími prostředky (přípravky) nebo vodičovými obvody?		
Jsou v technickém díle všechny rozpojovací vypínače a obvodové přerušovače oštítkovány tak, aby bylo zřejmé jejich užívání nebo obsluha zařízení?		
Jsou v technickém díle před výměnou pojistek odpojovací prostředky otevřené (tj. je provedeno odpojení od sítě)?		
Splňují v technickém díle všechny vnitřní elektroinstalace opatření na uzemnění kovových částí kabelových kanálů, zařízení a krytů? Jsou v technickém díle všechny elektrické kabely a uzávěry bezpečně upevněny v místě?		
Jsou v technickém díle všechny energetické části elektrických obvodů a zařízení chráněny proti havarijnímu kontaktu se schválenými skřínkami nebo kryty?		
Je v technickém díle dostatečný přístup a pracovní prostor, které umožňují pohotové a bezpečné provozy a údržby všech elektrických zařízení?		
Je v technickém díle dostatečný přístup a pracovní prostor, které umožňují pohotové a bezpečné provozy a údržby všech elektrických zařízení?		
Je v technickém díle dostatečný přístup a pracovní prostor, které umožňují pohotové a bezpečné provozy a údržby všech elektrických zařízení?		
Jsou v technickém díle všechny nepoužívané otvory (včetně odpojovačů proudu) v elektrických uzávěrech a instalacích uzavřeny vhodnými kryty, ucpávkami nebo pláty?		
Jsou v technickém díle elektrické uzávěry takové jako spínače, schránky, spojovací krabice atd. opatřeny těsně instalovanými kryty nebo pláty?		
Jsou v technickém díle odpojovací spínače elektrických motorů nad 2 koňské síly schopné otevřít obvod, je-li motor v zastavené poloze, aniž by došlo k explozi? (Vypínače musí mít výkon v koních shodný (rovný) nebo vyšší než je jmenovitý hp výkon motoru.)		
Provádí se v technickém díle nízkonapěťová ochrana v řídícím zařízení motorů pohonných strojů nebo zařízení, které by mohly pravděpodobně způsobit úraz neúmyslným nastartováním?		
Je v technickém díle každý odpojovací spínač motoru nebo přerušovač obvodu umístěn v dohledu řídícího zařízení motoru?		
Je v technickém díle každý motor umístěn v dohledu jeho řadiče nebo v dohledu vypínacích prostředků řadiče, které jsou schopné zůstat uzavřené v otevřené pozici nebo je nainstalováno separátní odpojovací zařízení v obvodu v dohledu motoru?		
Existuje v technickém díle řadič pro každý motor nad 2 koňské síly, řazený v koních shodný nebo vyšší než je jmenovitý výkon provozovaného motoru?		
Jsou zaměstnanci technického díla, kteří pravidelně pracují na nebo v blízkosti energetických elektrických zařízení nebo vedení proškoleni o metodách aplikace kardio-pulmonární resuscitace?		
Je zaměstnancům technického díla zakázáno pracovat osamoceně na energetických vedeních nebo zařízeních nad 600 voltů?		
CELKEM		

Tabulka 10. Kontrolní seznam pro posuzování bezpečnosti technického díla pro řídícího pracovníka.

Otázka	**Odpověď**	
	ANO	**NE**
Obsahuje dokumentace technického díla schémata, návody?		
Obsahuje dokumentace technického díla protokoly o zkouškách?		
Jsou součástí dokumentace technického díla informace o výcviku obsluhy?		
Jsou v dokumentaci technického díla uvedeny podmínky, za nichž zařízení nesmí být používáno?		
Jsou v dokumentaci technického díla upozornění na možná nebezpečí?		
Analyzovala se rizika zařízení technického díla pro všechny etapy jeho technického života a pro všechny podmínky užívání (instalace, údržba, obsluha)?		
Identifikovala se všechna možná významná ohrožení technického díla a byla oceněna jejich závažnost včetně odhadu četnosti výskytu?		
Specifikovala se v technickém díle opatření pro snížení / odstranění rizik?		
Zahrnuje analýza rizik technického díla také stavy způsobené nesprávnou obsluhou?		
Počítalo se při analýze rizik technického díla i s případy, které se mohou důvodně předpokládat?		
Vzalo se při analýze rizik technického díla v úvahu i možné nepohodlí vyplývající z užívání ochranných pomůcek a prostředků?		
Jsou výsledky analýzy rizik technického díla součástí dokumentace?		
CELKEM		

Tabulka 11. Kontrolní seznam pro posuzování bezpečnosti technického díla na základě posouzení kvality práce s riziky.

Otázka	**Odpověď**	
	ANO	**NE**
Jsou v dokumentaci technického díla odlišovány pojmy nebezpečí, ohrožení a riziko?		
Je dokumentace technického díla založena na kontextu, který zvažuje jen aktiva technického díla?		
Je dokumentace technického díla založena na kontextu, který zvažuje aktiva technického díla a vybraná veřejná aktiva (zaměstnanci, kontraktoři, návštěvních, lidé v okolí, pracovní a životní prostředí)?		
Je dokumentace technického díla založena na kontextu, který zvažuje aktiva technického díla a všechna veřejná aktiva?		
Jsou zvažovány zdroje rizik, které stanovuje zkušenost experta?		
Jsou zvažovány zdroje rizik, které stanovuje legislativa a zkušenost experta?		
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle?		
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle a lidský faktor spojený se špatně provedenými pracovními úkony?		
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle a lidský faktor v nejširším pojetí?		
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle, zdroje určené BOZP a zdroje spojené s ochranou pracovního prostředí?		
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle, zdroje určené BOZP a zdroje spojené s ochranou pracovního prostředí i s ochranou životního prostředí vně technického díla?		
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle, zdroje určené BOZP a zdroje spojené s ochranou pracovního prostředí i s ochranou životního prostředí vně technického díla v systémovém pojetí (tj., že všechny zdroje rizik jsou vzájemně propojené)?		
Jsou zvažovány zdroje rizik dle přístupu All-Hazard-Approach (tj. systémové pojetí i vnější zdroje) [1]?		
Je zvažováno jen dílčí riziko?		
Jsou zvažována dílčí rizika i integrované riziko?		

Jsou zvažována dílčí rizika, integrovaná rizika i integrální riziko?		
Jsou rizika v technickém díle systematicky sledována?		
Jsou rizika technického díla systematicky sledována až po výstavbě technického díla?		
Jsou rizika technického díla systematicky sledována po celou dobu životnosti technického dílu už od jeho projektu?		
Jsou rizika technického díla systematicky sledována po celou dobu životnosti technického dílu už od jeho projektu a v jeho projektu a provozu je uplatněn přístup Defence-In-Depth [1]?		
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky?		
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik?		
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik, která respektují veřejný zájem (tj. mají sociální rozměr)?		
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik a cíle řízení rizik?		
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik a cíle řízení rizik s ohledem na veřejný zájem?		
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik, cíle řízení rizik s ohledem na veřejný zájem a nápravná opatření v monitoringu pro případ, že riziko se stane nepřijatelné?		
Je při práci s riziky technického díla systematicky určen a sledován soubor prioritních rizik?		
Zajišťuje technika řízení rizik technického díla v každé fázi práce s riziky přezkoumání přínosů a nákladů spojených s opatřeními na vypořádání rizik, aby se zajistilo hospodárné nakládání se silami, zdroji a prostředky technického díla?		
Zajišťuje technika řízení rizik technického díla v každé fázi práce s riziky přezkoumání přínosů a nákladů spojených s opatřeními na vypořádání rizik, aby se zajistilo hospodárné nakládání se silami, zdroji a prostředky technického díla a veřejné správy?		
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to jen některých?		
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech prioritních?		
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu?		
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu a nepřijatelné dopady na okolní životní prostředí?		
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení největších dopadů rizik, a to jen některých?		
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení rizik, a to všech prioritních?		
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení dopadů rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu?		
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení dopadů rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu a mít nepřijatelné důsledky pro okolní životní prostředí?		
Je technické dílo pojištěno pro případ realizace rizik?		
Má technické dílo rezervy finanční, materiální, technické, personální a organizační pro odezvu v případě realizace závažného rizika?		
Má technické dílo rezervy finanční, materiální, technické, personální a organizační pro obnovu v případě realizace závažného rizika?		
Má technické dílo rezervy finanční, materiální, technické, personální a organizační pro odezvu a obnovu v případě realizace extrémního neočekávaného rizika?		
Jsou při práci s riziky v technickém díle zohledněny jen výsledky předběžných analýz rizik?		
Jsou při práci s riziky v technickém díle upřednostněny výsledky standardních, rychlých a méně přesných analýz rizik před výsledky předběžných analýz rizik?		

Jsou při práci s riziky v technickém díle upřednostněny výsledky detailních analýz rizik v souhrnném kontextu před výsledky standardních, rychlých a méně přesných analýz rizik a před výsledky předběžných analýz rizik?		
Jsou při práci s riziky v technickém díle upřednostněny výsledky individuálních a specifických analýz rizik před výsledky detailních analýz rizik v souhrnném kontextu, standardních, rychlých a méně přesných analýz rizik a předběžných analýz rizik?		
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení?		
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení technické a ekonomické?		
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení technické a ekonomické, externí a interní?		
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení technické a ekonomické, externí a interní a sociálně – politické?		
Jsou při práci s riziky v technickém díle stanoveny požadavky pro zajištění bezpečnosti?		
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti?		
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti a dílčí cíle?		
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle a metody a postupy?		
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle, metody a postupy a také limity a podmínky?		
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle, metody, postupy, limity a podmínky, a kompetence osob či institucí?		
Má správce technického díla systém řízení bezpečnosti, který je postaven na zásadách procesního řízení a systematické práci s riziky?		
Má správce technického díla systém řízení bezpečnosti, který obsahuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v technickém díle a v okolním území?		
Má správce technického díla systém řízení bezpečnosti (SMS), který má proces řízení, který obsahuje šest procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií?		
Má SMS správce technického díla proces koncepce a řízení, který obsahuje podprocesy 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?		
Má SMS správce technického díla proces administrativní postupy, který obsahuje podprocesy 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?		
Má SMS správce technického díla proces technické záležitosti, který obsahuje podprocesy pro: výzkum a vývoj; projektování a montáže; inherentně bezpečnější procesy; technické standardy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů?		
Má SMS správce technického díla proces vnější spolupráce, který obsahuje podprocesy pro: spolupráci se správními úřady; spolupráci s veřejností a dalšími zúčastněnými (včetně akademických pracovišť); a spolupráci s dalšími podniky?		
Má SMS správce technického díla proces nouzová připravenost, který 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?		
Má SMS správce technického díla proces dokumentace a šetření havárií, který obsahuje podprocesy pro: zpracování zpráv o pohromách, haváriích, skoro nehodách a dalších poučných zkušenostech; vyšetřování škod, ztrát a újmy a jejich příčin; a odezvu a následné činnosti po pohromách (včetně aplikace poučení a sdílení informací)?		

Má SMS správce technického díla proces pro zabezpečení technického díla, který obsahuje podprocesy pro: fyzické zabezpečení; a kybernetické zabezpečení.		
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém jsou stanoveny role zúčastněných, pravidla pro zvyšování kultury bezpečnosti (tzv. zlatá pravidla) a příslušné odpovědnosti?		
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém jsou: bezpečnostní plány (strategická, taktická, operativní a technická úroveň); vnitřní a vnější nouzové plány, plány kontinuity a krizové plány?		
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi?		
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje jen technická rizika?		
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická a organizační rizika?		
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická, organizační a vnější rizika?		
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická, organizační, vnější a kybernetická rizika?		
Je v SMS zajištěn kvalitní monitoring integrálního rizika a závažných dílčích rizik a nápravná opatření pro případ nepřijatelných rizik?		
CELKEM		

Tabulka 12. Kontrolní seznam pro posuzování bezpečnosti technického díla na základě posouzení plánu řízeni rizik.

Otázka	**Odpověď**	
	ANO	**NE**
Je plán technického díla pro zvládnutí rizik veden jasnou představou a sledovanými cíli?		
Uplatňuje se v plánu technického díla pro zvládnutí rizik princip celistvosti (tj. uvážení prosperity sociálního, ekologického a ekonomického subsystému; vyjádření nákladů a užitků; dopadů a přínosů ekonomické aktivity pomocí peněžních i nepeněžních hodnot)?		
Jsou v plánu technického díla pro zvládnutí rizik zváženy podstatné elementy (např. spravedlivá dělba využívání zdrojů mezi současnou generací a generacemi budoucími; nadměrná spotřeba a chudoba; lidská práva; ekologické poměry podmiňující život; prosperita umožněná ekonomickým rozvojem a mimotržními činnostmi)?		
Má plán technického díla pro zvládnutí rizik přiměřený rozsah (např. vhodné měřítko času a prostoru)?		
Je plán technického díla pro zvládnutí rizik prakticky zaměřen (např. explicitně definované kategorie, které spojují vytyčenou představu s indikátory a kritérii; omezený počet klíčových cílů; omezený počet indikátorů; standardizovaný způsob měření a porovnávání; referenční hodnoty indikátorů, prahové hodnoty, vývojové trendy)?		
Je plán technického díla pro zvládnutí rizik otevřený (např. všeobecně přijaté metody a databáze; explicitní věrohodnost, vyloučení nejistoty)?		
Je v plánu technického díla pro zvládnutí rizik zahrnuta efektivní komunikace v zájmové společnosti?		
Podílí se na plánu technického díla pro zvládnutí rizik široká veřejnost?		
Počítá se v plánu technického díla pro zvládnutí rizik s následným posuzováním (např. upřesňování postupných cílů vlivem vývoje systému)?		
Jsou v plánu technického díla pro zvládnutí rizik zabezpečeny kapacity institucí (např. určení odpovědnosti za dodržení cílů rozhodovacího procesu, sběr a uchovávání údajů, dokumentace)?		
CELKEM		

7. ZÁVĚR

Prezentace v praxi ověřených kontrolních seznamů je příkladem nástrojů pro řízení rizik technických dílech, tj. podnicích, objektech, dílnách, zařízení apod. Je třeba uvést, že sestavení kontrolního seznamu vyžaduje experta s nejvyšší odborností na posuzovanou problematiku, v případě multioborového problému tým expertů z jednotlivých oborů. Naproti tomu aplikace kontrolního seznamu již vyžaduje pouze základní znalosti v oboru a schopnost rozpoznání odchylek od popisovaného stavu. Uživatel kontrolního seznamu postupuje otázku po otázce a odpovídá na ně podle předem určené hodnotové stupnice, ať už logické (ano/ne), nebo číselné. Popřípadě provede měření sledované veličiny. Výsledkem hodnocení je pak statistická hodnota, určená podle daného postupu. Kontrolní seznamy jsou vhodné pro posuzování rutinních systémů, kde pouze sledujeme odchylky od běžného stavu a není potřeba invence.

Respektováním postupů inženýrství zacíleného na permanentní řízení rizik ve prospěch bezpečnosti, které se opírá o permanentní hodnocení rizik formou kontrolních seznamů, lze zajistit zvládnutí:

- slabin v zabezpečení entity vůči vnějším vlivům,
- vnitřních náhodných poruch entity,
- vnitřních systémových poruch zařízení entity,
- poruch v procesech entity,
- lidských chyb,
- nedostatku zdrojů,
- konfliktů mezi požadavky na bezpečnost a zabezpečení,
- chybných nebo nedostatečné identifikovaných ovlivňujících činitelů,
- neodpovědnosti manažerů či personálu,
- nekompetence manažerů či kritického personálu,
- závislosti a nedůvěryhodnosti řešitelských subjektů.

Kvalita řízení rizik ve prospěch bezpečnosti entit a jejich okolí závisí jak na projektu, zhotovení a údržbě entity, tak na úrovni vzdělání a výcviku obsluhy entity, a proto jsou důležité provozní předpisy obsahující bezpečné postupy, opatření osobní ochrany a předpisy stanovující odezvu na nehody a havárie.

LITERATURA

[1] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364 p. Doi: 10.14311%2FBK.9788001061824.

[2] UN. *Human Development Report*. New York: UN 1994, www.un.org.

[3] EU. Maastricht Treaty (C 191, 29.7.1992, pp. 1–112) ve znění pozdějších předpisů

[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

[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] 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.9788 001066751

[9] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury.* ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.

[10] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.

[11] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů.* ISBN: 978-80-01-05771-1. Praha: ČVUT 2015, 208 p.

[12] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. Doi: 10.14311%2FBK.9788001066096

[13] PROCHÁZKOVÁ D. Projektování technických děl založené na řízení rizik.. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 49-69. Doi:10.14311/ BK.9788001069066
[14] PROCHÁZKOVÁ D., PROCHÁZKA, J. Tool for Risk-Based Operation of Socio-Cyber-Physical Systems. *International Journal of Economics and Management Systems*, 6 (2021), pp. 69-81. http:// www.iaras.org/iaras/journals/ijems
[15] PETROCHEM. *Loss Prevention.* PCHE – PetroChemEng, Praha 2004, ISBN 80-02-01574-6. CD ROM
[16] 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.
[17] ALE, B., PAPAZOGLOU, I., ZIO, E., eds. *Reliability, Risk and Safety*. ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448 p.
[18] BARALDI, P., DI MAIO, F., ZIO, E., eds. *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15).* ISBN 978 -981-14-8593-0. Singapore: ESRA, Research Publishing 2021, 5067 p., enquiries@rps online.com.sg
[19] BEER, M., ZIO, E., eds. *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* ISBN 978-981-11-2724-3. Singapore: ESRA, Research Publishing 2019, 4315 p., e:enquiries @rps online.com.sg
[20] BÉRENGUER, C., GRALL, A., GUEDES SOARES, C., eds. *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035 p.
[21] BRIŠ, R., GUEDES SOARES, C. & MARTORELL, S., eds. *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362 p.
[22] CASTANIER, B., CEPIN, M., BIGAUD, D., BERENGUER, C., eds. *Proceedings of the 31st European Safety and Reliability Conference* . ISBN 978-981-18-2016-8. Singapore: ESRA, Research Publishing 2021, 3473 p., enquiries@rpsonline.com.sg
[23] CEPIN, M., BRIS, R., eds. *Safety and Reliability – Theory and Applications*. ISBN 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.
[24] 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 (Handbook). London: Taylor & Francis Group 2018, 3234 p. https://www.ntnu.edu/esrel2018
[25] IAPSAM, eds. *Probabilistic Safety Assessment and Management Conference. International. 11th 2012. (and Annual European Safety and Reliability Conference)*. ISBN 978-1-62276-436-5. Helsinki: IPSAM & ESRA 2012, 6889 p.
[26] LEVA, M.C., PATELLI, E., PODOFILLINI, L., WILSON, S., eds. Proceedings of the 32nd European Safety And Reliability Conference (ESREL 2022). ISBN 978-981-18-5183-4. Singapore: ESRA, Research Publishing 2022, 3413 p., enquiries@rpsonline.com.sg
[27] NOWAKOWSKI, T., MLYŇCZAK, M., JODEJKO-PIETRUCZUK, A., WERBIŇSKA-WOJCIECHOWSKA, S., eds. *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453 p.
[28] PODOFILLINI, L., SUDRET, B., STOJADINOVIC, B., ZIO, E., KRÖGER, W., eds. *Safety and Reliability of Complex Engineered System*. ISBN 978-1-138-02879-1. London: CRC Press 2015, 4560 p.
[29] STEENBERGEN, R., VAN GELDER, P., MIRAGLIA, S., TON VROUWENVELDER, A., eds. *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387 p.
[30] WALLS, L., REVIE, M., BEDFORD, T., eds. *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL*. ISBN 978-1-315-37498-7. London: CRC Press 2016, 2942 p.
[31] PROCHÁZKOVÁ D., PROCHÁZKA, J. Generic Model for Safety Management o Critical Infrastructure Elements. In: *Proceedings of Scientific Works.* ISBN 978-80-973844-4-9. Bratislava: Slovak Society for Environment 2021, pp. 104-125.
[32] PROCHAZKOVA D. Generic Model for Management of Safety of Technical Installations Powered by Small Modular Reactors. *Design, Construction, Maintenance*. ISSN 2732-9984. 3 (2023), 1, pp. 7-12. Doi: 10.37394/232022.2023.3.
[33] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.
[34] EU. *FOCUS Project*. Brussels: EU 2012, http://www.focusproject.eu/documents /14976/-5d7 63378-1198-4dc9-86ff-c46959712f8a

[35] PROCHÁZKOVÁ, D. Charakteristiky inženýrství zacíleného na bezpečnost. In: *Řízení rizik procesů, zařízení a složitých technických děl zacílené na bezpečnost.* ISBN 978-80-01-07060-4. Praha: ČVUT DSPACE 2022, pp. 7-34. Doi:10.14311/BK.9788001070604

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

[37] DOSKOČIL, R., LACKO, B. Risk Management and Knowledge Management as Critical Success Factors of Sustainability Projects. Sustainability. *Sustainability.* ISSN 2071-1050, 10 (2018), 5, pp.1-13.

[38] DAVIDOVÁ, O., LACKO, B. Fuzzy Logic Control Application for The Risk Quantification of Projects for Automation, In: *Conference MENDEL 2015.* ISBN 180-33814. Brno: Mendelova universita 2015, pp. 213-216.

[39] COASE, R. H. The Problem of Social Cost. *Journal of Law and Economics,* 3 (1960), pp. 1-44.

[40] PROCHÁZKOVÁ D. *Databáze havárií a selhání technických děl a zařízení.* Praha: ČVUT 2023.

[41] PROCHÁZKOVÁ D., PROCHÁZKA, J. Optimální nástroj pro řízení rizik systémů závisí na jejich složitosti. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 355-367. DSPACE. doi.org/10.14311/ BK.97880 01069066

[42] PROCHÁZKOVÁ, D., ŠESTÁK, B. *Kontrolní seznamy*. ISBN 80-7251-225-0. Praha: PA ČR 2006, 319 p.

[43] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. ISBN: 978-80-01-04841-2. Praha: ČVUT 2011, 405 p.

[44] PROCHÁZKOVÁ, D. Posudky pro praxi. Praha: ČVUT 2023.

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

[46] PROCHÁZKOVÁ, D., PROCHAZKA, J. Checklist for Judgement of Technical Facility Safety and Results Obtained by Its Application in Practice. In: *Proceedings of International European Safety and Reliability Conference, ESREL2018*. ISBN 978-0-8153-8682-7 (Handbook). London: Taylor & Francis Group 2018; ISBN: 978-1-351-17466-4 (eBook); https://www.ntnu.edu/esrel 2018; pp. 1175-1184.

BEZPEČNOST A RESILIENCE PRŮMYSLOVÝCH KOMPLEXŮ POHÁNĚNÝCH MALÝM MODULÁRNÍM REAKTOREM

SAFETY AND RESILIENCE INDUSTRIAL COMPLEXES POWERED BY SMALL MODULAR REACTOR

Dana Procházková, Jan Procházka, Václav Dostál

České vysoké učení technické v Praze, Technická 4, 166 00 Praha 6, Česká republika, danuse.prochazkova@fs.cvut.cz

Abstrakt: V současné době je průmysl v České republice energeticky náročný a je jejím hnacím motorem rozvoje. Spolehlivou základnu rozvoje bude dále plnit jen tehdy, když bude bezpečný a konkurenceschopný. Proto současné problémy v energetice nutí podniky hledat další zdroje energie. Vzhledem k rostoucí dostupnosti i bezpečnosti malých modulárních reaktorů v předloženém článku navrhujeme v určitém území propojit průmyslové objekty s malým modulárním reaktorem. Tím se vytvoří velmi složité systémy, u kterých lze zajistit požadovanou výkonnost jen tehdy, když budou mít velkou resilienci. To znamená, že budou složené z bezpečných objektů a celek bude mít schopnost i za kritických podmínek provést rychle kvalifikovanou odezvu a udržet výkonnost na stanovené úrovni. Vzhledem k proměnnosti světa, je nutno bezpečnost i resilienci řídit. V článku uvádíme metodiku pro řízení bezpečnosti i resilience na konkrétním příkladu, který v praxi řešíme.

Klíčová slova: Energetická základna, průmyslové komplexy, SMR, rizika, bezpečnost, resilience, model řízení bezpečnosti a resilience.

Abstract: At present, industry in the Czech Republic is energy-exigent and is driving force for its development. It will only continue to provide a reliable basis for development if it is safe and competitive. Therefore, the current problems in the energy sector are forcing companies to look for other sources of energy. Due to the increasing availability and safety of small modular reactors in the present article, we propose to connect industrial facilities with a small modular reactor in a certain area. This will create very complex systems that can only be given the expected performance if they have high resiliency. This means that they will be composed of safe objects and the whole will be safe and have the ability to quickly perform a qualified response and maintain performance at a specified level even under critical conditions. With regard to the variability of the world, both, the safety and the resiliency must be managed. In the article, we present the methodology for safety and resiliency management on a real example that we solve in practice.

Key words: Energy base, industrial complexes, SMRs, risks, safety, resilience, safety and resilience management model.

1. ÚVOD

Průmysl je významné odvětví hospodářství vyspělých států. Aplikuje různé technologie, které přispívají k hospodářskému rozvoji a lidské prosperitě. Dodávky výrobků i služeb proto musí být kvalitní a bezpečné. Bezpečný provoz průmyslu vyžaduje jak suroviny, energii, dobře zvládnutou technologii, kvalifikovaný personál a kvalifikované řízení, tak opatření na snižování nepřijatelných dopadů, kterými jsou znečištění složek prostředí a škody na zdraví lidí, kteří pracují v nebezpečných provozech, a popř. v jejich okolí. Z ekonomického pohledu průmysl musí být také konkurenceschopný, a proto je vysoce závislý na disponibilních zdrojích.

V současné době dochází v Evropě k problémům v oblasti materiálových a energetických zdrojů, což provoz průmyslu vážně ohrožuje. V předloženém článku řešíme proto energetickou základnu pro provoz průmyslových závodů soustředěných v určitém území. Vzhledem k rozvoji a výhodám malých modulárních reaktorů (SMR) navrhujeme vkládat do území s průmyslovými závody malé modulární reaktory (SMR). V praxi to znamená vytváření složitých celků (systémů), kdy je v určitém území umístěna řada technologií poháněných SMR. Je skutečností, že každý technický objekt i SMR má svá omezení a navíc se vzájemně ovlivňují. Je však také skutečností, že od určitých podmínek se vzájemná ovlivnění stanou nežádoucí a nepřijatelná, a povedou k narušení výkonnosti celku.

Pro zajištění dostatečné výkonnosti průmyslového celku je třeba zajistit okamžitou odezvu a poté obnovu, aby nedošlo k problémům ve státě, které by mohly odstartovat problémy i v sociální oblasti. Aby se zabránilo velkým problémům, je třeba průmyslové komplexy poháněné SMR řídit tak, aby byly jak bezpečné, tak vysoce resilientní. Resilience znamená, že jsou rezistentní vůči poruchám a v případě poruchy mají schopnost rychle reagovat, udělat správná opatření odezvy a brzy se navrátit do původního stavu.

Resilience průmyslového komplexu poháněného SMR znamená seřídit složitý systém typu SoS (otevřený systém vzájemně provázaných otevřených systémů) tak, aby během provozu: byl robustní; redundantní; vynalézavý; a rychlý. Vložení předmětných vlastností zaručí optimální provoz průmyslového komplexu, tj. požadovanou úroveň bezpečnosti, výkonnosti a spolehlivosti. Protože podmínky pro provoz se z důvodů dynamického vývoje světa (tj. proměny vnitřních i vnějších podmínek) mění, a někdy i skokem, tak resilienci je třeba kvalifikovaně řídit.

Na základě současného poznání [1-14], řízení resilience průmyslových komplexů poháněných SMR musí být integrované a strategické. Jeho cílem je v průběhu času optimalizovat provoz komplexu tak, aby za všech podmínek, které musí být zvažovány v projektu, riziko celého komplexu i rizika jednotlivých částí komplexu byla přijatelná a aby nebyly tolerovány funkční poruchy v komplexu. Článek obsahuje návrh modelu řízení bezpečnosti i resilience průmyslových komplexů poháněných SMR na příkladu. Vychází modelů založených na řízení rizik ve prospěch bezpečnosti u jednotlivých průmyslových celků a stanovuje limity pro provoz jednotlivých celků tak, aby byla za všech projektových podmínek zachována resilience celého komplexu poháněného SMR.

2. ENERGETICKÁ NÁROČNOST PRŮMYSLOVÝCH KOMPLEXŮ

Dnešní lidská společnost požaduje stále více produktů a služeb, které zajišťují průmyslové komplexy, ve kterých je řada technologií. Z hlediska snížení nároků na dopravu jsou průmyslové komplexy dnes soustředěny do určitých území. Předmětná území jsou vysoce náročná jak na energii, tak na technicky zdatný personál. V České republice se v průmyslu ze zdrojů energie nejvíce využívá elektřina, následuje zemní plyn a tuhá fosilní paliva [15]. Obnovitelné zdroje se na pokrytí energetických potřeb tuzemského průmyslu podílejí pouze necelými 7 %. Skutečností je, že zdrojem pro velkou většinu energií zůstávají tradiční fosilní paliva, jejichž zdroje jsou v řadě průmyslových zemí Evropy omezené, a tudíž jsou závislé na dovozu. Navíc se státy Evropské unie se zavázaly k přechodu na bezemisní energetiku.

Mezi energeticky náročná odvětví patří výroba kovů včetně hutního zpracování, chemický průmysl, výroba minerálních produktů, zpracování nekovových materiálů, strojírenství, sklářská a keramická výroba, výroba papíru, buničiny a tisk, které se na celkové konečné spotřebě paliv a energií v průmyslu podílejí dohromady téměř 70; energeticky náročný je pak i potravinářský. Dle statistik Eurostatu [16] tyto sektory pokrývají 95 procent celkové spotřeby průmyslu. Ačkoliv se předmětné provozy stále více zdokonalují a s tím souvisí, tak potřebují energii.

Energetická náročnost české ekonomiky, tj. spotřeba energie na jednotku HDP [17], je vysoká. Je dvojnásobná ve srovnání s Dánskem a dokonce o 40 % vyšší než v Německu. Vysoká energetická náročnost automaticky neznamená, že máme problém. V USA je náročnost ekonomiky ještě o cca 10 % vyšší než v ČR. Rozdíl je v soběstačnosti. Zatímco naše energetická soběstačnost je na 63 %, USA jsou dokonce na 104 %. USA vyrobí více energie, než potřebují. My musíme 37 % spotřebované energie dovézt. Jinými slovy se strukturou naší ekonomiky musí být ekonomickým zájmem ČR energetická soběstačnost a energetická bezpečnost.

Česká republika dováží především minerální paliva: ropu, plyn a uhlí. Za prvních sedm měsíců 2021 roku jsme byli čistými dovozci uhlí (nakoupili jsme je v zahraničí) ve výši cca 2 mld. Kč. V roce 2022 ve stejné době (leden–červenec) jsme nakoupili uhlí cca za 11 mld. Kč, tj. 5× více. Za ropu jsme vloni zaplatili 52 mld. Kč, letos 95 mld. Kč, tj. 2× více. Plyn jsme nakoupili vloni za 28 mld. Kč, letos za 128 mld. Kč tj. 4,6× více. Čisté dovozy minerálních paliv částečně kompenzoval čistý vývoz elektřiny, který stoupl ze 7 mld. Kč, v uvedeném období roku 2021 na 38 mld. Kč ve stejném období roku 2022. Celková bilance znamená zvýšení z -75 mld. Kč na -196 mld. Kč [15].

Např. studie pro ČR [18] uvádí, že největší prostor pro úspory je hlavně v organizačních opatřeních a důsledném energetickém managementu, tedy instalaci nebo zdokonalení řídících systémů a monitoringu. Zlepšit by se měla energetická efektivnost výroby a distribuce tepla. Mezi další opatření patří omezení tepelných ztrát v průmyslových budovách. Rezervy by v podnicích měl najít energetický audit. Podle této studie má největší příležitost ke snížení energetické náročnosti potravinářský průmysl, a to asi o 32 procent, v sektoru těžkého průmyslu je odhad poklesu mezi 14 a 18%.

Pro ministerstvo průmyslu [19] je zabezpečení dostatku energie a její efektivní využití s minimálním dopadem na životní prostředí největší výzvou, před níž stojí v 21. století. Od r. 2015 vydalo řadu vyhlášek a pokynů ke

snižování energetické náročnosti, zajistilo vzdělávací programy a dotační projekty v tomto směru. Jde však o běh na dlouhou trať. Pro podporu rozvoje našeho státu, potřebujeme řešení dostupné a rychlé, které spočívá v zajištění dostatečného množství energie pro náš průmysl. Je zapotřebí bezpečný, trvanlivý a levný zdroj.

Takovým zdrojem jsou malé modulární reaktory (SMR) [20,21], které byly testovány v ponorkách a na ledoborcích. Jejich projekty založené na rizicích (risk-based design) sledujeme [22] a jejich bezpečný provoz musí být regulován mezinárodními bezpečnostními normami, které připravuje MAAE. Výběr SMR závisí na nabídce na trhu; v současné době nejsou komerční SMR IV. generace stále k dispozici. Výhodou České republiky je vysoká technická vzdělanost populace i zkušenost s provozováním jaderných elektráren.

3. BEZPEČNOST A RESILIENCE PROPOJENÝCH SLOŽITÝCH SYSTÉMŮ

Analýza odborné literatury [1-14,23-30] ukazuje, že mezi odborníky je nejednotnost v konceptech pro kvalitní řízení entit zacílené na bezpečnost a výkonnost. V některých pracích, např. [24] se tradiční koncept bezpečnosti nazývá Safety-I a pro použití ve složitých sociotechnických systémech se doporučuje používat koncept Safety-II a inženýrství odolnosti, protože mají praktické přístupy; je v nich zdůrazněna role připravenosti, odezvy a obnovy. V jiných pracích [1-14,31], které řeší problematiku těsně spojených systémů, ve kterých zvažují různé technologie, organizační řízení i automatické řízení se klade důraz na řízení výkonosti, přičemž jde o ovládání rizik spojených s nelineárními, nepřímými a zpětnými vazbami. Při řešení praktických úloh však nestačí teoretické představy a modely, ale je třeba praktické řešení, které také splňuje požadavky platné legislativy. Legislativa požaduje bezpečnost a ekonomika požaduje výkonnost. Protože cíle jsou v mnoha případech konfliktní, je třeba najít oblast souladu, a v ní průmyslový komplex provozovat.

Od 90. let je bezpečnost považována za základní znak kvality systému [32,33]. Je budována pomocí technických a jiných norem a standardů, které zajišťují, že systémy jsou odolné vůči projektovým pohromám. Jelikož bezpečnost systému závisí na odolnosti systému, která je daná limitami, které jsou v projektu, pro: strukturu a formu složení prvků systému; formu, směr a intenzitu vazeb systému; formu, směr a intenzitu toků systému; a vytvoření nových či ztrátu nebo závažnou změnu interdependences, tj. vazeb napříč systému a jeho okolí, tak změna podmínek vede často k narušení prvků či vazeb systému či vzniku nežádoucích interdependencích, které naruší požadovanou úroveň bezpečnosti systému.

Vzhledem ke složitosti průmyslových komplexů [23,34] je třeba při návrhu a provozu sledovat a řídit specifické vlastnosti, jako jsou:

- interoperabilita (tj. schopnost průmyslového komplexu jako celku provádět úkoly v oblasti bezpečnosti a výkonnosti za běžných, abnormálních a kritických podmínek),
- integrita bezpečnosti (SIL), která je většinou sledována ve spojení s lidskými chybami (při specifikaci, návrhu, instalaci, údržbě, úpravě atd.),
- kritičnost (tj. rozsah, v jakém může dojít ke zranění osob, materiálnímu zničení, škodě nebo jiným ztrátám majetku – prahová hodnota, pod kterou je požadován stav sledovaného zařízení a naopak),
- spolehlivost (provozní spolehlivost), která zajišťuje, že systém splňuje stanovené požadavky a jeho provoz splňuje stanovené podmínky (rozšiřuje se na dvě základní charakteristiky, kterými jsou zranitelnost a trvanlivost a další charakteristiky.

Existují tři prioritní pokyny, jejichž faktory je třeba sledovat při ochraně pracovníků technických zařízení: provádí účinný způsob ochrany člověka, prováděná ochrana životního prostředí stanovené limity a podmínky pro provoz sledovaného zařízení.

Protože vzhledem k dynamickému vývoji světa, se mění velikost rizik a vznikají nová rizika, tak je nutno řídit rizika. Odolnost systému je daná projektem systému a její zvyšování technickými opatřeními při provozu lze dosáhnout jen v malém rozmezí [23,34]. Proto při provozu systému je třeba snižovat úroveň zranitelnosti a zvyšovat odolnost také organizačními opatřeními a vzdělaností. To znamená řídit rizika v čase tak, aby byla zajištěna požadovaná úroveň bezpečnosti a zajištěna požadovaná výkonnost systému.

Koncept [35] přinesl velký pokrok v zajišťování bezpečnosti průmyslovýh objektů. V práci [34] byl na jeho základě a poznatků z praxe vytvořen model řízení rizik objektu, který je složitým systémem, ve prospěch integrální bezpečnosti, založený na integrovaném řízení šesti procesů a jejich podprocesů, který byl později doplněn o proces, kterým se zajišťuje fyzické a kybernetické zabezpečení objektu [36].

Jestliže propojíme několik různorodých objektů ve formě složitých systémů, tak vzniká problém řízení, protože zranitelnosti a odolnosti jednotlivých objektů vůči pohromám všeho druhu obvykle nejsou stejné. Proto je zřejmé,

že zajištění požadované výkonnosti a řízení bezpečnosti celku skládajícího se z různorodých objektů ve formě složitých systémů není jednoduché; každý objekt platí jisté limity a podmínky dané projektem, které nejsou stejné. Proto se nabízí použít také koncept řízení pružné odolnosti. Resilience nebo spíše odolná výkonnost (resilient performence) je o tom, jak objekt funguje a ne o tom, jak je bezpečný.

Resilience (houževnatost) systému vyjadřuje potenciál systému, který spočívá ve specifickém uspořádání systému, které udržuje funkce a zpětné vazby systému, které zahrnují schopnost systému reorganizovat se na základě změn vyvolaných poruchami [23]. Řízení odolnosti je proces integrace všech ochranných činností organizace do jedné, jasné struktury řízení [23]. Má dva cíle: zabránit tomu, aby se objekt dostával do nežádoucích stavů v důsledcích vnějších poruch a vnější zátěže; a uchovat prvky aktivující systémovou reorganizaci a obnovu v důsledku masivních změn. Zpravidla se realizuje ve třech krocích, tj.:

1. Resilience koho, čeho? Navrhuje se konceptuální model objektu na základě specifických otázek: Jaké jsou prostorové hranice objektu?; Jaké jsou klíčové systémové služby využívané v objektu?; Jaké jsou zainteresované skupiny?; Jaké jsou klíčové složky objektu, jak se charakterizují, jaký je jejich význam a dynamika?; Jaký je historický profil objektu?; Jaké systémové proměnné působí jako hybné síly klíčových systémových služeb a produktů?; Které faktory jsou kontrolovatelné a zvladatelné?
2. Resilience vůči čemu? (scénáře). Analyzují se vnější poruchy a rozvojové procesy (procesy udržitelného rozvoje) a popisují se žádoucí uspořádání, která jsou resilientní. Scénáře se musí vyhnout především nekontrolovatelným a víceznačným vnějším hybným silám.
3. Analýza resilience. Zkoumají se interakce mezi vnějším působením a resilientními složkami a zjišťují se procesy v objektu, které ovládají dynamiku objektu. Klíčovým prvkem analýzy resilience je určení prahové hodnoty.

Prahová hodnota charakterizuje situaci, v níž se objekt vyskytuje mezi alternativními stavy rovnováhy, jež mohou, ale nemusí být vratné, tj. odděluje různé stabilní stavy. Prahové hodnoty nejsou konstantní, protože souvisí často s resiliencí a zranitelností. Výběr prahové hodnoty pro konkrétní objekt často závisí na hodnotách a preferencích [23].

4. METODA ŘÍZENÍ BEZPEČNÝCH A RESILIENTNÍCH PRŮMYSLOVÝCH KOMPLEXŮ

Na základě požadavků legislativy a pro zajištění požadované výkonnosti průmyslové komplexy musí být bezpečné a resilientní. Zajištění obou vlastností znamená, že řízení průmyslového komplexu musí mít nástroje pro řízení rizik v čase, které zajistí jak bezpečnost (což zahrnuje i spolehlivost), tak resilientní výkonnost.

Inženýrské techniky pro zajištění spolehlivosti, bezpečnosti a houževnatosti systému jsou založené na řízení rizik.. Cíle řízení rizik nejsou však u jmenovaných disciplín stejné a s jejich naplňováním je spojena řada náhodných i znalostních nejistot. Proto rozhodování o nich vyžaduje aplikaci zásad systémové analýzy. Je nutno používat multikriteriální hodnocení položek, které určují chování průmyslového komplexu z řady oblastí, které nejsou jednoduše souměřitelné.

V praxi se osvědčil koncept Multiatribute Utility Theory [37], která umožňuje stanovit číselné hodnoty souhrnné funkce užitku (nebo integrálního rizika) pro danou kombinaci položek. Výsledkem aplikace předmětné teorie jsou systémy pro podporu rozhodování(DSS), které jsou nástrojem řízení sledované entity.

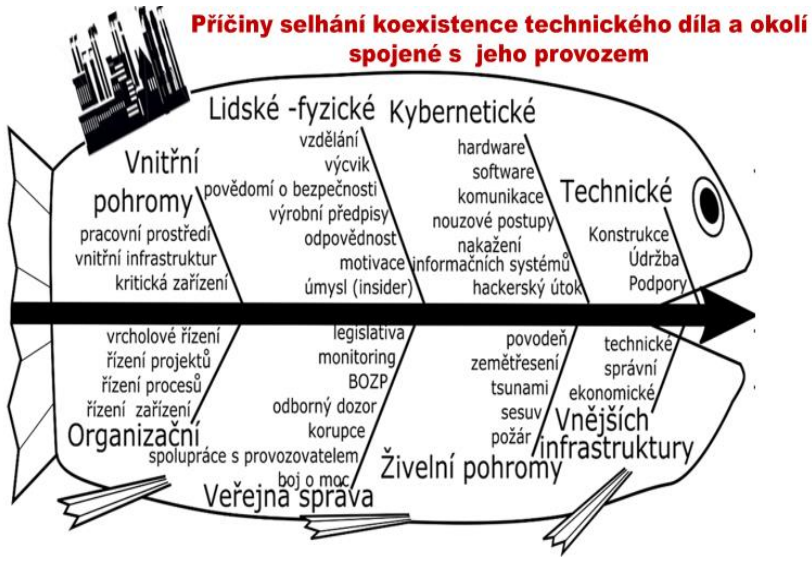
Již při samotném řízení bezpečnosti složitých entit je nutno vzhledem ke složitosti používat k rozhodování o rizicích ve prospěch bezpečnosti systém pro podporu rozjhodování [23,40]. Když pro průmyslový komplex složený z bezpečných entit požadujeme, aby byl bezpečný a resilientní, tak musíme opět použít zásady systémové analýzy s cílem najít takové podmínky provozu celku a jeho částí, při kterých také celý komplex je bezpečný a resilientní. Jelikož jde opět o hodnocení řady nesouměřitelných položek, tak je třeba opět vytvořit systém pro podporu rozhodování o rizicích pro úroveň řízení řízení celého průmyslového komplexu.

Zkušenosti z praxe [23,40] ukazují, že pro rychlé a kvalitní řešení problémů odezvy na nežádoucí situace v jednotlivých podnicích i v průmyslovém komplexu je třeba také sestavit plány řízení rizik [38,39], ve kterých se zvažují prioritní rizika dané entity, která nebylo možno vypořádat opatřeními v projektu a která mají potenciál vážně poškodit entitu anebo až celek, a plány obnovy [23].

Dále na příkladu uvedené DSS pro řízení bezpečnosti i resilience složitého průmyslového komplexu.

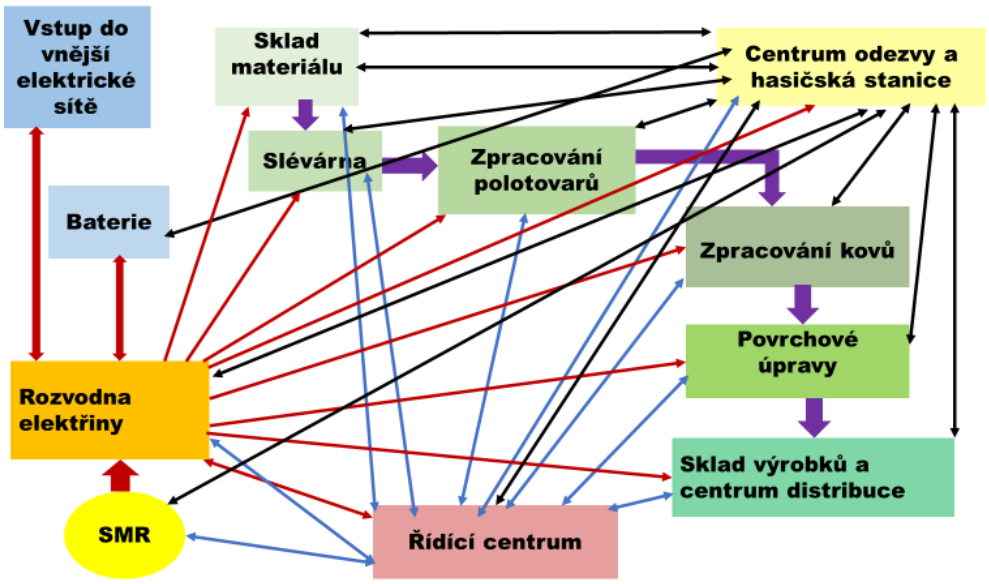
5. DATA PRO PRŮMYSLOVÝ KOMPLEX POHÁNĚNÝ SMR

Analýza a podrobné studium 7289 havárií a selhání technických děl [23] ukázaly: zdroje rizik zobrazené na obrázku 1; příčinami havárií a selhání jsou v 80% kombinace několika zdrojů rizik; vysoce zranitelné jsou propojení mezi prvky, a to nejen ty, které jsou úmyslně vložené, ale hlavně ty, které vznikají neplánovaně za určitých podmínek a s nimiž se v projektu nepočítalo. Z logické úvahy vyplývá, že čím složitější je objekt, tak existuje tím více možností propojení, která nejsou zvažována v projektu. Zvlášť velké nebezpečí vzniká v případech, kdy propojujeme existující objekty do nějakého složitého komplexu.



Obr.1. Základní kategorie zdrojů rizik spojených s provozem technických děl, které vedou k selhání koexistence technického díla s okolím během jeho provozu.

Abychom v současné době zajistili ekonomicky přijatelnou energetickou základnu pro český průmysl, tak plánujeme budovat průmyslové celky poháněné SMR. Na obrázku 2 je modelový příklad jednoho z celků, který je v přípravě. Místně specifické zdroje rizik, jejich velikosti a četnosti výskytu, velikosti jejich maximálních dopadů na území, ve kterém je umístěn sledovaný průmyslový komplex jsou v dokumentu [40].



Obr. 2. Model sledovaného komplexního objektu. Červené šipky označují přenos energie; fialové šipky označují výrobní proces; modré šipky označují procesy řízení; a černé šipky označují vybudovaná propojení pro stav nouze; data v [40].

Sledovaný komplex obsahuje vysoce energeticky náročné provozy jako jsou: slévárna (cca 4 GW); zpracování kovů (cca 4 GW); a povrchové úpravy (cca 4 GW); celkově je požadavek na výkon 20 GW.

6. NÁSTROJ PRO ŘÍZENÍ VYBRANÉHO PRŮMYSLOVÉHO KOMPLEXU, KTERÝ ZAJIŠŤUJE BEZPEČNOST A RESILIENCI

Při integrovaném řízení bezpečnosti i resilience předmětného systému je nutné zvážit fakta a požadavky legislativy jako:

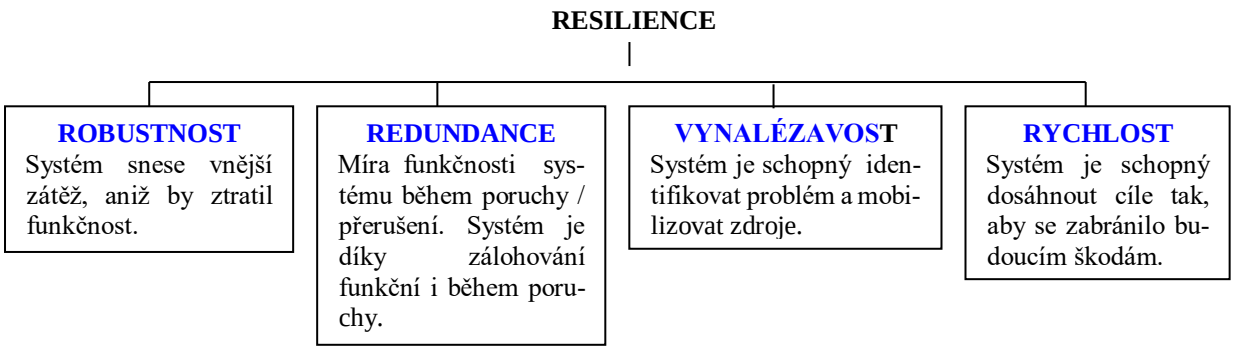
- bezpečnost provozu SMR závisí jednak na jeho risk-based design a jednak na risk-based operation, což vyžaduje požadavek na plynulost a dlouhodobou stabilitu výkonu [23],
- pracovní proces průmyslových celků má střídavý řád (např. dvousměnný provoz, volné soboty a neděle, přestávky na dovolenou) [40],
- odstávky jednotlivých provozů nelze vyloučit např. z hlediska údržby [40],

a to přináší další problém do tak složitého řízení průmyslového celku. Proto z hlediska udržitelnosti je třeba pro zajistit vysokou odolnost průmyslového celku. Proto pro zajištění resilience průmyslový celek obsahuje nejen specifická zařízení, a to: centrum odezvy; úložiště přebytečné energie; a propojení na vnější síť, ale i vysoké požadavky na spolupráci všech zúčastněných.

Z hlediska řízení odolnosti sledovaného celku, které má zajistit stabilní výkonnost průmyslového celku a zabránit kontaminaci prostředí radioaktivními nebo toxickými látkami, jde o nastavení požadavků na:

- vysokou bezpečnost provozu SMR, protože jde nejen o výkon, ale i o prevenci úniku radioaktivních a toxických látek,
- vysokou bezpečnost provozu řídícího centra a vazby mezi řídícím centrem a SMR, protože jde nejvyšší úroveň řízení celku, na které závisí nejen výkonnost průmyslového celku, ale i prevence úniku radioaktivních a toxických látek,
- vysokou bezpečnost: provozu centra odezvy; vazby mezi řídícím centrem a centrem odezvy; a vazby mezi SMR a centrem odezvy, protože jde o druhou úroveň řízení celku, na které závisí nejen výkonnost průmyslového celku, ale i prevence úniku radioaktivních a toxických látek,
- bezpečný provoz dílčích částí i ostatních dílčích vazeb, které jsou důležité pro výkonnost jak jednotlivých celků, tak celého provozu,
- nastavení limitů pro provoz u dílčích částí tak, aby výkon celku byl za normálních a abnormálních podmínek bezpečný a plynulý,
- připravenost a provedení odezvy na všechny očekávané kritické podmínky, které naruší výkonnost celku tak, aby se zajistila vnitřní schopnost celku udržet nebo znovu získat stabilní stav.

Cílem řízení bezpečnosti i resilience celku skládajícího se z různorodých objektů ve formě složitých systémů je cíl najít takové prahové hodnoty pro jednotlivé objekty a takový způsob spolupráce řízení jednotlivých objektů, které zajistí vlastnosti celku, kterými jsou: robustnost; redundance; vynalézavost; a rychlost nastartování správné odezvy v případě potřeby, obrázek 3 [23]. Z pohledu řízení celku skládajícího se z různorodých objektů ve formě složitých systémů je třeba, pro každý objekt určit limity a podmínky pro provoz takové, aby: selhání jednoho objektu nenarušilo provoz ostatních objektů a aby selhání bylo co nejkratší.



Obr. 3. Souvislosti resilience (houževnatosti) systému s robustností, redundancí, vynalézavostí a rychlostí.

Na základě znalostí a zkušeností, shrnutých v práci [23,40] pro každou položku vyznačenou na obrázku 2 jsou vytvořeny systémy pro podporu rozhodování o rizicích položek zobrazených na obrázku 2 s ohledem na bezpečnost a resilienci. Odpovědi na kritéria posuzujících stav pro očekávané scénáře provozu jsou oklasifikovány stupnicí 0 - 5 a dle konceptu „čím vyšší hodnota, tím je vyšší riziko“ [37]. Hodnocení kritérií dělá tým specialistů nezávisle z různých oborů. V daném případě používáme tým:

- pracovník veřejné správy odpovědný za bezpečnost území,
- pracovník veřejné správy odpovědný za dozor nad provozem technických děl,
- pracovník technického díla, odpovědný za řízení rizik,
- pracovník technické inspekce,
- pracovník SÚJB
- a pracovník Integrovaného záchranného systému, který odpovědného za odezvu na havárie a selhání technických děl.

Výsledná hodnota u každého kritéria je medián, přičemž v případě velkého rozptylu hodnot u některého kritéria je třeba, aby pracovník veřejné správy odpovědný za bezpečnost území zajistil další šetření, na kterém každý hodnotitel sdělí zdůvodnění svého hodnocení v předmětném případě a na základě panelové diskuse nebo brainstormingu se určí výsledné hodnocení. Pro vyhodnocení celkového rizika jednotlivých položek použijeme stupnici uvedenou v tabulce 1.

Tabulka 1. Hodnotová stupnice pro určení míry rizika položky a jejího okolí; N = pětinásobku počtu kritérií v systému pro podporu rozhodování dané položky.

Míra rizika	**Hodnoty v % N**
Extrémně vysoká – 5	Více než 95 %
Velmi vysoká – 4	70–95 %
Vysoká – 3	45–70 %
Střední - 2	25–45 %
Nízká – 1	5–25 %
Zanedbatelná – 0	Méně než 5 %

Podle zjištěných hodnot rizika se výsledky posouzení rizik u položek rozdělují do tří skupin: přijatelné riziko – kategorie 0 a 1; riziko ALARA, tj. podmíněně přijatelné – kategorie 2 a 3; a riziko nepřijatelné – kategorie 4 a 5.

Z důvodů prevence úniku radioaktivních a toxických látek a zachování schopnosti odezvy označujeme míru rizika u 10 vybraných položek komplexu červeně, a to u zdrojů rizik, které zapříčiní:

- vznik organizační havárie průmyslového komplexu,
- selhání řízení průmyslového komplexu,
- selhání propojení mezi centrem řízení a SMR,
- selhání SMR,
- selhání přenosu energie mezi SMR a rozvodnou sítí elektřiny,
- selhání rozvodny elektřiny,
- selhání centra odezvy,
- selhání nouzového spojení mezi centrem odezvy a centrem řízení,
- selhání nouzového spojení mezi centrem odezvy a SMR,
- selhání nouzového spojení mezi centrem odezvy a rozvodnou stanicí elektrické energie.

V těchto případech vkládáme do systému zálohy tak, aby vždy příslušná rizika byla zanedbatelná. U ostatních položek připouštíme rizika patřící do kategorie ALARA.

S cílem zajistit výkonnost jednotlivých objektů zpracováváme plány řízení rizik, které obsahují:

- zdroje rizik,
- dopady rizik,
- velikost a četnost výskytu jednotlivých rizik,
- připravená opatření, vykonavatele opatření a osobu odpovědnou za kvalitní a včasné provedení opatření.

Tím se zajistí nejen rychlé a kvalitní odezvy, ale sníží se doby výpadků na minimum, a tím i možnost nepřijatelného ovlivnění ostatních položek. To znamená, že se posílí i resilience průmyslového komplexu.

Výsledné hodnoty integrálních rizik pro očekávané scénáře provozu položek dáme do tabulky 2. Hodnocení kritérií děláme stejným způsobem jako u systémů pro podporu rozhodování u dílčích položek s tím, že u 11 vybraných položek (vyznačených červeně) použijeme váhu 2.

Tabulka 2. Systém pro podporu rozhodování průmyslového komplexu

Kritérium	**Hodnocení**
Míra rizika výskytu organizační havárie průmyslového komplexu	
Míra rizika řídícího centra	
Míra rizika komunikačního a informačního propojení řídícího centra a objektu se SMR	
Míra rizika komunikačního a informačního propojení mezi řídícím centrem a skladem materiálu	
Míra rizika komunikačního a informačního propojení mezi řídícím centrem a slévárnou	
Míra rizika komunikačního a informačního propojení mezi řídícím centrem a objektem na zpracování polotovarů	
Míra rizika komunikačního a informačního propojení mezi řídícím centrem a objektem na zpracování kovů	
Míra rizika komunikačního a informačního propojení mezi řídícím centrem a objektem, ve kterém se provádí povrchové úpravy	
Míra rizika komunikačního a informačního propojení mezi řídícím centrem a skladem výrobků a centrem distribuce	
Míra rizika komunikačního a informačního propojení mezi řídícím centrem a rozvodnou elektřiny	
Míra rizika objektu SMR	
Míra rizika dodávání elektrické energie z objektu SMR do rozvodny elektřiny	
Míra rizika přenosu energie z rozvodny elektrické energie do baterií	
Míra rizika přenosu elektrické energie z rozvodny elektřiny do vnější sítě	
Míra rizika centra odezvy a hasičské stanice	
Míra rizika přenosu elektřiny z rozvodny elektřiny do centra odezvy a hasičské stanice	
Míra rizika rozvodny elektřiny	
Míra rizika přenosu elektrické energie z rozvodny elektřiny do skladu materiálu	
Míra rizika přenosu elektrické energie z rozvodny elektřiny do slévárny	
Míra rizika přenosu elektrické energie z rozvodny elektřiny do objektu na zpracování polotovarů	
Míra rizika přenosu elektrické energie z rozvodny elektřiny do objektu na zpracování kovů	
Míra rizika přenosu elektrické energie z rozvodny elektřiny do objektu, ve kterém se provádí povrchové úpravy	
Míra rizika přenosu elektrické energie z rozvodny elektřiny do objektu, ve kterém je sklad výrobků a centrum distribuce	
Míra rizika spojená s provozem skladu materiálu	
Míra rizika procesu přesunu materiálu ze skladu materiálu do slévárny	
Míra rizika spojená s provozem slévárny	
Míra rizika procesu přesunu polotovaru do objektu na zpracování polotovarů	
Míra rizika spojená s provozem objektu na zpracování polotovarů	
Míra rizika procesu přesunu produktu z objektu na zpracování polotovarů do objektu na zpracování kovů	
Míra rizika spojená s provozem objektu na zpracování kovů	
Míra rizika procesu přesunu produktu z objektu na zpracování kovů do objektu, ve kterém se provádí povrchové úpravy	
Míra rizika spojená s provozem objektu, ve kterém se provádí povrchové úpravy	
Míra rizika procesu přesunu produktu z objektu, ve kterém se provádí povrchové úpravy do skladu výrobků a centra distribuce	
Míra rizika spojená s provozem objektu, ve kterém je sklad výrobků a centrum distribuce	
Míra rizika nouzového propojení mezi řídícím centrem a centrem odezvy a hasičskou stanicí	
Míra rizika nouzového propojení mezi objektem se SMR a centrem odezvy a hasičskou stanicí	
Míra rizika nouzového propojení mez rozvodnou elektřiny a centrem odezvy a hasičskou stanicí	
Míra rizika mezi nouzového propojení mezi objektem s bateriemi a centrem odezvy a hasičskou stanicí	

Míra rizika mezi nouzového propojení mezi skladem materiálu a centrem odezvy a hasičskou stanicí	
Míra rizika mezi nouzového propojení mezi slévárnou a centrem odezvy a hasičskou stanicí	
Míra rizika mezi nouzového propojení mezi objektem, ve kterém se zpracovávají polotovary a centrem odezvy a hasičskou stanicí	
Míra rizika mezi nouzového propojení mezi objektem, ve kterém se provádí zpracování kovů a centrem odezvy a hasičskou stanicí	
Míra rizika mezi nouzového propojení mezi objektem, ve kterém se provádí povrchové úpravy a centrem odezvy a hasičskou stanicí	
Míra rizika mezi nouzového propojení mezi skladem výrobků a centrem distribuce a centrem odezvy a hasičskou stanicí	
Celkem	

Na základě hodnot integrálního rizika pro různé scénáře integrovaného řízení chování průmyslového komplexu vybíráme scénáře provozu průmyslového komplexu, které jsou ALARA a zároveň jsou ekonomicky přijatelné. Na základě těchto scénářů stanovujeme požadavky na řízení a sestavujeme provozní předpisy pro normální, abnormální i kritické podmínky, a to na všech organizačních úrovních.

Pro potřeby řízení zavádíme monitoringy prioritních rizik a monitoringy stavu zařízení, komponent a kritického personálu, a to na všech organizačních úrovních. Řízení personálu zaměřujeme na zvyšování kultury bezpečnosti a na získávání schopnosti umět předvídat budoucí chování položek důležitých pro bezpečnost a resilienci a umět nasadit správná opatření odezvy včas. Proto pro zajištění kvalitní odezvy pro celý průmyslový komplex připravujeme pro možné scénáře chování průmyslového komplexu plány řízení rizik a podle české legislativy i plány krizové připravenosti - Nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).

7. ZÁVĚR

V průmyslové praxi je důležitá jak bezpečnost, tak resilience objektů. Pro jejich zajištění je třeba vnímat řízení objektů i celých průmyslových komplexů jako dynamický proces, který k dosažení svých cílů se neustále přizpůsobuje tak, aby kvalitně reagoval na změny uvnitř i vně průmyslového komplexu. Jelikož cíle označené jako bezpečnost a výkonnost nejsou souměřitelné, tak je třeba použít multikriteriální přístupy založené na užitku.

V předloženém příkladu je nesplnění cílů průmyslového komplexu je považováno za selhání procesů, které zahrnují interakce mezi lidmi, organizačními strukturami, inženýrskými činnostmi a fyzickými a kybernetickými komponentami. Během provozu jsou důležité zpětné vazby na okamžité podmínky. Základní zpětné vazby jsou vloženy do risk-based desigs položek. Zkušenost z provozu technických děl ukazují, že v důsledku dynamických změn světa je však třeba během provozu odstraňovat zastaralé reakce a nahrazovat je novými, které jsou efektivní. Proto je důležité mít plán řízení rizik, které jsou aktualizovány pravidelně, anebo po každém kritickém stavu průmyslového komplexu.

Poděkování: Autoři děkuji za podporu projektu TAČR TK05010146

LITERATURA

[1] BRIŠ, R., GUEDES SOARES, C. & MARTORELL, S., eds. *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362 p.

[2] ALE, B., PAPAZOGLOU, I., ZIO, E., eds. *Reliability, Risk and Safety.* ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448 p.

[3] BÉRENGUER, C., GRALL, A., GUEDES SOARES, C., eds. *Advances in Safety, Reliability and Risk Management.* ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035 p.

[4] IAPSAM, eds. *Probabilistic Safety Assessment and Management.* (Conference International 11th 2012 (and Annual European Safety and Reliability Conference). ISBN: 978-1-62276-436-5. Helsinki: IPSAM & ESRA 2012, 6889 p.

[5] STEENBERGEN, R., VAN GELDER, P., MIRAGLIA, S., TON VROUWENVELDER, A., eds. *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387 p.
[6] NOWAKOWSKI, T., MLYŇCZAK, M., JODEJKO-PIETRUCZUK, A., WERBIŇSKA-WOJCIECHOWSKA, S., eds. *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453 p.
[7] PODOFILLINI, L., SUDRET, B., STOJADINOVIC, B., ZIO, E., KRÖGER, W., eds. *Safety and Reliability of Complex Engineered System*. ISBN 978-1-138-02879-1. London: CRC Press 2015, 4560 p.
[8] WALLS, L., REVIE, M., BEDFORD, T., eds. *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL.* ISBN 978-1-315-37498-7. London: CRC Press 2016, 2942 p.
[9] CEPIN, M., BRIS, R., eds. *Safety and Reliability – Theory and Applications*. ISBN: 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.
[10] 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.; ISBN: 978-1-351-17466-4 (eBook); https://www.ntnu.edu/esrel2018.
[11] BEER, M., ZIO, E., eds. *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* ISBN 978-981-11-2724-3. Singapore: ESRA, Research Publishing 2019, 4315 p., e:enquiries @rps online.com.sg
[12] BARALDI, P., DI MAIO, F., ZIO, E., eds. *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference* (ESREL2020 PSAM15). ISBN 978 -981-14-8593-0. Singapore: ESRA, Research Publishing 2020, 5067 p., enquiries@rps online.com.sg
[13] CASTANIER, B., CEPIN, M., BIGAUD, D., BERENGUER, C., eds. *Proceedings of the 31st European Safety and Reliability Conference*. ISBN 978-981-18-2016-8. Singapore: ESRA, Research Publishing 2021, 3473 p., enquiries@rpsonline.com.sg
[14] LEVA, M.C., PATELLI, E., PODOFILLINI, L., WILSON, S. *Proceedings of the 32nd European Safety And Reliability Conference (ESREL 2022)*. ISBN 978-981-18-5183-4. Singapore: ESRA, Research Publishing 2022, 3413 p., enquiries@rpsonline.com.sg
[15] CSU (2022). *Archiv*. https://www.czso.cz
[16] EU (2022). *Archiv*. https://ec.europa.eu
[17] CSSI (2021). *Archiv*. https://www.casopisstavebnictvi.cz
[18] EKO (2020). *Archiv*. www.enviweb.cz
[19] MPO (2022). *Archiv*. https://www.mpo.cz
[20] ARIS. *Advances in Small Modular Reactor Technology Developments*. Vienna: IAEA 2020 (ARIS).
[21] PANNIER, C. P., SKODA, R. Comparison of Small Modular Reactor and Large Nuclear Reactor Fuel Costs. *Energy and Power Engineering.* 6 (2014), 4, pp. 82-94. Doi: 10.4236/epe.2014.65009Panier, Škoda 2014
[22] PROCHAZKOVA, D., PROCHAZKA, J., DOSTAL, V. Risks of Power Plants with Small Modular Reactors. *Proceedings of the 31st European Safety and Reliability Conference*. ISBN 978-981-18-2016-8. Singapore: ESRA, Research Publishing 2021. Doi:10.3850/978-981-18-2016-8_125-cd
[23] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Řízení rizik procesů spojených s provozem technických děl během jejich životnosti.* ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. Doi:10.14311%2FBK.9788001066751
[24] HOLLNAGEL, E., WOODS, D.D. Resilience Engineering. ISBN 978-131560-5685. London: CRC Press 2017, 416 p.
[25] RASMUSSEN, J. Risk Management in a Dynamic Society. *Safety Science*, 27 (1997), 2, pp.183-213.
[26] LEPLAT, J. Occupational Accident Research and Systems Approach. In: *New Technology and Human Error.* ISBN 978-0471910442. New York: John Wiley & Sons 1987, pp. 181–191.
[27] LEVESON, N. A New Accident Model for Engineering Safer Systems. *Safety Science*, 42 (2004),4, pp. 237–270.
[28] LEVESON, N., DAOUK, M., DULAC, N., MARAIS, K. Applying STAMP in Accident Analysis. *Workshop on the Investigation and Reporting of Accidents.* Massachusetts: MIT 2003, pp. 177-198.
[29] MARAIS, K., LEVESON, N. Archetypes for Organizational Safety. *Workshop on the Investigation and Reporting of Accidents.* Massachusetts: MIT 2003, pp. 199-207.
[30] STERMAN, J. *Business Dynamics: Systems Thinking and Modeling for a Complex World.* Massachusetts: MIT 2002, http://hdl.handle.net/1721.1/102741
[31] LEVESON, N., DULAC, N., ZIPKIN, D., CUTCHER-GERSHENFELD, J., CARROLL, J., BARRETT, B. *Engineering Resilience into Safety-Critical Systems.* ISBN 978-131560-5685. Massachusetts: MIT 2006, pp. 1-22.

[32] EU. *Maastricht Treaty* (C 191, 29.7. Brussels: EU 1992, pp. 1–112.
[33] UN. *Human Development Report*. New York 1994, www.un.org
[34] 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/BK.9788001061824.
[35] 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.
[36] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. Praha: ČVUT 2022,129 p. Doi:10.14311/BK.97880010 69950
[37] KEENEY, R. L, RAIFFA, H. *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1993, 569 p.
[38] ISO. *ISO 31 000. Risk Management.* Zuerich: ISO 2010.
[39] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd. 1991.
[40] ČVUT. *Archiv pohrom, havárií, selhání a prací s rizik.* Praha: ČVUT 2023.

OCHRANA JADERNÝCH ZAŘÍZENÍ PŘED PODVODNÝMI POLOŽKAMI

PROTECTION OF NUCLEAR FACILITIES FROM FRAUDULENT ITEMS

Dana Procházková[1] , Jan Procházka[1] , Jan Jiroušek[2]

[1] České vysoké učení technické, Fakulta strojní, Technická 4, 166 00 Praha 6, danuse.prochazkova@fs.cvut.cz
[2] Statní úřad pro jadernou bezpečnost, pracoviště Temelín, 373 05 Temelín-elektrárna, jan.jirousek@sujb.cz

Abstrakt: Článek shrnuje poznatky o problematice podvodných položek, které narušují bezpečnost průmyslu, energetiky a dalších objektů, které jsou důležité pro život lidské společnosti. Uvádí: příčiny výskytu podvodných položek v jaderných elektrárnách; principy pro snížení rizika, které je spojeno s podvodnými položkami; generický model pro řízení bezpečnosti procesu výměny kritických položek v jaderném zařízení; a metodiku hodnocení přijatelnosti položek komerční kvality pro jaderná zařízení..

Klíčová slova: Podvodné položky; kritická zařízení a služby; jaderná zařízení; bezpečnost; principy pro zmírnění rizik.

Abstract: The article summarizes knowledge about the issue of fraudulent items that disrupt the safety of industry, energetics and other objects that are important for the life of human society. It states: the causes of the occurrence of fraudulent items in nuclear power plants; principles for reducing the risk associated with fraudulent items; a generic model for managing the safety of the process of replacing the critical items at a nuclear facility; and a methodology for assessing the acceptability of commercial quality items for nuclear installations.

Key words: Fraudulent items; critical facilities and services; nuclear installations; safety; principles for risk mitigation.

1. ÚVOD

Padělek, falzifikát nebo falzum je předmět, který se vydává za jiný, obvykle cennější předmět. Jeho původce je padělatel nebo falzifikátor a jeho činnost je označována jako padělání. Padělky se vyskytují v mnoha oblastech, počínaje platidly (penězokazectví), listinami a dokumenty, přes umělecké předměty, starožitnost i až po průmyslové zboží, zejména značkové nebo velmi důležité. V současné době jsou padělané a podvodné položky pro průmysl stále větším problémem.

Míst, ve kterých vznikají padělky je mnoho, jde o celý dodavatelský řetězec. Proto v jaderných zařízeních musí být z hlediska zajištění bezpečnosti zavedeny postupy pro odhalování a hlášení podezřelých položek. Článek sleduje vybrané postupy pro zajištění ochrany jaderných zařízení před podvodnými položkami. Konkrétně uvádí:

- příčiny výskytu podvodných položek v jaderných elektrárnách,
- principy pro snížení rizik, která jsou spojená s podvodnými položkami,
- generický model pro řízení bezpečnosti procesu výměny kritických položek v jaderných zařízeních
- a metodiku hodnocení přijatelnosti položek komerční kvality pro jaderná zařízení.

2. SOUČASNÝ STAV

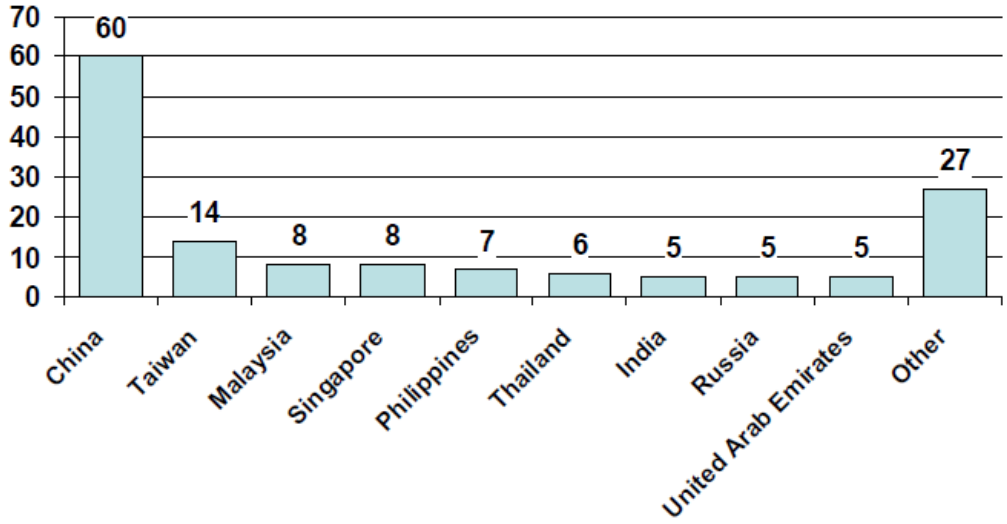
Padělané a podvodné položky vzbuzují celosvětově rostoucí obavy, což platí zejména pro jaderná zařízení. Představují mnohdy bezprostřední a potenciální hrozbu pro bezpečí pracovníků, výkonnost zařízení, bezpečí veřejnosti a životní ho prostředí a mají velký potenciál nežádoucím způsobem ovlivnit náklady na provoz a údržbu jaderných zařízení. Předmětné obavy značně přesahují úroveň samotných jaderných zařízení a zasahují až do úrovně polotovarů používaných při výstavbě jaderných zařízení a při výběru chemických a dalších pomocných látek, které se používají v těchto jaderných zařízeních. Dokonce i v případech, kdy je určitá položka pro jaderné zařízení zakoupena od certifikovaného výrobce originálního vybavení, existuje možnost, že materiály nebo součásti používané výrobcem mohou být v některé části dodavatelského řetězce padělané nebo podvodné [1]. Proto sledování dodavatelských řetězců a postupy zadávání veřejných zakázek v jaderných zařízeních hrají velkou úlohu při odhalování a prevenci zavlečení takových padělaných nebo podvodných položek do jaderných zařízení.

Současnou situaci ilustrují dále uvedená fakta - dle [1] Ministerstvo obchodu Spojených států uvádí, že došlo ke 140 % nárůstu padělaných položek mezi dodavateli průmyslových dílů pro Ministerstvo obrany Spojených států v letech 2006 až 2009, a to znamenalo problémy nejen v obraně, ale i v bezpečnosti státu. Podle amerických úřadů pro cla, ochranu hranic a imigrační a celní orgány USA maloobchodní hodnota padělaného a pirátského zboží, které bylo zabaveno v roce 2012 činila více než 1,26 miliardy dolarů, což představovalo více než 21% nárůst hodnoty zabaveného zboží oproti hodnotám v roce 2011 [2].

Podvodné položky v jaderných zařízeních např. dle [3] byly zjištěny v mnoha oblastech:
- strojní zařízení,
- elektrická zařízení,
- přístroje,
- software,
- certifikáty,
- služby
- i stavební prvky.

Jedním zřejmým společným prvkem podvodů je potenciál zisku [2]. Padělatelé mohou prodávat své výrobky na trhu za ceny stejné nebo nižší než je cena originálních položek, aniž by nesly náklady spojené s:
- výzkumem a vývojem v oblasti materiálů, výroby a testování,
- odpovědnostmi při licencování,
- marketingem
- a dalšími výdaji, které obvykle vznikají legitimním výrobcům.

Obzvláště vysoký tok padělaných materiálů a výrobků je z Asie [2]; obrázek 1.



Obr. 1. Země, které jsou podezřelé jako zdroje padělků - výsledky průzkumu z ledna 2010 [2].

3. POZNATKY A POKYNY MAAE, KTERÉ SE TÝKAJÍ PODVODNÝCH POLOŽEK

MAAE v dokumentu [1] uvádí fakta, ze kterých vyplývají příčiny výskytu podvodných položek v jaderných zařízeních a také ochranná opatření:

1. V posledních letech byla jaderná zařízení ovlivněna významnými událostmi a skutečnostmi, které souvisely se zadáváním veřejných zakázek. Došlo k dočasným i trvalým odstávkám jaderných elektráren z důvodu instalace padělků, podvodných a podezřelých položek, které souvisely se:
   - zvýšenou závislostí jaderných elektráren na digitálních zařízeních a na součástech obsahujících software,
   - počítačovou bezpečností,
   - zvýšenou globalizací jaderného dodavatelského řetězce,
   - zastaráním položek a stárnutím komponent jaderných elektráren,
   - postupným zužováním dodavatelského řetězce v důsledku přerušení výstavby jaderných zařízení v 90. letech,

- redukcí dodavatelských řetězců vyvolaných změnami v atomové legislativě a následným pojišťováním jaderných škod,
- zvýšením dostupnosti technologií pro padělání průvodní technické dokumentace,
- zvýšením dostupnosti technologií „reverzního inženýrství“,

a proto je nutné, aby uvedené skutečnosti zvažovaly organizace, které se zabývají nákupem (pořizováním) kritických položek pro jaderná zařízení.

2. Značný počet jaderných elektráren v některých zemích se blíží ke konci své původní projektované životnosti nebo usiluje o prodlouženou životnost. Se stárnutím zařízení jsou spojeny zvýšené obtíže při získávání dílů na podporu provádění údržby a oprav kritických komponent. Více než 20 % zařízení jaderných elektráren v některých zemích je zastaralých. Původní dodavatelé součástí zcela ukončily svou činnost, konsolidovaly se s jinými společnostmi nebo učinily obchodní rozhodnutí (obvykle kvůli snížení poptávky na trhu) nevyrábět určité položky nebo jim nedodávat osvědčení o jaderné kvalitě (tj. že mají požadovanou bezpečnost), protože se stalo nákladné udržování jaderných certifikátů národních dozorových orgánů.

3. Současnou situaci komplikuje i skutečnost, že jsou k dispozici jen omezené informace o původních zadáních zakázek pro originální součásti jaderných elektráren. Vzhledem ke změnám v průběhu času, technické informace a odborné znalosti, které se týkají některých položek, jsou neúplné nebo ztracené. To platí zejména pro produkty, které představují malou část produktů dodavatelů. Uvedené skutečnosti jsou proto zdrojem rizik pro bezpečnost i ekonomiku, které se projeví při provozu. Předmětná rizika vedou ke vzniku neplánovaných odstávek, protože zařízení související s bezpečností není k dispozici v momentě, kdy je požadováno, anebo nemá požadovanou kvalitu. V důsledku této skutečnosti již vznikla v některých zemích inženýrská funkce v oblasti nákupu. Hlavní funkce předmětného inženýre je identifikovat technické, kvalitativní a obchodní požadavky na kritické položky a provádět hodnocení shody (rovnocennosti) položek, a to hlavně těch, které jsou z komerčního trhu.

4. Funkce zadávání veřejných zakázek pro jaderná zařízení hraje klíčovou úlohu v jaderné bezpečnosti. Poptávání ve veřejných soutěžích může působit pozitivně z hlediska nabídnuté ceny. Zároveň však stejný mechanismus působí proti zajištění vysoké kvality a bezpečnosti v případě, že se obvykle používá kritérium „minimální nabídnuté ceny“. Při této aplikaci obvykle dochází k diskriminaci výrobců s dlouhou tradicí výroby, kteří jsou zatíženi náklady spojenými s vývojem technologií a udržováním klíčových pracovníků, technologií a dokumentace, které jsou nezbytné pro výrobu a ověřování kvality / bezpečnosti dané položky. Nákup položek, a to hlavně těch kritických, ovlivňuje životnost jaderných zařízení. Během počátečního návrhu, návrháři specifikují materiály, které mají být použity pro výrobu určitého zařízení. Tato specifikace má dlouhodobé důsledky pro účastníky dodavatelského řetězce a pro budoucí provoz. Během výstavby a uvádění do provozu jsou uzavírány servisní smlouvy za účelem získání personálu a souvisejících služeb. Během provozu jsou pořizovány náhradní díly pro údržbu, používány inženýrské a další služby a jsou prováděny i menší konstrukční změny (spojené se souvisejícími nákupy materiálů). Kvalita a velikost zásob materiálů i náhradních dílů má dopad na provozní náklady zařízení. Během vyřazování z provozu jsou uzavírány významné zakázky, jejichž důsledkem je, že některé příliš neopotřebované části či přebytky zásob se dostanou na volný trh, kde po malé úpravě mohou být prodávány jako nové.

5. V řadě případů jaderných zařízení není dodržován osvědčený postup zadávání veřejných zakázek na dodávky a činnosti spojené s provozem a údržbou jaderných zařízení, který má u každé položky obsahovat činnosti:
   - identifikace potřeb,
   - popis požadavků,
   - provedení hodnotové analýzy,
   - provedení průzkumu mezi dodavateli,
   - vyjednávání o kvalitě, výrobním postupu a ceně,
   - nákupní činnosti,
   - stanovení kritérií pro přijatelnost výrobku,
   - plán kontrol a zkoušek položky,
   - správa smluv,
   - kontroly a inventury,
   - způsob dopravy,
   - příjem a přejímací zkoušky,
   - požadavky na skladování.

6. Řízení dodavatelského řetězce zahrnuje plánování a řízení všech činností spojených se získáváním zdrojů, řízením nákupu, změnami a logistikou. Zahrnuje také koordinaci a spolupráci s distribučními partnery, kteří nejsou přímými dodavateli, zprostředkovateli či poskytovateli služeb. Řízení dodavatelského řetězce integruje nabídku a poptávku v rámci zúčastněných společností i napříč společnostmi. V souvislosti s jadernými zařízeními se předpokládá, že:
   - v řízení dodavatelského řetězce má aktivní úlohu zadávání veřejných zakázek
   - a v organizaci dodavatelského řetězce provozní organizace, tj. jaderné zařízení,

   a to na rozdíl od klasické relativně pasivní role provozní organizace, která spočívá v jednoduchém vydávání specifikací pro zadávání veřejných zakázek a v reakci na nabídky. Proto u projektů nových staveb jaderných zařízení je třeba, aby dodavatelé technologií úrovně 1 (tj. kritických položek) nastavili a spravovali dodavatelské řetězce, zatímco při obstarávání náhradních dílů spojeném s činnostmi provozu a údržby se používala komerční báze. Tyto dvě aktivity jsou vždy propojené, jako rozhodnutí a volby nákupu provedené dodavatelem technologie (např. volba a místo klíčových dodavatelů) má důsledky pro celý dodavatelský řetězec po celou dobu životnosti zařízení. Zmíněná nezbytná opatření, kultivující prostředí dodavatelských řetězců, mohou při nepoučené interpretaci u neodborné veřejnosti vyvolat nesprávný dojem, že jejich zaváděním je deformován volný pohyb zboží a služeb na trhu, s průvodními jevy dále popsanými.

7. Rizika v procesu zadávání zakázek jsou:
   - úplatkářství,
   - dávání darů,
   - střet zájmů,
   - přehlížení absence nebo padělání dokumentace,
   - praní špinavých peněz,
   - nepotismus,
   - vydírání,
   - ovlivnění obchodu,
   - snížení zdánlivé hodnoty nákupu, aby se předešlo požadavkům týkajícím se hospodářské soutěže,
   - schválení nekalého postupu (např. rozdělení a zadání projektů nebo zakázek jako více po sobě jdoucích zakázek stejnému dodavateli),
   - nucení pracovníků (včetně pracovníků subdodavatelů) prostřednictvím nekalých pracovních praktik k nerespektování norem průmyslové bezpečnosti.

8. Pro zajištění bezpečnosti musí být jasná strategie řízení rizik zacílená na bezpečnost – ISO 31000, 31010. Řízení rizik je nepřetržitý a iterativní proces, který zahrnuje dokumenty o rizicích a související plány řízení rizik. Klade také důraz na sdělování rizik a opatření přijatá k jejich zmírnění. V souvislosti se zadáváním veřejných zakázek na zboží i služby se sledují rizika:
   - technická,
   - časová,
   - nákladová
   - a dopady jevů, které narušují transparentnost a důvěryhodnost dodavatelského řetězce .

   Organizace zařízení, která jsou spojená s kritickou infrastrukturou mají mít definovanou strukturu pro řízení rizik, která obsahuje:
   - řetězec pravomocí,
   - komunikační strukturu,
   - rámec řízení, podle kterého probíhá řízení rizik a rozhodovací procesy.

9. Příklady rizik spojených se zadáváním veřejných zakázek jsou:
   - podhodnocení potřeby,
   - nadhodnocení potřeby,
   - nedostatečné finanční prostředky na řešení potřeb,
   - nepraktická cílová data,
   - neprovedení spravedlivého zadávacího řízení,
   - nesprávný výklad potřeb uživatelů,
   - politické nebo podnikové prostředí (např. změny směru ze strany vrcholného vedení nebo vlády),
   - pravděpodobný zájem médií,

- úzká definice nebo obchodní specifikace (např. konkrétní identifikovaný produkt nebo obchodní značka, a nikoli obecný požadavek),
- definice nevhodného výrobku nebo služby,
- zkreslená specifikace,
- neuvedení specifikace technických požadavků nebo požadavků na kvalitu "zvláštní objednávky", které vyžadují, aby dodavatelé prováděli činnosti, mimo své běžné výrobní postupy,
- první nákupy svého druhu, nové položky, přizpůsobené položky nebo položky, které nebyly dlouho vyrobeny časové období,
- nedostatečná specifikace zakázky nebo nepožadování výkazu práce (pro služby), včetně nedostatečné specifikace:
  - kritérií a metod kontroly,
  - zkoušek nebo podmínek přijetí,
  - opatření počítačové bezpečnosti,
  - balení,
  - značení,
  - požadavků na přepravu a skladování
- neřešené škodlivé dopady na životní prostředí nebo na pověst jaderného zařízení.

10. Rizika spojená se scénářem zadávání veřejných zakázek:
    - nejsou identifikovány potenciální nedostatky zdroje,
    - je vybrána nevhodná metoda,
    - je tajná dohoda s dodavatelem,
    - výběr společnosti, která ovládá trh,
    - podmínky nepřijatelné pro poskytovatele služeb,
    - poskytování nedostatečných informací (pozdější otázky týkající se výkladu nebo spory z důvodu nejasností nebo rozporů dokumentace, požadavky nebo smlouvy),
    - neřešení dotazů poskytovatelů služeb,
    - skutečné nebo domnělé zvýhodňování při poskytování informací,
    - skutečné nebo domnělé porušení důvěrnosti,
    - nevyžadování hodnocení poskytovatelů služeb kvality,
    - nedodržení účinných postupů hodnocení,
    - porušení bezpečnosti či zabezpečení (např. neoprávněný přístup nebo zveřejnění citlivých obchodních nebo bezpečnostních záležitostí, informace),
    - přehlédnutí faktu, že nabídky nesplňují potřeby,
    - rozhodnutí učiněné ze subjektivních důvodů,
    - výběr nevhodného poskytovatele služeb,
    - výběr nevhodného výrobku,
    - patová situace ohledně podrobností dohody,
    - nezajištění závazných podmínek,
    - nespravedlivé nebo zatěžující požadavky na poskytovatele služeb ve smluvních podmínkách,
    - nezohlednění podmínek nabízených a dohodnutých ve smlouvě,
    - neúmyslné vytvoření smlouvy bez řádného schválení nebo pro nevhodný výrobek.
11. Rizika v oblasti práv a plnění smluv:
    - kolísání cen a směny cizích měn,
    - neochota poskytovatele služeb přijmout smlouvu,
    - nedostatečná správa smlouvy,
    - špatná koordinace (např. zpoždění při předávání, špatná komunikace, jazykové nebo kulturní otázky),
    - neexistence účinného postupu řešení sporů, který způsobuje zpoždění smluvních činností,
    - výrobní tlaky nebo tlaky na dodržení plánu vedoucí k nedodržení výrobního postupu nebo postupu a harmonogramů testů ,
    - problémy se zaváděním systému řízení kvality u dodavatelů nebo programu zabezpečování jakosti (zejména pro nové nebo obnovené programy),

- zahájení prací poskytovatelem služeb před výměnou smlouvy nebo doručením dopisu o přijetí služby,
- neoprávněné nebo neočekávané zvýšení rozsahu práce,
- ztráta duševního vlastnictví,
- nesplnění závazků třetích stran (např. licenční poplatky nebo pojištění majetku třetí strany),
- ztráta nebo poškození zboží v tranzitu,
- podvod nebo jiné neetické chování (včetně dodání padělaných nebo podvodných předmětů),
- zlovolné kybernetické ohrožení elektronických zařízení v místě prodejce, během skladování nebo při přepravě,
- nedostatečné zabezpečení během výroby, včetně nedostatku bezpečného prostředí pro vývoj počítačů, kvalifikace dodavatelů a bezpečnostní kontroly na místě,
- zveřejnění citlivých informací nebo technologií prodejci nebo subdodavateli,
- nejsou k dispozici klíčoví zaměstnanci (tj. odchod do důchodu, odchod k jiné společnosti, přeřazení společnosti na jinou práci),
- nedostupnost pracovních sil nebo produktů (personál nebo materiál, který není v případě potřeby k dispozici, včetně neschopnosti naplnit větší objednávky než obvyklé, nesprávně odeslaný produkt nebo dopad možných pracovních sporů),
- významná změna v činnostech dodavatelů (včetně ukončení činnosti dodavatele nebo jeho koupení nebo sloučení s jiným subjektem),
- technologické poruchy (výrobek nebo projekt nefunguje, selhání návrhu),
- dodavatel není obeznámen se specifikovanými konstrukčními normami (zejména při mezinárodním nákupu),
- dodavatel nemá zkušenosti s požadavky na identifikaci podezřelých položek,
- neobvyklé nebo dokonce normální (tj. v rámci předpokládaných normálních rozmezí pro dané místo) povětrnostní podmínky, které vedou k neplánovaným činnostem,
- neočekávané polní podmínky,
- skluzy v plnění subdodávek,
- špatná produktivita a výkonnost subdodavatele,
- poškození, krádež nebo neoprávněná manipulace s položkou během přepravy (včetně únosu, pirátství nebo kybernetických útoků) nebo skladování,
- přehlédnutí otázek průmyslové nebo radiační bezpečnosti (tj. procesní nehody, události nebo téměř nezdařené postupy),
- nesprávné odstraňování odpadů (dopady na životní prostředí, položky vstupující do padělaného nebo podvodného dodavatelského řetězce, a dopady na pověst),
- nevyhodnocování postupů zadávání veřejných zakázek a jejich řízení,
- nepoučení z problémů a získaných zkušeností a neprovedení nápravných opatření (interních i mimo organizaci),
- desinterpretace chování zainteresovaných subjektů v dodavatelském řetězci způsobená kulturními odlišnostmi,
- nedostatečná kultura jakosti a bezpečnosti.

12. Klíčovým výstupem každého procesu řízení rizik je řádně sestavený a zdokumentovaný plán řízení rizik.

13. Pobídky a sankce nebývají součástí průmyslových smluv, což vede k opoždění dodávek nebo ke snížení kvality položek.

14. Pojištění se používá jako nástroj ke zmírnění rizik, což vede ke snížení kvality položek.

15. Kritéria přijatelnosti a metody přejímky v řadě jaderných zařízení nejsou stanoveny tak, aby poskytovaly záruku, že byly splněny požadované technické požadavky a požadavky na kvalitu. Stanovení technických kritérií přijatelnosti je inženýrskou funkcí. Kritéria přijatelnosti položky jsou:
    - výčet předepsaných měření,
    - výčet kontrol nebo výsledků testů, které lze objektivně ověřit.

    Vzhledem k tomu, že měření nemohou být nikdy absolutně přesná, musí být uvedeny tolerance výsledků u všech kritérií. Dobrým pravidlem je vybrat alespoň jedno kritérium přijatelnosti, které řeší každou bezpečnostní funkci. Stanovená kritéria by po ověření měla poskytovat přiměřenou jistotu, že položka splňuje

všechny technické požadavky a požadavky na kvalitu, které byly stanoveny při zadávání zakázky. Faktory, které je třeba vzít v úvahu při vypracovávání kritérií přijatelnosti, zahrnují:

- možné důsledky selhání položky pro jadernou bezpečnost, zabezpečení a provozuschopnost zařízení,
- historická výkonnost dodavatele při poskytování položek, které splňují stanovené požadavky,
- historická výkonnost položky v provozu,
- složitost návrhu,
- složitost výrobního procesu,
- zkušenosti z průmyslu,
- vliv, který má ověření kritérií přijatelnosti na provozuschopnost položky (např. možnost poškození položky v důsledku zkoušek),
- náklady na ověření kritérií přijatelnosti ve vztahu ke zvýšené jistotě poskytované ověřováním,
- přístup k zařízením dodavatelů, je-li položka k dispozici na skladě nebo pokud bude vyrobena až při přijetí objednávky,
- požadavky, je-li dodavatelem výrobce, který nemá zkušenosti, anebo přes zprostředkovatele třetí strana,
- dostupnost informací o návrhu,
- uplatňování pravidelného dohledu a přezkumů,
- schopnost provozního personálu organizace provádět zkoušky po instalaci,
- důvěra v dokumentaci dodavatele,
- praktičnost provádění ověřování zdrojů,
- inspekce a schopnost otestování provozu organizace.

16. Kontrola u zdroje (tj. dodavatelů materiálů a výrobců) je nutná, pokud je pořizována položka životně důležitá (kritická) pro bezpečnost zařízení, anebo je složitá při návrhu nebo výrobě, obtížně zkoušená nebo má obtížně ověřitelná kritéria přijatelnosti po obdržení (po dodání), anebo když systém řízení dodavatelů nebyl přímo auditován. U kritických zařízení, která jsou montována daleko od umístění provozní organizace, by mělo být zváženo zřízení rezidentního dozorového personálu v místě továrny během výroby součástí.

17. Důvěryhodný dodavatel by měl mít zaveden dostatečně robustní systém řízení neshod, který dokáže nejen identifikovat , ale i včas z procesu dodavatelského řetězce vyloučit padělané, podvodné či podezřelé položky. Systém řízení neshod nemá sám o sobě význam, nejsou-li zároveň odpovědní pracovníci v jeho užíváním dostatečně seznámeni a trvale trénováni v jeho užívání. Pracovníci kontroly položek musí zpozornět při přejímání, když objeví:
    - změněné nebo neúplné označení,
    - zjevné pokusy o zkrášlení,
    - důkazy o ručně řezaných znacích,
    - odchylky ve způsobu balení a značení obalů zboží od stejného výrobce,
    - nesrovnalosti v dokumentaci nebo nečitelnost některých partií dokumentace.

18. Sledovatelnost položek od výrobce, přes dopravce, přes skladování , dopravu do místa uložení, instalaci v konkrétním zařízení je důležitá, stejně jako sledování procesů spojených s manipulací, přepravou a skladováním, protože je třeba zabránit poškození, ztrátě, zhoršení nebo neúmyslnému použití předmětné položky.

19. Zvláštní pozornost při zadávání zakázek musí být věnována přístrojům a řídicím prvkům (I&C). Hlavně jde o pořizování software a vybavení s vestavěným softwarem nebo firmwarem. To je zvláště důležité pro přístrojová, řídicí a monitorovací zařízení v elektronice a výpočetní technice. Nedostatečná kontrola software může:
    - ohrozit bezpečnost nebo provoz zařízení,
    - narušit provoz nebo údržbu zařízení,
    - umožnit neoprávněný přístup ke kritickým místům nebo k tajné dokumentaci,
    - poskytovat informace, které by mohly být použity k útokům nebo přidávat další administrativní zátěž.

    Chyby software mohou vyplývat buď ze špatné, nebo nejasné specifikace požadavků (což vede k chybám v logickém návrhu nebo implementaci) nebo mohou vzniknout během implementační fáze či v provozu.

4. PRINCIPY PRO SNÍŽENÍ RIZIK SPOJENÝCH S PODVODNÝMI POLOŽKAMI

Dle výsledků obsažených v dokumentech [4,5], provozovatelé jaderných zařízení z důvodu ochrany před padělaným a podvodným zbožím, musí mít programy pro řízení bezpečnosti, které obsahují opatření, jejichž cílem je:

- zabránit podezřelým a podvodným položkám ve vstupu a v instalaci do jaderného zařízení,
- identifikovat, vyšetřovat a řešit podezřelé a podvodné položky,
- řídit, monitorovat a kontrolovat identifikované podezřelé a podvodné položky,
- sdílet informace s dalšími potenciálně postiženými zařízeními, regulačními orgány a dalšími účastníky průmyslu.

Uvedené čtyři soubory opatření musí být vzájemně propojené.

Na základě poznatků shrnutých v [4,5] základní principy ke zmírnění rizika spojeného se zavedením podezřelých a podvodných položek do jaderných zařízení jsou:

- zavést, ověřovat a zdokonalovat programy, procesy a nástroje podporující bezpečnost,
- zapojit management jaderného zařízení,
- včasná identifikace a zásah pro podporu bezpečnosti,
- efektivní řízení, monitorování a kontroly,
- dokumentace a zničení podezřelých položek,
- sdílení informací.

Činnosti související s nákupem kritických položek pro jaderná zařízení mají klíčový dopad na bezpečnost. Odstupňované přístupy umožňují energetickým společnostem soustředit úsilí na kritická zařízení a zajistit, aby procesy v dodavatelském řetězci nemohly nepříznivě ovlivnit bezpečný provoz jaderné elektrárny [4,5].

5. GENERICKÝ MODEL PRO ŘÍZENÍ BEZPEČNOSTI PROCESU VÝMĚNY KRITICKÝCH POLOŽEK V JADERNÉM ZAŘÍZENÍ

V dokumentech MAAE, OECD, WANO, EPRI, US NRC i FORATOM se zvažují modely procesů k dosažení stanovených cílů. Liší se od sebe podle cílů řešení konkrétních úkolů. Jejich cílem je, aby dílčí procesy i celý proces výměny kritických komponent v jaderných zařízení byly bezpečné, tj. aby neohrozily bezpečnost jaderného zařízení i jeho okolí. Cílem je snížit rizika a zvýšit bezpečnost, přičemž zvýšení bezpečnosti lze dosáhnout nejen snížením rizik, ale i vzděláním a připraveností lidí a lidské společnosti [4,6]. 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 rizika jsou rozdělená na lokální, regionální i státní úroveň.

Při zajišťování bezpečnosti objektu či procesu [6] 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,
- míra schopnosti systému řízení bezpečnosti zvládnout existující ohrožení, tj. zda se 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.

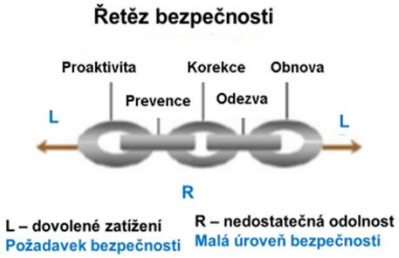
Základní principy pro práci a riziky dle [7] jsou:

- být proaktivní,
- domýšlet možné důsledky,
- správně určovat priority z pohledu veřejného zájmu,
- myslet na zvládnutí nepřijatelných dopadů,
- zvažovat možné synergie,
- být ostražitý, protože svět se dynamicky mění.

Proto při stanovení rizik pro strategické rozhodování se musí používat hierarchický multikriteriální postup. Recentní odborné práce používají pojem hierarchické holografické modelování (HHM) [7] a jejich výsledky jsou vysoce kvalitní, protože zohledňují řadu faktorů, které jsou původci neurčitostí.

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 [8] „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.

Analýza použitých modelů řízení rizik procesů, uvedených v pracích MAAE a EPRI, ukazuje, že modely mají stejný cíl a velmi podobnou logiku struktury [9]. Z citované práce vyplývá, že řízení rizik sledovaného procesu je proces, který hledá všechny potenciální stavy, které by ohrožovaly úspěšné fungování sledovaného systému ve všech etapách jeho životnosti, a identifikuje možnosti pro jejich zvládnutí prevencí, připraveností, odezvou a popř. obnovou, když přes všechno úsilí se do jaderného zařízení instalovala podezřelá položka a došlo k nežádoucím dopadům na jaderné zařízení a popř. i na jeho okolí. Řízení rizik ve prospěch bezpečnosti procesu se provádí podle modelu uvedeného na obrázku 2.



Obr. 2. Činnosti pro zajištění bezpečnosti procesu.

Bezpečnost objektu (technického zařízení i technických děl) či procesu a jejich okolí lze zajistit jen kvalitním antropogenním řízením [4,6]. Na základě hospodárnosti je třeba především provést snížení rizik v nejkritičtějších místech v rámci prevence, i připravit odezvu a obnovu na rizika, která nejsou vypořádána buď z důvodu opomenutí nebo neznalostí v procesu projektování a zhotovení, anebo preventivní opatření jsou velmi nákladná. Jedná se o velmi nákladnou činnost, a proto je nutná vzájemná komunikace mezi vlastníky a provozovateli technických děl, veřejnou správou, veřejností a médii [4].

Dle analogie k výsledkům uvedeným v [9], systém řízení bezpečnosti procesů spojených s ochranou před podvodnými položkami:

- řeší role spojené s bezpečností v oblasti provádění procesu a role v technice procesu i jejich interakce,
- obsahuje opakující se postup: identifikace problémů v oblasti bezpečnosti; vyhodnocení zjištěných problémů v oblasti bezpečnosti; určení opatření a činností pro zvýšení bezpečnosti; implementace opatření a činností pro zvýšení bezpečnosti a monitoring situace; a ocenění míry bezpečnosti.

Systém řízení bezpečnosti objektu je postaven na zásadách řízení procesů dle TQM [10], tj. zahrnuje:

- organizační strukturu řešitelů procesu,
- odpovědnosti,
- praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence škodlivých jevů či alespoň zmírnění jejich nepřijatelných dopadů v jaderném zařízení.

Zpravidla se týká řady otázek, kromě jiného i organizace řešitelů, 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.

S ohledem na dynamický vývoj světa, existují rizika, která:

- nelze eliminovat preventivními opatřeními, která zaručují bezpečnost pomocí technických limitů stanovených pro projektové podmínky,
- jsou proměnná v čase a místě, a proměnnost má řadu neurčitostí,

a proto je třeba zpracovat plán řízení rizik dle ISO 31 000. Plán řízení rizik je nástroj pro proaktivní řízení rizik, které zvažuje možná vzájemná propojení v čase [10], který je klíčovým výstupem každého řízení rizik.

Plán řízení rizik se opírá o způsob řízení TQM [10]. Zvažuje prioritní rizika, která nebylo možno vypořádat jistými preventivními opatřeními, a která při realizaci mají potenciál významně poškodit proces. Zpracovává se ve formě tabulky, kde se pro každé riziko uvádí:

- příčiny rizika,
- dopady selhání procesu na jaderné zařízení a popř. i jeho okolí,
- pravděpodobnost / četnost výskytu realizace rizika a velikost dopadů rizika,
- opatření pro zvládnutí nebo alespoň zmírnění dopadů rizika, které jsou jasně stanoveny, a u každého z nich je uvedena organizace (či její odpovědný zástupce), která provede odezvu a osoba odpovědná za správné a včasné provedení odezvy je uvedena odpovědnost za jejich provedení.

Důležitou roli při řízení rizik sledovaného procesu hraje organizační struktura řízení procesu [9], tj. mechanismus, který slouží ke koordinaci a řízení procesu. Představuje hierarchické uspořádání vztahů nadřízenosti a podřízenosti a řeší vzájemné pravomoci (kompetence), vazby a odpovědnost. Uvolnění velkých finančních a dalších prostředků na řízení a vypořádání rizik pochopitelně je jen na nejvyšší hierarchické úrovni. Na základě analogie s materiály [10] se zvažuje jak struktura řízení sledovaného procesu, tak role dozoru, který vykonává dohled nad bezpečností ve veřejném zájmu.

6. METODIKA HODNOCENÍ PŘIJATELNOSTI POLOŽEK KOMERČNÍ KVALITY

Metodika hodnocení přijatelnosti položek komerční kvality, které mají nahradit kritické položky v jaderných zařízeních je v USA začleněna do standardů kvality, protože bezpečnost je základním znakem kvality každé entity. Je určena pro použití všech subjektů, kteří zpracovávají programy QC/QA, tj. držitelé licencí, dodavatele komerčních položek a další organizace, které se podílí na projektování, výstavbě, provozu a údržbě jaderných zařízení. Týká se materiálů a součástí, včetně náhradních a náhradních dílů nezbytných pro provoz zařízení, doplňování paliva, údržbu a úpravy. Platí US NRC Regulatory Guide 1.28. Zmíněná metodika používá postup, který ukazuje výše uvedený generický model pro řízení procesů.

Shrnutí požadavků, které zajistí přijatelnost položek komerční kvality dle [3,11]:

1. Organizace, která nakupuje položku, musí uvést požadavky na položku v nákupních dokumentech nebo specifikacích a vybrat produkt, který splňuje příslušné požadavky. V některých případech musí uvést i požadavky na zkoušky, které prokazují, že položka splňuje příslušné požadavky. Požadavky na položku v zadávací dokumentaci musí být uvedeny v technických specifikacích, včetně plánu přejímky, který poskytne přiměřenou záruku, že požadavky na položku jsou splněny. Jen tak bude poskytnuta přiměřená záruka, že pořizovaná položka bude plnit své funkce související s bezpečností. V zadávací dokumentaci musí být uvedeny i požadavky na zabalení a dopravu položky od dodavatele do jaderného zařízení, aby nedošlo k jejímu poškození.
2. Rozhodnutí o přijatelnosti musí být prováděna na základě výsledků technických hodnocení, která provádí kvalifikovaný personál, který má zkušenosti z oblasti projektování, inženýrství, výroby, funkčnosti zařízení, kvality a požadavků dozoru.
3. Pro hodnocení se doporučuje používat metodu FMEA a kontrolní seznamy. Pro technická hodnocení, která ověřují, že položka má požadovanou kvalitu a vlastnosti, jsou vhodné metody nedestruktivního testování a v nejnutnějších případech i inženýrský úsudek.
4. V případě, že je třeba použít náhradní položku, která není fyzicky totožná s originálem, tak je nutno prokázat shodu, aby bylo zajištěno, že projektovaná i konstrukční funkce položky bude zachována.
5. Materiál, proces výroby položky, proces testování položky, proces zabalení položky i proces dopravy položky na místo určení musí být takové, aby bylo zaručeno, že položka bude plnit svou zamýšlenou bezpečnostní funkci.
6. Zadávací dokumentace je chápaná jako soubor smluvně závazných dokumentů, které identifikují a definují požadavky, které musí zboží nebo služby splňovat, aby byly pro kupujícího považovány za přijatelné. U kritických položek, tj. položek souvisejících s bezpečností, musí být ještě Q-list (průkaz bezpečnosti – tj. průkaz nejvyšší kvality).
7. Každá komerční položka, která nahrazuje kritickou položku, musí splnit požadavky technického hodnocení a procesu přejímky:

a) Technické hodnocení položky se obvykle skládá z:
   - posouzení bezpečnostní klasifikace,
   - náhradního ověření shody,
   - ověření technických a kvalitativních požadavků,
   - vytvoření zprávy o přijatelnosti položky.

   Do technického hodnocení se zahrnuje také posouzení rizik, která jsou spojená s nákupem (např. výsledky hodnocení, zda by položka mohla být padělkem nebo podvodem, zastaralou položkou, položkou se zranitelností). Technické hodnocení je upraveno v práci [11], kde je specifikována metoda odběru vzorků (velikost vzorků pro nedestruktivní zkoušení, zvážení bezpečnostního významu při určení velikosti vzorku, homogenita; požadavky na dokumentaci).

b) Proces přejímky musí poskytovat jistotu, že pořízená položka splňuje stanovené požadavky, a proto se doporučuje aplikace jedné nebo několika metod z:
   - 1 – speciální zkoušky a inspekce,
   - 2 – průzkum úrovně subjektu komerce,
   - 3 – ověření zdroje (inspekce nebo výslech svědků),
   - 4 - posouzení pověstí (jména) dodavatele.

c) Procesy hodnocení u přejímky jsou:
   - specifikace položky a zadávací dokumentace pro dodavatele,
   - kontrola kvality dodavatele,
   - technické hodnocení pro posouzení kvality dodané položky,
   - plán přejímky – včetně požadavků na výsledky testů,
   - kontrola položky po přijetí, instalace a monitoring výkonnosti položky.

Hlavním cílem hodnocení komerčního dodavatele by mělo být ověření, zda jsou kritické vlastnosti pořizovaných položek náležitě kontrolovány během výroby, dopravy a skladování.

8. Položky podezřelé z podvodu musí být vyhodnoceny a nahlášeny do příslušných oborových databází, jako provozní zkušenosti s komerčními subjekty.

9. Po dokončení zkoušek položky po instalaci by měla být pořízena zkušební dokumentace související se specifickou zkouškou nebo dozorem a uchována jako záznam o provedených zkušebních činnostech a jako důkaz o uspokojivém dokončení zkoušky po instalaci.

10. Služby, které vyžadují prověřování kritické položky jsou:
    - opravy,
    - testovací služby,
    - výrobní služby,
    - poradenské služby,
    - kalibrační služby,
    - inženýrské / technické služby
    - služby spojené se software.

11. Opatření ke zlepšení odhalování padělaných a podvodně označených výrobků pro produkty používané v jaderných elektrárnách je zaručeno jen odpovídajícím zapojením inženýrů během procesů zadávání zakázek a přejímce produktů, včetně testování.

7. ZÁVĚR

Padělané nebo podvodné zboží představuje nejen pro jaderný průmysl stále větší problém. Má dopady na bezpečnost i ekonomické dopady. Proto pracujeme na nástrojích pro inspekce jaderných zařízení v České republice, které jsou zacílené na posouzení kvality jeho ochrany vůči podezřelým a podvodným položkám v případě výměny kritických položek. Vycházíme z toho, že zabránění vložení padělaných nebo podezřelých položek do jaderného zařízení znamená řízení bezpečnosti procesu (Process Safety Management - PSM) vkládání položky do jaderného zařízení při výměně položky nebo při modernizaci.

Řízení bezpečnosti procesů (PSM) má ve světě různé verze. Představuje složitý postup a vyžaduje multidimenzionální přístup, který spojuje technologie a jejich řízení [4]. Řízení bezpečnosti procesů je spojeno s kulturou bezpečnosti a pro hodnocení bezpečnosti se často používá kontrolní seznam [12].V Evropské unii souvisí řízení bezpečnosti procesů se skladováním nebezpečných chemických látek a manipulací s nimi [13] s cílem omezit

rizika. Ve Spojeném království se nařízení o kontrole nebezpečí závažných havárií (COMAH) z roku 2015 vztahuje na PSM [14] - zabývají se jím např. specifické normy pro všeobecný a stavební průmysl.

LITERATURA

[1] IAEA. *Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities. No. NP-T-3.21.* ISSN 1995–7807, ISBN 978–92–0–107315–0. Vienna: IAEA 2016, 268 p.

[2] TANNENBAUM, M. *Plant Support Engineering: Counterfeit and Fraudulent Items Mitigating the Increasing Risk.* Revision 1 of 1019163. EPRI 2014, 128 p.

[3] 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.

[4] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364 p. Doi:10.14311%2FBK.9788001061824

[5] IAEA. *No. NP-T-3.26. Managing Counterfeit and Fraudulent Items in the Nuclear Industry.* ISBN 978–92–0–102318–6.ISSN 1995–7807. Vienna: IAEA 2019. 110 p.

[6] 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.978 8001064801

[7] HAIMES, Y. Y. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis* 29 (2009), 12, pp. 1647–1654.

[8] FAWCETT, H.H. Hazardous and Toxic Materials. Safe Handling and Disposal. New York: Willey 1984.

[9] PROCHÁZKOVÁ, D. Charakteristiky inženýrství zacíleného na bezpečnost. In: *Řízení rizik procesů, zařízení a složitých technických děl zacílené na bezpečnost.* ISBN 978-80-01-07060-4. Praha: ČVUT 2022, pp. 7-34. Doi:10.14311/BK.9788001070604

[10] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd. 1991.

[11] EPRI. *Guideline for Sampling in the Commercial-Grade Item Acceptance Process*. TR-017218-R1. Palo Alto: EPRI 1999, 99 p.

[12] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessse: US DOE 1996, 180 p.

[13] EU. *Seveso III Directive (2012/18/EU).* Brussels: EU 2012.

[14] UK. *COMAH*. London 2015. www.hse.gov.uk

TRESTNÍ ODPOVĚDNOST ZA PROVOZ ROBOTŮ S UMĚLOU INTELIGENCÍ

CRIMINAL LIABILITY FOR THE OPERATION OF ROBOTS WITH ARTIFICIAL INTELLIGENCE

Vladimír Smejkal

VUT v Brně, Fakulta podnikatelská. Kolejní 2906/4, 612 00 Brno. Česká republika. smejkal@znalci.cz

Abstrakt: Legislativa občanskoprávní odpovědnosti se v současné době připravuje v rámci EU, ale problematice trestní odpovědnosti za jednání robotů byla doposud věnována malá pozornost. Čím více se roboti stanou autonomní a čím větší budou mít schopnost samoučení, tím obtížnější bude prokázat, do jaké míry bylo možné selhání v době návrhu předvídat, zjistit, kdo za ně odpovídá, a zda lze zvážit znaky konkrétního trestného činu. Ukazuje se, že není třeba zavádět nové trestněprávní konstrukce, ale zaměřit se na proces prevence a dokazování. Místo změny právního systému je nutné vytvořit co nejpodrobnější auditní stopu vypovídající o jednání a okolí robota, případně také mít digitální dvojče robota.

Klíčová slova: Umělá inteligence, robot, provoz robotů, rizika, trestní odpovědnost.

Abstract: Civil liability legislation is currently being prepared within the EU, but little attention has been paid to the issue of criminal liability for the actions of robots. The more autonomous robots become and the greater their capacity for self-learning, the more difficult it will be to demonstrate to what extent failures could have been foreseen at design time, to identify who is responsible for them and whether the characteristics of a specific crime can be considered. It turns out that there is no need to introduce new criminal law constructions, but to focus on the process of prevention and evidence. Instead of changing the legal system, it is necessary to create as detailed an audit trail as possible about the behaviour and surroundings of the robot, or to have a digital twin of the robot.

Key words: Artificial intelligence, robot, operation of robots, risks, criminal liability.

1. ÚVOD

Čím více jsou roboti vybavováni řídícími moduly využívajícími umělou inteligenci (artificial inteligency - AI), pak zejména v případě samoučících se systémů se objevuje naléhavá otázka trestní odpovědnost za provoz robotů.

V současnosti byly zveřejněny návrhy dvou právních aktů EU, které mohou vytvářet dojem, že řeší beze zbytku problematiku odpovědnosti za jednání umělé inteligence (AI):

1. Akt o umělé inteligenci [1]
2. a Směrnice o odpovědnosti za umělou inteligenci [2].

Není tomu zcela tak, protože tímto není dotčena otázka trestněprávní odpovědnosti za jednání robotů, případně jiných systémů AI jako takové. Problematice trestní odpovědnosti za jednání robotů byla doposud věnována malá pozornost, přičemž v ČR se jí věnoval zejména autor tohoto příspěvku [3,4].

Dnes se setkáváme s další vlnou IT bublin: po bublinách dot-comové, blockchainové a kryptoměnové je zde AI bublina, přičemž ve sdělovacích prostředcích jsou uveřejňovány pouze nepodloženě optimistické perspektivy spojené s AI nebo naopak různé katastrofické scénáře a tendenční varování vyslovovaná různými světovými celebritami. Pokud je realisticky zmiňována otázka rizik spojených s AI, většina diskusí se přitom zaměřuje na ryze softwarové roboty či jiné programy, jako jsou např. konverzační systémy AI (např. ChatGPT) nebo systémy pro uměleckou tvorbu (DeepArt, Magenta, Aiva atd.). Stále více je pak upozorňováno na tzv. deepfake ("deep learning" a "fake") podvody, kdy AI využívá hluboké učení k vytvoření falešných fragmentů obrazu, videa nebo zvuku a napodobuje něčí hlas, výraz obličeje nebo chování (nástroji jako Deep Art Effects, Deepswap, Deep Video Portraits atd.). Využívání těchto nástrojů přitom také může sloužit v páchání trestné činnosti různých skutkových podstat.

Tento text se zabývá odpovědností za roboty, zejména pak za roboty využívající AI, tedy za zařízení, která mají přímou nebo nepřímou odezvu ve fyzickém světě (ne nutně přímou mechanickou manipulací, ale také předáním

příkazu jinému systému, který má rozhraní s fyzickým světem – například řízení vodovodní sítě nebo silničního provozu). řízení). Roboty pouze softwarovými se tento příspěvek nezabývá.

2. ANALÝZA PROBLEMATIKY UMĚLÉ INTELIGENCE Z PRÁVNÍHO HLEDISKA

Většina lidí se domnívá, že před roboty je chrání tzv. Zákony robotiky, nebo také Asimovovy zákony [5]. Jde ale jen o literární fikci, která se sice stala základním kamenem pohledu na vztah člověka a robota v sci-fi literatuře, ale nelze z nich dovozovat cokoliv reálného a právně závazného. Z hlediska právního řádu ve vztahu k robotům se nyní nacházíme v podobné situaci, jako při vzniku a zejména masovém rozšíření Internetu, kdy se diskutovalo tom, zda v kyberprostoru platí stávající právní řád, měl by platit nějaký jiný nebo zda jde o sféru právem neupravitelnou. Podobné diskuse nyní probíhají ve vztahu k AI [6] a dle názoru autora i zde je třeba preferovat aplikaci existujícího právního řádu, před vymýšleních nějakých nových, umělých konstrukcí.

2.1. Roboti

Robot se od informačního systému, resp. „čistého" software liší svou schopností přímo fyzicky interagovat se svým prostředím a po dlouhou dobu byl pojem robot (kromě domácích robotů) z velké části chápán jako „průmyslový robot", i když slovo „ industrial", tj. systém primárně určený k provádění jednoduchých, typicky opakujících se mechanických operací, se nyní může zdát příliš omezující, protože roboti pronikají do výrazně „neprůmyslových" oblastí, jako je medicína. Definici průmyslového robota podle International Federation of Robotics (IFR) „*Průmyslový robot je definován jako automaticky řízený, přeprogramovatelný, víceúčelový manipulátor, programovatelný ve třech nebo více osách, který může být buď upevněn na místě, nebo připevněn k mobilní platformě pro použití v automatizačních aplikacích v průmyslovém prostředí* [7]*"* lze aplikovat pro jakékoliv, nikoliv pouze průmyslové prostředí.

Technická podstata robota se vyvíjí neustále směrem od jednoduchých manipulátorů až k autonomním systémům, kde robot vykazuje schopnost provádět zamýšlené úkoly na základě aktuálního stavu a údajů ze snímačů bez lidského zásahu, ve svém prostředí se pohybuje a provádí zamýšlené úkoly, přičemž obsahuje řídicí systém a rozhraní řídícího systému [8].

Roboti mohou být plně nebo částečně autonomní, nebo je lze ovládat na dálku (programem v cloudu a/nebo člověkem), často pravděpodobně obojí v nějaké předvídatelné synergii. Stupeň autonomie robota je stále určován člověkem, a to buď a priori na základě vytvořeného programu nebo v konkrétní situaci osobou ovládající, kdy lidský operátor je vždy součástí řídicí smyčky programu takového robota. Příkladem je autopilot v letadle, u kterého mu pilot po nastavení určitých parametrů předá řízení letadla, ale dohlíží na jeho chod a může do práce tohoto robota kdykoliv zasáhnout – korigovat jeho řízení letadla, případně ho úplně vypnout. Podmínky, za kterých může pilot tomuto systému předat řízení letadla, jsou však definovány v leteckých předpisech a předpisech výrobce letadla a konkrétními letovými podmínkami.

Ve skutečnosti ale ani lidský dozor v případě komplexních systémů, jako jsou letadla, není schopen zabránit nehodám s osudnými důsledky. V roce 2018 a 2019 jen v rozmezí několika měsíců došlo ke dvěma fatálním nehodám zbrusu nových a moderních letounů Boeing 737 MAX, které si vyžádaly 346 obětí. Vyšetřování jako hlavní příčinu nehod odhalilo systém MCAS (Maneuvering Characteristics Augmentation System), resp. jeho problematické fungování v případě chybných dat ze senzorů náběhu. Podle interních vývojových dokumentů Boeingu neměl systém MCAS „nežádoucím způsobem zasahovat do pilotování letadla" a neměl zasahovat do řešení situace po překonání kritického úhlu náběhu. To se však dělo. To nicméně Boeing ani FAA nepředpokládaly a setkání se s chybnou aktivací systému navíc vypadalo extrémně nepravděpodobně. Potřeba byla specifická kombinace okolností a závad. Piloti proto nebyli na fungování systému nijak speciálně školeni a upozorněni nebyli ani na další drobné změny některých souvisejících systémů. Změněna přitom ale byla i logika deaktivace tohoto asistenta [9]. Ovšem ani zde není jediná a přímá vazba mezi příčinou a následkem. *„Zjistili jsme, že k nehodě přispělo dohromady devět různých faktorů. Kdyby jeden z nich nenastal, možná by k nehodě nedošlo,*" citovala BBC vyšetřovatele indonéského Národního výboru pro bezpečnost dopravy (NTSC). Zpráva popisuje seznam selhání – od špatné komunikace přes špatný design až po nedostatečné letecké dovednosti. *„Je tu spousta „co kdyby". Kdyby posádka letu z předchozích dnů podala podrobnější popis problémů, kterým čelila, letadlo by možná nikdy nevzlétlo na svůj osudný let. A kdyby kapitán, který úspěšně udržel letadlo ve vzduchu – navzdory zásahu zlotřilého automatizovaného systému, kterému nerozuměl – nepředal řízení svému méně schopnému prvnímu důstojníkovi, katastrofě by se dalo zabránit*" [10].

Tento ilustrativní příklad ukazuje, jak obtížné bude hledání příčin a následků včetně případné trestní odpovědnosti u složitých systémů, zejména pak u těch, které nebudou fungovat podle deterministických programů.

V souvislosti s robotizací a rostoucími schopnostmi robotů využívajících AI se čím dál více objevuje zcela nový fenomén, kterým je cosi jako vlastní vůle, vlastní iniciativa, či vlastní, samostatné rozhodování robotických systémů, které opouštějí pozice po staletí vyhražené postavení nemyslících, více či méně sofistikovaných, ale pouhých mechanismů, plně podléhajících vůli a pokynům člověka. Někteří roboti se ocitají se v nové roli čehosi, co by se snad nejlépe dalo pro začátek nazvat samostatně jednajícím, tedy autonomním strojem. Je patrno, že takový nový aspekt se nepochybně promítne i do práva; proto je třeba zaměřit na eventuální trestní odpovědnost za protiprávní následky jednání robotů a jak ji prokázat.

Roboty je z hlediska úrovně jejich schopnosti k samostatnému rozhodování možno pro účely tohoto textu rozdělit do pěti generací:

1. Do nulté generace jsou zařazeny manipulátory a roboti zpravidla bez zpětné vazby, kdy veškeré poruchy či změny ve sledované oblasti (signalizované čidly) vedou k nedovolení dalšího kroku, zastavení systému (tzv. „central stop“) a přivolání údržbáře.
2. Do prvé generace zařazujeme roboty s jednoduchou zpětnou vazbou, schopné přepínání několika deterministicky pracujících podprogramů (předem vytvořených člověkem) a práce podle nich.
3. Ve druhé generaci jsou roboti se schopností optimalizace, tj. schopností vybírat z předem zadaných programů optimální, a to podle zadaného kritéria, tedy je stále známo přesné pravidlo, které rozhodování o další činnosti řídí.
4. Třetí generace je charakterizována roboty, jež jsou schopni samostatné modifikace původního programu, tedy plánu činnosti, neboť se dokáží učit z nabytých zkušeností. Zde se předem zadává pouze cíl činnosti (úkol), přičemž způsob jeho splnění je ponechán na inteligenci řídicího systému, který si sám vytvoří plánu činnosti, sestávající z jednotlivých postupných kroků a činností k dosažení daného cíle. Plánem činnosti se rozumí posloupnost stavů robota v prostoru popsaná buď numericky nebo symbolicky – logickými výroky, které si robot sám interpretuje, aby dosáhl zadaného globálního cíle [11]. Formulování plánu pak spočívá v hledání cesty ve stavovém prostoru od současného stavu k cílovému stavu.
5. Čtvrtá generace je reprezentována autonomními roboty se sociálním chováním, které se chovají podobně jako člověk, tedy samostatně si volí i cíle jednotlivých prací na základě vhodného globálního kritéria.

Počínaje třetí generací bude zřejmě problémem již stanovení příčiny nežádoucího jednání robota, které vede k nepřijatelným důsledkům pro lidi a životní prostředí. A o to těžší bude eventuální hledání trestněprávní odpovědnosti.

2.2. Řízení robota

Klíčovým problémem je způsob řízení robota, které se vyvíjí od deterministického počítače k samoučícímu se stroji. Zatímco doposud převažují roboti řízení klasickým počítačovým systémem v podobě deterministického automatu, tedy roboti 1. a 2. generace, ke změnám v paradigmatu dojde v souvislosti s nástupem AI v podobě samoučících se strojů (self-learning systems). Dlouhou dobu a až prakticky doposud fungovaly počítače podle von Neumannovo schéma z roku 1945 [12].

Principem je systém řízený programem, který je uložen s daty společně v paměti. Časem přišly odlišnosti, např. v podobě tzv. Harvardské architektury, ale existence programu řídícího práci počítače zůstala zachována. Tento princip se nezměnil ani u „hitu“ dneška, jakým jsou kvantové počítače. Jejich způsob výpočtu je odlišný:

- kvantový počítač využívá k zápisu informace kvantově mechanické vlastnosti částic, například spin elektronů, spin atomových jader nebo jiné vlastnosti kvantově se chovajících objektů,
- kvantový počítač nese současně informaci o všech možných hodnotách kvantované veličiny, a tím provádí paralelně výpočet všech možností, které mohou nastat. Výpočet je mnohonásobně efektivnější než u klasického počítače [13].

Koncem října 2019 oznámila společnost Google (prostřednictvím článku v Nature), že dosáhla takzvané kvantové nadřazenosti, tedy okamžiku, kdy kvantový počítač provede výpočet řádově rychleji než superpočítač klasické architektury [14]. Nic se ale nezměnilo na tom, že stále existuje programování a programovací jazyky, které umožňují psát programy pro kvantové počítače (např. Twist). Pracujeme s kvantovými algoritmy, které implementujeme. A vznikly nástroje či služby umožňující vyvíjet kvantové algoritmy a programovat a spouštět je na skutečném hardwaru – např. Azure Quantum [15].

Klasické, ale i kvantové počítače stále fungují na principu navrženém před 80ti lety, tj. s řídící jednotkou, aritmetickou jednotkou a pamětí, s pevnou hardwarovou strukturou a předem daným programem definované struktury, který byl vytvořený nějakým programátorem. Všechny provozní funkce a stavy stroje jsou tak pevně definovány, takže jakkoliv může program fungovat velmi variabilně, nemůže se dostat do jiného než přepokládaného stavu. V opačném případě dojde k provozní chybě (např. stack overflow). Zde se již objevuje první problém a požadavek: je třeba zajistit, aby k provozní chybě nedošlo (což není absolutně možné), pokud ale ano, pak aby byly minimalizovány případné škody na majetku, zdraví a životech osob.

Naproti tomu AI by měla být schopna úplného nebo alespoň částečného samostatného učení, tedy mít schopnost automaticky samostatně přizpůsobit svojí funkci na nové, doposud jí neznámé situace. Řídící systém umělé inteligence je stručně řečeno tvořen nějakou obecnou funkční strukturou stejnou pro velké množství různých aplikací, která se až postupným učením začne profilovat na konkrétní provozní funkcí / operací. Zatímco u klasické koncepce strojů s přesně stavově definovaným logických řídícím programem je veškerá odpovědnost za správnou funkci "na bedrech" programátora, který musel vymyslet a rozhodnout, jaké funkce a reakce stroje do programu implementuje, u umělé inteligence realizované na nějaké formě tzv. neuronových sítí se při učení předkládají standardní neuronové struktuře jednotlivé reálné vzorky či úkony, se kterými má pak stroj fyzicky pracovat. Ty definují („předvádí“) operace, které s nimi má robot provádět, společně s informací, zda daný úkon je žádoucí (správný) či nežádoucí (nesprávný). Neuronová struktura si již sama najde společné či rozdílové znaky mezi předkládanými předměty či definovanými operacemi a také si sama určí ideální posloupnost operaci, aby funkce systému byla co nejrychlejší a nejefektivnější [16].

Tím se ale dostáváme do stavů, které nemůžeme předem definovat a budeme obtížně vyvozovat, kdo za jejich dosažení, pokud se projeví nepřijatelnými důsledky na svém okolí či na robotu samém, odpovídá.

2.3. Nový rozměr odpovědnostních vztahů

Nový rozměr odpovědnostních vztahů bude dán tím, že snad u všech doposud používaných strojů a zařízení příslušejících k 0. až 2. generaci je z hlediska případné odpovědnosti relativně jednoduchá linie jednání a následku. Ať již jde o konstrukci a výrobu těchto strojů, na jejímž začátku je projekt s prakticky vždy verifikovatelnými parametry, a tedy s relativně jednoduchou možností následného prověření, zda nějaká významná skutečnost nebyla při projektování opomenuta. Totéž platí o výrobním procesu, u kterého, vyjdeme-li z premisy, že projekt neměl podstatnou vadu, jde o zjištění, zda byl respektován anebo z nějakého důvodu došlo k odchylce, která mohla či nemusela být v příčinné souvislosti s následným protiprávním následkem.

Další fází je samotné užití konečného produktu, které tam, kde jde o složitější výrobek s relativně větším škodním potenciálem, je regulováno právními předpisy a provozními příručkami. Typicky pokud jde o dopravní prostředky všeho druhu, kde právní předpisy výslovně stanoví způsob provozování těchto dopravních prostředků na veřejných komunikacích. U jiných je upravena jen odpovědnost za protiprávní následek, např. v případě odpovědnosti za škodu způsobenou provozní činností. Kromě toho existuje řada technických předpisů a technických norem, upravujících vlastnosti výrobků. Zde již ovšem bude k diskusi otázka povinnosti aplikace takových předpisů či norem na straně jedné, nebo naopak neexistence uvedených předpisů či norem, přestože by z hlediska prevenční povinnosti to bylo namístě.

U robotů 3. a zejména 4. generace ale již tomu tak není či nebude, takže bude velmi důležitá úprava jejich užívání a všeho co s tím souvisí, včetně případné odpovědnosti za škodu či újmu, která v důsledku selhání robota vznikne. V případě následku, který je v rozporu s účelem a smyslem stroje či zařízení, lze relativně jednoduše analyzovat jednání a jeho soulad s právem, určit příčinný vztah mezi tímto jednáním a následkem a z toho odvodit případné zavinění jako subjektivní stránku možného trestného činu. Současně se ovšem zcela zákonitě bude nabízet otázka, do jaké míry mohlo být toto selhání předvídáno při konstrukci robota a zda v této fázi nebo snad ve fázi výroby nedošlo k jednání, které by bylo možné dát do příčinné souvislosti s následkem a posléze zvažovat zavinění, respektive naplnění skutkové podstaty určitého trestného činu.

Nicméně vždy bude nezbytné počítat s faktem, že i v jednodušším případu zcela deterministického chování řídicího systému takového robota nelze při náhodných (neočekávaných) vstupních signálech a datech (pozorování okolního světa) s jistotou určit výsledné chování robota za všech možných okolností. Tím se otevře značný prostor pro technicko-právní analýzy toho, co se při konstrukci a programování robota dalo předpokládat jako možné selhání, čemu se v rámci tohoto předpokladu dalo zabránit vhodnými úpravami a co je v kategorii náhody, či vyšší mocí (*vis maior*).

2.4. Deliktní odpovědnost v robotice

Zřejmě ani existence a posléze hromadné užívání robotů třetí, čtvrté případně snad i nějaké vyšší generace nezmění nic na základním paradigmatu, podle něhož je-li základní či jedinou příčinou újmy selhání stroje, je z trestně právního hlediska důležité, zda jde to selhání zaviněné či nezaviněné. Jak známo, civilní právo zná i objektivní odpovědnost za následek – viz výše, tu ale nyní nezkoumáme. Zkoumáme, co lze v případě ještě označit za zavinění ve smyslu trestního zákoníku, tj. kdy půjde o zavinění, a kdy o událost, která nebyla zaviněna jednáním fyzické či právnické osoby. Například zda jde o nezaviněné selhání či havárii, obecně coby důsledek náhody, resp. i nešťastné náhody. Toto bipolární schéma – zavinění vs. náhoda jistě platí i u robotů, pokud problém zjednodušíme a neuvažujeme jednání trestně neodpovědných osob, jakož i jednání za okolností vylučující trestní odpovědnost, např. stav přípustného rizika. Problém je ale s rozlišením, které je či spíše bude velice obtížné tam, kde robot má značnou autonomii jednání a nadto se může i učit, či samo-programovat. (Učením se pouze nastavuji parametry nějakého fixního systému situačního klasifikátoru, neuronové sítě, produkčního systému atp., zatímco samo-programováním lze podstatně modifikovat rozhodovací principy, které chování robota ovlivňují.)

A. Nepochybně již dlouhá léta fungují roboti či robotické systémy, které v řízených vnějších podmínkách vykonávají stále stejné opakující se operace (typicky průmyslové, montážní roboty/manipulátory). Manipulátory ve výrobní lince, které pokud někdo přímo nevstoupí do jejich operačního pole, jsou z hlediska níže uvedené úvahy, prakticky neškodné.

B. Pak jsou ale roboty, které obecně pracují v prostředí s proměnlivými až velmi proměnlivými vnějšími okolnostmi, tedy v prostředí s nejistotou. Mezi tyto okolnosti patří i možnost kolize s někým jiným, ať již s člověkem nebo jiným robotem, či jinou věcí movitou či nemovitou. Typicky to jsou roboticky řízená auta, různé autonomní logistické mobilní roboty apod. Nicméně jde o roboty, kteří mají sice možná rozsáhlou, ale předem definovanou, a tedy i předvídatelnou škálu reakcí a postupů. Jinak řečeno, vše, co umí, do nich vložil člověk prostřednictvím programu.

C. Autonomní systémy, učící se roboti, inteligentní roboti, hybridní roboti apod. jsou složitá zařízení, někdy v kombinaci „živého“ (biologické struktury) a „neživého“, jejichž reakce a postupy již tak předvídatelné nejsou, protože se v nějaké míře, větší či menší, programují sami v rámci oné sebeedukace, případně přejímají vzory jednání člověka, resp. většího okruhu osob. S pokračující mírou autonomie ale stále méně víme, resp. jsme schopni zjistit, co se v „mozku“ takového zařízení odehrává, či odehrálo před určitým incidentem.

Z hlediska trestní odpovědnosti bude třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti. V případě úmyslu hovoříme o úmyslu přímém a úmyslu eventuálním, přičemž pachatel si je vědom toho, že svým činem může způsobit protiprávní následek, nebo je s tím srozuměn (srozuměním se rozumí i smíření pachatele s tím, že způsobem uvedeným v trestním zákoně může porušit nebo ohrozit zájem chráněný takovým zákonem).

Limitem trestní odpovědnosti z nedbalosti je § 16 zákona č. 40/2009 Sb., trestního zákoníku:
(1) Trestný čin je spáchán z nedbalosti, jestliže pachatel a) věděl, že může způsobem uvedeným v trestním zákoně porušit nebo ohrozit zájem chráněný takovým zákonem, ale bez přiměřených důvodů spoléhal, že takové porušení nebo ohrožení nezpůsobí, nebo b) nevěděl, že svým jednáním může takové porušení nebo ohrožení způsobit, ač o tom vzhledem k okolnostem a k svým osobním poměrům vědět měl a mohl.
(2) Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.

Vyloučíme-li úmysl, nedbalost hrubou a vědomou, je v případě strojů zařaditelných do kategorie ***A*** relativně snadné určit, co měl ten, kdo robota provozuje vědět měl, ač tvrdí, že to nevěděl. Je to dáno tím relativně snadnou předvídatelností toho, co lze od robota očekávat.

U kategorie ***B*** už je situace složitější. Zde už může být problém dovodit, co provozovatel robota měl vědět, aby bylo možné posuzovat jeho jednání jako zavinění ve formě vědomé nedbalosti. Tedy do jaké míry například může již zmiňovaný řidič spoléhat na to, že systém ovládaný aktivním radarem zabrzdí jeho auto před překážkou, když to dělá běžně a toto je jasně deklarováno i v návodu. A dokonce je auto vybaveno signalizací poruchy tohoto systému. Je spoléhání na tento systém přiměřeným důvodem nemít nohu na brzdě, když se auto blíží k překážce? Anebo – což je ještě fatálnější – když náhle někdo vstoupí do vozovky?

Ještě větším problémy přinese užívání prakticky zcela autonomních robotů, které jsou zmíněny v kategorii ***C***. U této skupiny bude zřejmě i problém prokazovat i úmysl. Pokud například „myslící“ robot sestrojí jiného robota, který místo aby zvedal břemena a nakládal je do drtičky, naloží do drtičky obsluhu, bude především zjišťována technická příčina selhání robota. Ale paralelně bude nutno se zabývat i tím, stejně jako v případě jakékoliv jiné

průmyslové havárie, zda provozovatel případně výrobce (původního robota) udělali vše, aby k takovému selhání nedošlo. Aby například „myslící" robot nevyrobil místo funkčního robota zmetek. Což ovšem zase znamená zjistit, co onen „myslící" robot vlastně vyrobil a hlavně proč.

Významné bude, zda potenciálnímu pachateli byla pro provozování robota uložena zákonem nebo případně podzákonným či dokonce interním předpisem povinnost určitého chování. V souvislosti s roboty to mohou být zcela obecně předpisy, jako je třeba zákoník práce v oblasti týkající se bezpečností a ochrany zdraví při práci, nebo ochrana obecně prospěšných zařízení, stejně jako Nařízení EU o zdravotnických prostředcích [17] nebo připravovaná legislativa EU popsaná v odstavci 1. A zda dotyčná osoba úmyslně či z nedbalosti jednala v rozporu se svými povinnostmi. Což může být kvalifikováno jako úmysl, nedbalost anebo opomenutí. V této souvislosti se jako relevantní jeví rozhodnutí Nejvyššího soudu ČR ze dne 12. 10. 2017, spis. zn. 6 Tdo 1062/2017-28: „*Za porušení důležité povinnosti ve smyslu § 143 odst. 2 trestního zákoníku není možné považovat porušení jakéhokoli předpisu, ale jen takové v něm zakotvené povinnosti, jejíž porušení má zpravidla za následek nebezpečí pro lidský život nebo zdraví, jestliže jejím porušením může snadno dojít k takovému následku a také k němu často dochází. Rozhodujícím hlediskem při posuzování, zda jde o důležitou povinnost, je zvážení toho, jaký následek a s jakou pravděpodobností z porušení konkrétní povinnosti plyne. Aby bylo možno opomenutí klást na roveň konání, musí se jednat o opomenutí zvláštní povinnosti vyplývající z konkrétního postavení pachatele, tedy jde o situaci, ve které společnost s konáním určité osoby předem počítá a spoléhá na ni. Osoba, která má zvláštní povinnost konat, je předem v konkrétním vztahu k chráněnému zájmu. Jestliže není možno takovou konkrétní povinnost konat z postavení pachatele dovodit, chybí jednání jako podmínka trestní odpovědnosti.*"

Budeme tedy vycházet z výše uvedeného a chápat robota jako systém sestávající kromě ryze mechanických součástek, které umožňují něco konat, především z počítačového hardware a software, který sice není v biologickém smyslu živý, ale má schopnost samostatného učení na základě zkušeností a interakce, je autonomní díky senzorům nebo výměně dat s okolním prostředím a má schopnost přizpůsobit své jednání a svou činnost okolnímu prostředí. Jinými slovy, jednání robota navenek je dané dílem primárním vnitřním nastavením (původním programem, vytvořeným člověkem) a dílem následným přetvářením tohoto programu AI, které může spočívat v různých krocích:

- parametrizaci,
- vytváření databáze vzorů (modelů, heuristik),
- ale na vyšší úrovni přetvářením výchozí neuronové sítě na základě výše uvedených interakcí s okolím, tedy tím, co se nejvíce blíží lidskému pojmu „učení".

Mimořádně obtížné může být v takovém případě hledání příčinné souvislosti mezi selháním robota a jednáním těch, kteří ho vyrobili a naprogramovali. A teprve poté, kdy tato příčinná souvislost bude spolehlivě zjištěna (prokázána), lze se zabývat i případným zaviněním fyzické nebo právnické osoby z hlediska její případné trestněprávní odpovědnosti.

2.5. Příčinná souvislost v robotice

Jak již bylo zmíněno výše, zdrojem dalších obtíží nepochybně bude zjišťování a případně prokazování příčinného vztahu mezi jednáním a následkem – nález Ústavního soudu ČR ze dne 1. 11. 2007, sp. zn. I. ÚS 312/05. U medicínsko-právních sporů, kdy známe vstupní jednání, známe i následek, ale vlastní průběh je zcela nejasný, se mluví o tzv. fenoménu černé skříňky [18]. V takových záležitostech jde většinově o zavinění (obvykle nevědomou nedbalost), a tedy předvídatelnost následku. O kauzálním nexu nebývá sporu, nejde-li o působení více faktorů.

Selže-li zásadním způsobem robot 3., a především 4. kategorie, jak jsou popsány výše, bude namnoze velkým problémem hledání kauzálního řetězce mezi příčinou a následkem. Nadto s nejistým výsledkem. Zde totiž nemusíme vždy znát všechny faktory, která ovlivnily fungování např. autonomního mechanismu. Můžeme znát jeho vstupní nastavení (resp. jaké mělo být, nedošlo-li k nějaké chybě při vývoji nebo výrobě), otázkou ovšem je, zda zjistíme, jaké všechny informace ovlivnily fungování robota. Také prozkoumání oné „černé skříňky", budeme-li za ni považovat hardware a software robota, nemusí být za určitých podmínek úspěšné či dokonce realizovatelné (u biorobota), jakkoliv v současnosti to je zatím stále snáze uskutečnitelnější nežli zjištění všech procesů probíhajících v lidském těle.

Dalším problémem může být možná multikauzalita, kdy může dojít k souběhu nebo kumulaci více možných příčin negativní (deliktní) události, z nichž bude nutné vybrat jednu jako příčinu v daném případě rozhodující. Tím může být např. současná kombinace vstupních dat (tedy okolí robota), programu, který je vyhodnotí, a případně hardware (např. mechanické ruky), která učiní pohyb, jež bude mít za následek deliktní jednání. Jednou z možností by snad mohlo být vyjádření procentuálního poměru těchto vlivů, pokud to ovšem bude možné. K tomuto se jeví vhodné citovat usnesení Nejvyššího soudu ze dne 27. 2. 2002, sp. zn. 3 Tz 317/2001, podle kterého „*Příčinná*

souvislost mezi jednáním pachatele a následkem se nepřerušuje, jestliže k jednání pachatele přistoupí další skutečnost, jež spolupůsobí při vzniku následku, avšak jednání pachatele zůstává takovou skutečností, bez níž by k následku nebylo došlo.“

Příkladem může být ovladač pohybů robota, který nepředpokládá, že by se jeho rameno mohlo dostat do určité polohy prostě proto, že je naprogramován tak, aby tato poloha byla vyloučena. Pokud někdo násilím rameno do takové polohy uvede, čímž dojde k ovlivnění funkčnosti a bezpečnosti robota tak, že dalším pohybem se dostane do jiné, nepředvídatelné polohy, kde zraní jinou osobu, nelze přičítat odpovědnost programátorům, neboť bez zmíněného zásahu by k tomuto účinku vůbec nedošlo. Z toho lze odvodit jeden z hlavních požadavků na roboty: maximální vytváření tzv. auditní stopy, vypovídající o každém kroku robota a o jeho vnitřním stavu.

2.6. Nepředvídatelné chování robotů

Nepředvídatelné chování robotů může mít různé příčiny, od hardwarových závad až po softwarové chyby. Mezi běžné příčiny patří:

1. Hardwarové závady: Roboty se skládají z různých součástí, jako jsou senzory, aktuátory a řídicí systémy, které mohou selhat a způsobit nepředvídatelné chování.
2. Softwarové chyby: Roboty se spoléhají na složité softwarové systémy a chyby v kódu mohou způsobit neočekávané chování.
3. Nesprávně kalibrované senzory: Pokud nejsou senzory robota správně kalibrovány, může to vést k nesprávným údajům a nepředvídatelnému chování.
4. Rušení z okolí: Roboty mohou být ovlivněny vnějšími faktory, jako je elektromagnetické rušení, které může způsobit nepředvídatelné chování.
5. Nedostatečné testování: Pokud robot nebyl důkladně otestován, může v reálných scénářích vykazovat nepředvídatelné chování. Kvalita testování je klíčovým předpokladem minimalizace rizika. Vhodné je postupovat tak, že komponenty systému jsou rozděleny na jednotlivé funkčnosti, které mohou být popsány jednoduchými konečnými automaty, jejichž chování lze z velké části analyzovat úplným způsobem.

Pro řešení nepředvídatelného chování robotů je důležité diagnostikovat hlavní příčinu důkladným testováním a laděním. V některých případech může být nutné vyměnit hardwarové komponenty a v jiných, pravděpodobně častějších případech může být nutné aktualizovat nebo zcela přepsat software.

Zde zřejmě bude vhodné vycházet z principu „potřebné (požadovatelné, rozumné) míry opatrnosti“, která by měla být výrobcem robota zakotvena v principu *secure by design*, což znamená, že navržený výrobek (můžeme tak chápat celého robota nebo jen jeho software) je od samého počátku vývoje a ve všech jeho etapách konstruován tak, aby byl bezpečný [4]. Problém je ale dán tím, že ani hardware, ani software není možné prohlásit jako zcela prosté všech chyb s pravděpodobností 100 %. A pokud k tomu připočítáme ještě nutnou spolehlivost komunikace, pak i při spolehlivosti systému 99,9999 % může činit výpadek u robota neuvěřitelně dlouhých 31,5 sekund!

Většina textů zabývajících se bezpečností (a to nejen v souvislosti s informačními systémy či roboty) zdůrazňuje, že nezbytným krokem pro zvýšení bezpečnosti (a tedy i snížení pravděpodobnosti provozní havárie a případné následné odpovědnosti) je existence systému řízení rizik (nejznámější je norma ISO/IEC 27001, doplněná dalšími normami z řady 270xx). Při posuzování konkrétních případů pak to bude zřejmě otázka věcná, následně však i právní, zda se jednalo o riziko běžné či mimořádné, předvídatelné či nepředvídatelné, a jaká byla učiněna opatření pro jeho minimalizaci.

Ani v běžném životě se nemůžeme vyhnout situacím, kdy vznik jakékoliv škody není zcela vyloučen. V každém konkrétním případě se proto z tohoto hlediska musí zkoumat, jak dalece bylo možné vznik škodlivého následku vůbec předvídat a jaká dostupná opatření byla nebo mohla být provedena, aby případný škodlivý následek byl minimalizován. Podle ustanovení § 31 odst. 2 trestního zákoníku „*Nejde o přípustné riziko, jestliže taková činnost ohrozí život nebo zdraví člověka, aniž by jím byl dán k ní v souladu s jiným právním předpisem souhlas, nebo výsledek, k němuž směřuje, zcela zřejmě neodpovídá míře rizika, anebo provádění této činnosti zřejmě odporuje požadavkům jiného právního předpisu, veřejnému zájmu, zásadám lidskosti nebo se příčí dobrým mravům.*“

Konstatování, zda šlo či nešlo o přípustné riziko, je primárně věcí soudu. Při posuzování rizika v oblasti robotiky je ovšem velmi pravděpodobné, že bude nutno zohlednit nejen současný stav poznání, ale – v případě skokové změny technologie, která bude již mimo rámec tohoto stavu poznání – posoudit zcela novou situaci. Pokud byla provedena analýza rizik zahrnující všechny možné (předpokladatelné) škodlivé situace, vyloučena rizika činností,

která způsobí újmu na zdraví, smrt nebo větší hmotnou škodu, a zároveň je patrné, že zamýšleného (a legálního) cíle nelze dosáhnout jinak, lze přistoupit k jednání, jež vykazuje prvky rizika a následně by dodržení těchto podmínek mělo být zohledněno při posuzování okolností vylučujících protiprávnost.

Konkrétní příklady, které se mohou vyskytnout, pak budou různé podle stupně autonomie robota a dalších okolností. Může se vyskytnout taková chyba v programu, která způsobí, že činnost robota bude nejen neaprobovatelná, ale i ohrožovat zájem chráněný trestním zákoníkem; taková chyba, jakkoliv by se to nemělo stát, není nemožná, ovšem podstatná bude existence a funkčnost bezpečnostního mechanismu, který zastaví robota dříve, nežli k incidentu dojde. Jedním z kritérií pro posuzování případné odpovědnosti je provedení či neprovedení funkčních zkoušek před zahájením výroby.

2.7. Další faktory ovlivňující činnost robotů

Zde je nutno upozornit na existenci dalších faktorů, majících vliv na jednání robota. Každý program pracuje s daty, přičemž některá data mohou být zadávána jako konstanty (např. výrobcem), jiná jako proměnné (např. uživatelem) a jiná může získávat robot sám prostřednictvím čidel (senzorů) nebo v rámci výuky prostřednictvím datasetů (Big data). Takže opět může dojít i při bezchybném fungování programu k nesprávnému (neaprobovanému) jednání robota, přičemž pouze v prvních dvou případech bude zřejmě snadno zjistitelné, co se stalo. Pokud bude daný případ v sobě zahrnovat ovlivnění vnějšími faktory, a to neúmyslné i úmyslné, budeme opět závislí na možnosti analyzovat procesy uvnitř robota.

Neúmyslné ovlivnění může nastat např. kombinací vnějších signálů sejmutých senzory robota, které budou chybně vyhodnoceny a nastane incident. Pak je otázkou posoudit, zda se jednalo natolik o neočekávanou, ale i neočekávatelnou situaci, kterou nemohl výrobce předvídat. Vyloučí-li analýza, že nejde o zmíněnou nepředvídanou a neočekávatelnou situaci, stejně jako že došlo k selhání robota z důvodů spojených s ním samotným (vada konstrukce, programu apod.), budeme muset přepokládat, že šlo o situaci předvídatelnou, která mohla být zčásti nebo zcela vyvolána vnějším vlivem včetně zásahu jiné osoby. A v případě zjištění lidského faktoru bude třeba (kromě zjištění této osoby) řešit otázku úmyslu versus nedbalosti, jak již bylo popsáno výše. Lze si představit nedbalé jednání někoho, kdo mimoděk nebo v souvislosti s jinou činností změní fyzickou konfiguraci robota, jenž se začne pohybovat po jiné dráze.

V případě úmyslu se může jednat o útok zvenčí, kdy se útočník bude snažit ovlivnit procesy probíhající v robotovi natolik, aby došlo ke změně jeho funkcí či fungování a následně ke vzniku incidentu. Ten, kdo může ovlivnit robota k jednání způsobem který ohrožuje zájem chráněný trestním zákoníkem, může být v podstatě kdokoliv: majitel (uživatel, operátor apod.), který mu (vědomě či nevědomě) zadá chybná data – pak se zřejmě budeme pohybovat v oblasti posuzování případného nedbalostního jednání při protiprávním činu, možná ale i naplnění skutkové podstaty trestného činu „Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti“. V případě jiné třetí osoby (hackera), který může provést útok na program ovládající robota (ale samozřejmě i na data) s cílem, aby robot učinil něco, co není v souladu s jeho určením, je situace jednoznačnější. Pak se bude jednat o zneužití věci (použití robota jako předmět nebo nástroj trestného činu).

Majitelé (provozovatelé, uživatelé) robotů, jejichž činnost může v případě poruchy způsobit obecné ohrožení (kvůli váze, povaze činnosti atd.), případně jejichž provoz lze označit dnešním pojmem „zvlášť nebezpečný“ (ustanovení § 2925 občanského zákoníku „Škoda způsobená provozem zvlášť nebezpečným“), mohou být také trestně odpovědni za případnou havárii, způsobenou robotem.

„*Provoz zvlášť nebezpečný je soustavně prováděná činnost fyzické nebo právnické osoby, s níž je spojena možnost zvýšeného nebezpečí vzniku závažných škod. Zvlášť nebezpečná je podle speciálního vymezení ve třetím odstavci vždy tovární výroba, výroba výbušnin či podobně nebezpečných látek (jedů, toxických látek). Provoz továrním způsobem je potom pravidelná, soustředěná a organizovaná velkovýroba, při níž se činnost více pracovníků dělí mezi jednotlivé tovární úseky* [19].“

Jakkoliv jde o oblast práva občanského, při posuzování charakteru provozu, ve kterém došlo k deliktnímu jednání a naplnění skutkové podstaty určitého trestného činu, bude s největší pravděpodobností posuzován a priori daný charakter provozu vždy individuálně a podle obdobných principů.

Jejich deliktní odpovědnost, co se týká nedbalostního jednání, pak může mít přinejmenším dvě roviny:
- postupovali v rozporu s pokyny (příručkou) výrobce, např. přetížením robota, nedostatečnou údržbou, neproškolenou obsluhou apod.,
- nezachovali potřebnou míru opatrnosti, kterou by vzhledem k vlastnostem daného robota měli dodržovat.

3. ZÁVĚR

Odpovědnost za nezákonné nebo trestné jednání robotů nebo obecně systémů AI je složitá otázka, kterou právní systém dosud plně nevyřešil. V některých případech může být odpovědný výrobce robota, pokud se prokáže, že robot byl vadně navržen nebo vyroben. V jiných případech může být odpovědný vlastník robota, pokud byl robot používán nezákonným způsobem, například pokud byl naprogramován k páchání trestné činnosti. Mohou se však vyskytnout i případy, kdy může být faktorem programování nebo data použitá k tréninku systému AI, a v takovém případě by mohl být odpovědný i programátor nebo poskytovatel dat. Nelze vyloučit ani odpovědnost regulačních orgánů: pokud neexistovaly jasné předpisy nebo technické normy pro výrobu a/nebo bezpečné používání robota, mohou být regulační orgány činěny odpovědnými za to, že na technologii řádně nedohlížely.

Odpovědnost za jednání robotů bude nakonec pravděpodobně určována případ od případu s přihlédnutím k řadě faktorů, včetně konkrétních okolností situace, konstrukce a schopností robota a platných zákonů a obecně závazných technických předpisů. Nicméně s tím, jak se roboti stávají pokročilejšími a autonomnějšími, je stále obtížnější určit, kdo by měl primárně nést odpovědnost za jejich jednání.

Usnesení Evropského parlamentu ze dne 16. února 2017 [20] uvádí v čl. 12, že „*by mělo být vždy možné podat odůvodnění každého rozhodnutí učiněného s pomocí umělé inteligence, které může mít významný dopad na život jedné nebo více osob*“. Evropský parlament se domnívá, že „*výpočetní činnost systémů umělé inteligence by mělo být vždy možné převést do formy pochopitelné pro člověka, a že pokročilí roboti by měli být vybaveni „černou skříňkou“, kde budou zaznamenávány údaje o každé operaci, kterou daný stroj provede, včetně logiky, na níž se jeho rozhodnutí zakládají*“. Problémem bude, zda se nám u skutečně vyspělých robotů, např. vybavených neuronovými mozky (lhostejno, zda umělými nebo biologickými) podaří všechna rozhodnutí robota převést do formy pochopitelné pro člověka, a ještě více, zda bude možno vůbec zjistit logiku, na níž se jeho rozhodnutí zakládají. Tato „černá skříňka“, pokud bude obsahovat skutečně všechny potřebné informace (inspirovat se můžeme v oboru letectví), může sloužit jako auditní stopa představující významný, ne-li hlavní či dokonce jediný důkaz při zjišťování, co se v rámci incidentu odehrálo, jaký byl stav robota a kdo či co jej způsobilo. Z toho potom můžeme dojít k závěru na otázku položenou v úvodu tohoto článku: jednalo se o zavinění úmyslné, nedbalost, náhodu či totálně nepředpokladatelnou událost – Černou labuť [21]?

Rozvoj schopností autonomních mechanismů a jejich rozumových schopností bude proto velkou výzvou i pro oblast trestního práva a kriminalistiky. Přitom potenciální útočníci budou stále schopni nacházet nové možnosti útoků. „*Pokročilé útočné strategie jsou silně polymorfní, neopakují přenosy týchž binárních sekvencí, nepřistupují opakovaně na stejné servery atd. … Lze očekávat další výrazný nárůst ekonomicky motivovaných a cílených útoků na podnikovou výrobní infrastrukturu. V případě dopravy je velmi důležitou otázkou také bezpečnost autonomních vozidel. Vážnou hrozbou jsou trestné činy zaměřené nejen proti autonomním vozidlům (např. krádeže vozidel), ale i trestné činy páchané pomocí autonomních vozidel (např. možnost teroristického útoku pomocí autonomního vozidla naloženého trhavinou a naprogramovaného do cílového místa útoku)* [22].“

Je třeba se připravit jak v oblasti právní teorie a praxe, promítnuté do legislativy a rozhodovací praxe soudů, v oblasti technologické, promítnuté do normotvorné činnosti a vytváření „best practices“, jakož i do oblasti kriminalistické, promítnuté do vzniku nových postupů, případně podoblastí v rámci oboru kriminalistiky. Aplikace metodik a nástrojů, jako jsou Big Data, AI a digitální dvojčata by mohlo zvýšit výtěžnost zaznamenávaných dat (logování, auditní stopa), a tedy i napomoci ke snížení entropie v rámci konkrétního vyšetřování trestné činnosti související s roboty.

LITERATURA

[1] EVROPSKÁ KOMISE. *Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) a mění určité legislativní akty unie*. Brusel: EU 2021. COM(2021) 206 final 2021/0106 (COD).

[2] EVROPSKÁ KOMISE. *Návrh směrnice Evropského parlamentu a Rady o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligenci (směrnice o odpovědnosti za umělou inteligenci).* Brusel: EU 2022. COM(2022) 496 final.

[3] SMEJKAL, V., SOKOL, T. Trestněprávní aspekty robotiky. *Právní rozhledy,* XXVI. (2018), 15-16, pp. 530-540.

[4] SMEJKAL, V. *Kybernetická kriminalita*. ISBN 978-80-7380-849-5. 3. vyd. Plzeň: Aleš Čeněk 2022, 831 p.

[5] ASIMOV, I. Runaround (Hra na honěnou). *Astounding Science Fiction.* 1942. hptts://otechnice.cz

[6] CALO, R. Robotics and the Lessons of Cyberlaw. *California Law Review,* 103 (2015), 4, pp. 513-563.

[7] INTERNATIONAL FEDERATION OF ROBOTICS. https://ifr.org/standardisation.
[8] ISO. *ISO 8373:1994 Manipulating Industrial Robots – Vocabulary*. https://www.iso.org/stadard/15532.html.
[9] KROMPOLC, T. Co stálo v pozadí nehod Boeingu 737 MAX? Pomalé inovace i snaha ušetřit. *Smartmania, 21. 7. 2021*. https://smartmania.cz/co-stalo-v-pozadi-nehod-boeingu-737-max-pomale-inovace-i-snaha-usetrit/.
[10] LEGGETT, T. Boeing 737 Max Lion Air Crash Caused by Series of Failures. *BBC News*, 25 October 2019. https://www.bbc.com/news/business-50177788.
[11] FIKES, R. E., NILSSON, N. J. STRIPS: A New Approach to the Application of Theorem Proving to Problem Solving. *Artificial Intelligence*, 2 (1971), 3–4, pp. 189-208.
[12] VON NEUMANN, J. First Draft of a Report on the EDVAC. Lecture 30. 6. 1945, University of Pennsylvania. *IEEE Annals of the History of Computing*, 15 (1993), 4, pp. 27-47.
[13] KULHÁNEK, P. Kvantový počítač IBM Q. *Aldebaran Bulletin*, XV.(2017), 38. https://www.aldebaran.cz /bulletin/2017_38_ibq.php.
[14] ARUTE, F., ARYA, K., BABBUSH, R. *ET AL*. Quantum Supremacy Using a Programmable Superconducting Processor. *Nature*, 574 (2019) , pp. 505–510. Doi:10.1038/s41586-019-1666-5.
[15] MICROSOFT. Co je Azure Quantum? 15. 8. 2023. https://learn.microsoft.com/cs-cz/azure/quantum/overview-azure-quantum.
[16] VOJÁČEK, A. Obecná problematika použití umělé inteligence v průmyslových aplikacích. automatizace.hw.cz, 18. 4. 2019. https://automatizace.hw.cz/obecna-problematika-pouziti-umele-inteligence-v-prumyslovych-aplikacich.html.
[17] EVROPSKÝ PARLAMENT, RADA EU. Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS. *Úřední věstník*, L 117, pp. 1–175..
[18] DOLEŽAL, A., DOLEŽAL, T. *Kauzalita v civilním právu se zaměřením na medicínskoprávní spory*. Praha: Ústav státu a práva AV ČR 2016.
[19] JIRSA, J., SVĚŽENOVÁ, L., VEČEŘA, J. a HOLUB, T. *Občanský zákoník. Komentář s judikaturou. Svazek XIII – Závazky z deliktů a z jiných právních důvodů (§ 2894–3014)*. ISBN 978-80-7624-007-0. Ostrava: CODEXIS publishing 2018.
[20] EVROPSKÝ PARLAMENT. *Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení Komisi o občanskoprávních pravidlech pro robotiku*. 2015/2103(INL)). P8_TA(2017)0051.
[21] TALEB, N. N. *The Black Swan. The Impact of the Highly Improbable*. ISBN 978-07139 9995-2. London: U Penguin Books Ltd. 2008, 400 p.
[22] MINISTERSTVO PRŮMYSLU A OBCHODU ČR. *Iniciativa Průmysl 4.0*. Praha: vláda ČR 2016.

ZMĚNY V ŘEŠENÍ TECHNICKÉ INFRASTRUKTURY SÍDEL JSOU JIŽ NUTNÉ

CHANGES IN SOLUTIONS OF TECHNICAL INFRASTRUCTURE IN CITIES AND VILLAGES ARE ALREADY NECESSARY

Petr Šrytr, Lenka Střelbová

ČVUT v Praze. Fakulta stavební, Thákurova 7, 166 00 Praha 6. srytr@fsv.cvut.cz, lenka.strelbova@fsv.cvut.cz

Abstrakt: Vývoj podmínek řešení technické infrastruktury sídel se dostává do stádia, kdy jsou nezbytné radikální změny v užití adekvátních nástrojů řešení včetně užití těmto změnám přizpůsobených nástrojů typu *risk management a management kritické infrastruktury*. Demonstrace této situace je cílem příspěvku.

Klíčová slova: Stavební průmysl, řízení rizik, technická infrastruktura, kritická infrastruktura, udržitelný stav a rozvoj.

Abstract: The development of the conditions for the solution of the technical infrastructure of settlements is getting to the stage where radical changes in the use of adequate solution tools are necessary, including the use of tools adapted to these changes, such as *risk management* and *critical infrastructure management*. Demonstrating this situation is the aim of the article.

Key words: Building industry, risk management, technical infrastructure, critical infrastructure, sustainable conditions and development.

1. ÚVOD

Je především nutné se orientovat na zpřehlednění nejvýraznějších problémů spojených s aplikací nástroje pro kontrolu a řízení rizik technické infrastruktury sídel/TIS, zejména pak nejzranitelnějších subsystémů inženýrských sítí/IS, nástroje, označovaného jako *Risk Management*.

Technická infrastruktura sídel/TIS je přestavována především systémy jejich technické obsluhy typu zásobování vodou, odkanalizování území včetně čištění odpadních vod, zásobování energiemi (plošnou elektrifikací, plynofikací a teplofikací), typu telekomunikační obsluhy území, dále systémy odstraňování odpadů, systémy monitoringu čistoty ovzduší, systémy městského mobiliáře, vlastně i systémem městské zeleně atp. Ve správním území sídel pak se jedná o zařízení, které je součástí veřejného prostoru, ve kterém je soustředěna celá řada dalších aktivit (narůstajících co do svého počtu, kvality i rozsahu) včetně dominantních aktivit dopravních. To vše pak zcela oprávněně řadíme mezi tzv. *civilizační hodnoty*, o kterých nepochybujeme a kterých se vlastně ani nemůžeme a nesmíme vzdát, máme-li mít jako uživatelé sídel a celého urbanizovaného území šanci na adekvátní úrovni přežít a civilizační procesy dále rozvíjet.

C*ivilizační hodnoty* tohoto typu pak vnímáme tak, že je považujeme za zcela samozřejmé, že je máme permanentně s dostatečnou garancí k dispozici. Vůbec si vlastně příliš nepřipouštíme existenci rizik, že by se mohlo případně stát, že nám delší dobu nepoteče voda do kuchyně, na a z WC či do a z koupelny, že budeme často vystaveni jevům označovaným jako *blackout*, že budeme strádat z důvodu nedodávky jiných energií, že budeme strádat z důvodů disfunkce telekomunikační obsluhy, že budeme strádat z důvodů disfunkce komunálních služeb nakládání s odpady atd.

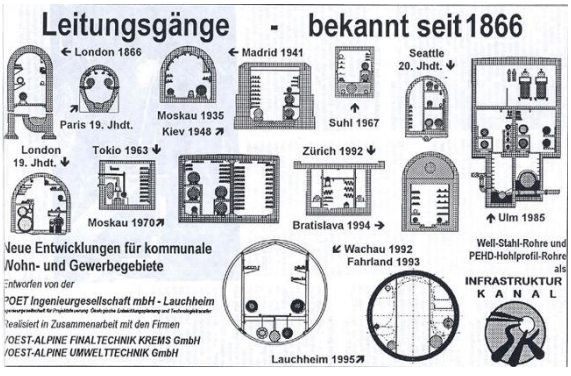
Podrobná a úplná analýza stavu podzemí veřejného prostoru našich měst a obcí (je-li to vůbec reálné dokonale zvládnout) by s největší pravděpodobností jen potvrdila to, co již dlouhodobě víme z opakovaných přímých vizuálních zjištění při prakticky improvizovaném odstraňování havárií a poruch vedení technického vybavení/VTV, při rozsáhlejších investičních akcích ve veřejném prostoru, při akcích obnovy a kompletace VTV (jsou však dnes již k dispozici nedestruktivní technologie průzkumu podzemí, ale jsou v ČR zatím využívány jen omezeně, zřejmě z důvodu problematických úspor nákladů či z důvodu omezeného času pro kvalitní přípravu investičních akcí apod.). Taková analýza by nabídla zcela srozumitelné poznatky a zkušenosti, vlastně urgentní výzvu s tím začít konečně něco poctivě dělat, uceleně, tj. systémově řešit a neodkládat to jako zátěž na bedra příštích generací. Jedině tak lze dostatečně pojistit fungování měst a obcí z hlediska udržitelného rozvoje.

Za základ fungování měst a obcí lze logicky považovat jejich schopnost fungovat z technického hlediska. To pak závisí na stavu a úrovni řešení veřejného prostoru včetně všech zařízení a prvků v něm se nacházejících. Vycházíme-li pak z reálného poznatku značně heterogenního a celkově nedobrého stavu a úrovně řešení veřejného prostoru ve městech a obcích v ČR včetně nedostatečné kontroly a absence odpovídajících nástrojů k jejímu zajištění, pak *bychom již měli být všichni oprávněně značně znepokojeni*. Situace se pak bude s největší pravděpodobností čím dále, tím více komplikovat s potenciálně narůstajícím podílem případů havarijních stavů včetně *stavů nouze, stavů obecného ohrožení* a nepřijatelné rozsáhlé disfunkce veřejného prostoru. Navíc je též již dnes možné zaznamenat zásadní disproporce v souvislosti s narůstajícími požadavky na pokrytí nároků rozšiřujících se druhů aktivit, odehrávajících se ve veřejném prostoru. Dostáváme se tak do stádia, kdy je nanejvýš akutní se postarat o nápravu a to, především důslednější koordinací, důslednějším, tj. systémovým řešením všech nazrálých problémů. Začátek tohoto procesu lze spatřovat mj. i v adekvátní revizi a inovaci ČSN 73 6005 *Prostorové uspořádání vedení technického vybavení* a následně i norem a dalších technických podkladů přímo souvisejících. Navíc není v dohledu ani nějaká podobná samospasitelná EN! V jednotlivých státech Evropy i světa byly a jsou natolik odlišné podmínky či specifičnosti, odlišný historický vývoj řešení problémů veřejného prostoru, a proto nikdo zatím nepřichází s takovouto podobnou iniciativou.

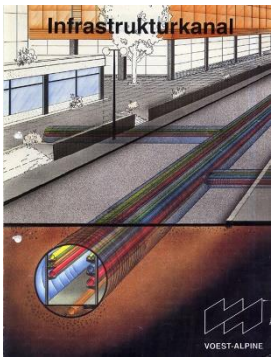
Lze si tedy klást mnoho otázek k adekvátnímu řešení vždy i v konkrétních případech jednotlivých sídel a jejich okolí. Ty základní lze alespoň stručně zpřehlednit:

1. Máme adekvátní garance udržitelnosti vývoje sektoru TIS? - Zatím to nikdo nenabízí.
2. Jak dalece to mají pod kontrolou ti, kteří jsou majiteli a provozovateli TIS a jak jsou schopni preventivně předcházet potenciálním situacím výskytu výpadků/poruch a havárií svých zařízení? – Zatím předvádí, že umí jen improvizovat.
3. Jak dalece to mají pod kontrolou ti, kteří též nesou přímou odpovědnost za dobrou funkci sídel jako celku, tj. managementy měst a obcí a následně i instituce státní správy tyto managementy zastřešující, na ně dohlížející a podporující výkonem státní správy, koordinačně, metodicky i jinak? – Zatím nabízí jen *úřednické triky*.
4. Jak jsou připraveni a jak na to reagují záchranné složky státu? – Zatím nereagují (čekají až na reakci příslušných státních orgánů).

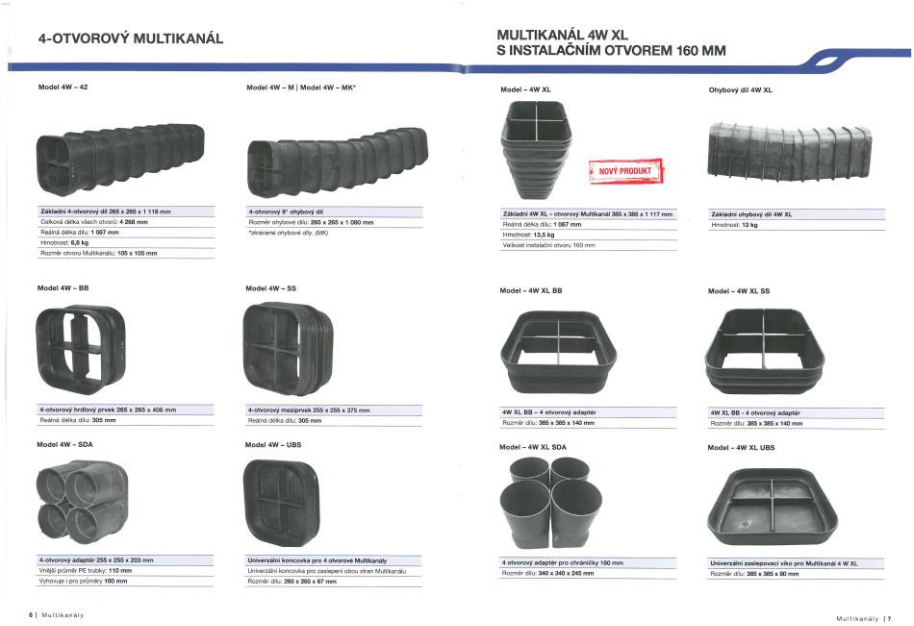
Již na soubor těchto základních otázek není snadné odpovídat a již vůbec ne jednorázově vyčerpávajícím způsobem, jakkoliv je to evidentně ve veřejném zájmu. Jde vlastně o urgentní výzvu s tím začít konečně něco poctivě dělat, systémově řešit a neodkládat to jako zátěž na bedra příštím generacím. Jedině tak lze dostatečně pojistit fungování měst a obcí z hlediska udržitelného rozvoje. V případě TIS je za dané situace především třeba reagovat na faktický stav TIS, na stavy prostorové nouze, na častý výskyt komplikovaných situací, často přímo chaosu ve veřejném prostoru sídel a dále též na požadavky adekvátní zvýšené ochrany TIS ve veřejném prostoru sídel. Adekvátní reakce pak má již své historické kořeny v podobě prosazování adekvátních typů ochranných konstrukcí *sdružených tras* VTV, obrázky 1 až 8 (s tím, že vývoj progresivně pokračuje), či též *kombinovaných tras* v případech, kdy VTV *klasicky ukládané prostě do země* jsou i výhledově budou adekvátně odolné a relativně snadno udržitelné, pod operativní provozní kontrolou svého stavu včetně prokazatelně použitelné adekvátní varianty *bezvýkopové technologie*/BT (*trenchless/bezrýhové technologie)* jejich údržby, opravy, obnovy, kompletace i modernizace [1-5].



Obr. 1a. Příklady výhodného, nutného a zcela logického uplatnění kolektorů a následně i jiných ochranných konstrukcí sdružených tras VTV, které má historicky svůj začátek v Londýně v r. 1866 (ČR v tomto ohledu nezaostala, naopak má dobrou pozici v rámci vyspělých států; šlo však vždy jen o dílčí řešení).

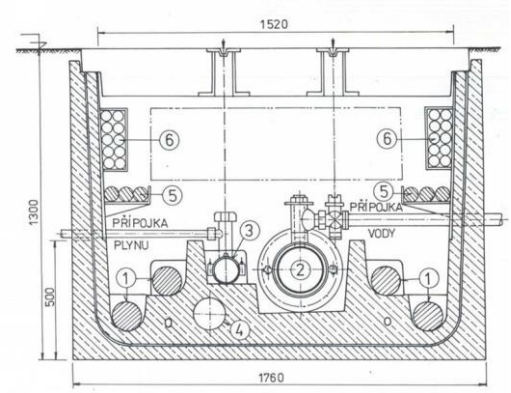


Obr. 1b. Příklad unifikovaného řešení kolektoru *Infrastrukturkanal VOEST-ALPINE* (nabídka typových řešení je dnes dostatečně široká včetně progresivních způsobů realizace, např. BT, technologie *microtunnellig* [9,10].

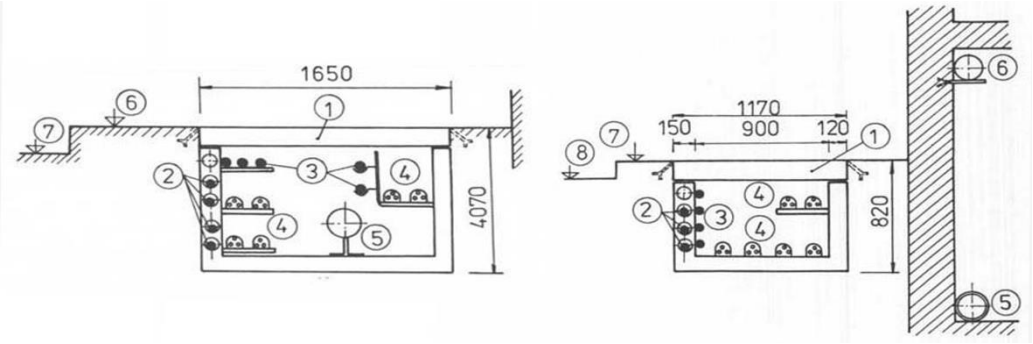


Obr. 2. Příklad aplikace stavebnice multikanálu SITEL (Carson-Brooks), zdroj SITEL s.r.o. (www.sitel.cz) a [11]. Jistým potvrzením dalšího vývoje stavebnice SITEL jsou aktuálně např. její další komponenty pro čtyřotvorový stavebnicový prvek multikanálu SITEL, umožňující instalaci potrubního vedení do velikosti DN 400.

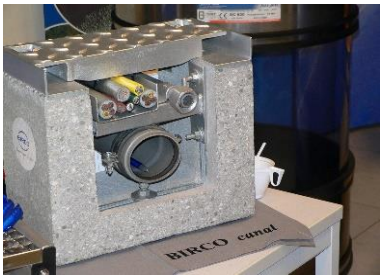
Obr. 3. Příklad sdružené chráničky HYDROS pro vedení 4. kategorie dle ČSN 73 6005, zdroj HYDROS (www.hydros.de).



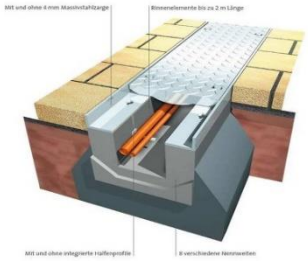
Obr. 4. Příklad podchodníkového technického kanálu typu EUREKA (1-kabely silové VN, 2-vodovod, 3-plynovod *stl/ntl*, 4-chránička, 5- kabely silové NN, 6-vedení elektronických komunikací), zdroj EUREKA (www.eureka.com).



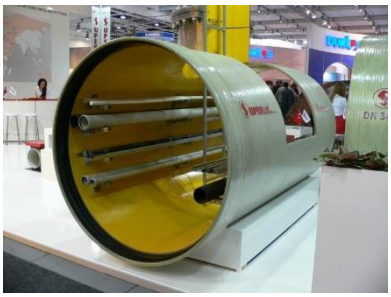
Obr. 5. Příklad podchodníkového technického kanálu typu INTERPROJEKT Praha (1-pochozí snímatelná deska, 2-vedení elektronických komunikací, 3- kabely silové NN, 4-kabely silové VN 22 kV, 5-vodovod DN 200, 6-chodník (alternativně ntl plynovod do DN 150 v případě varianty kombinované se suterénním umístěním; 5 – vodovod, 6 - plynovod), 7- chodník resp. 8-vozovka, zdroj INTERPROJEKT Praha.



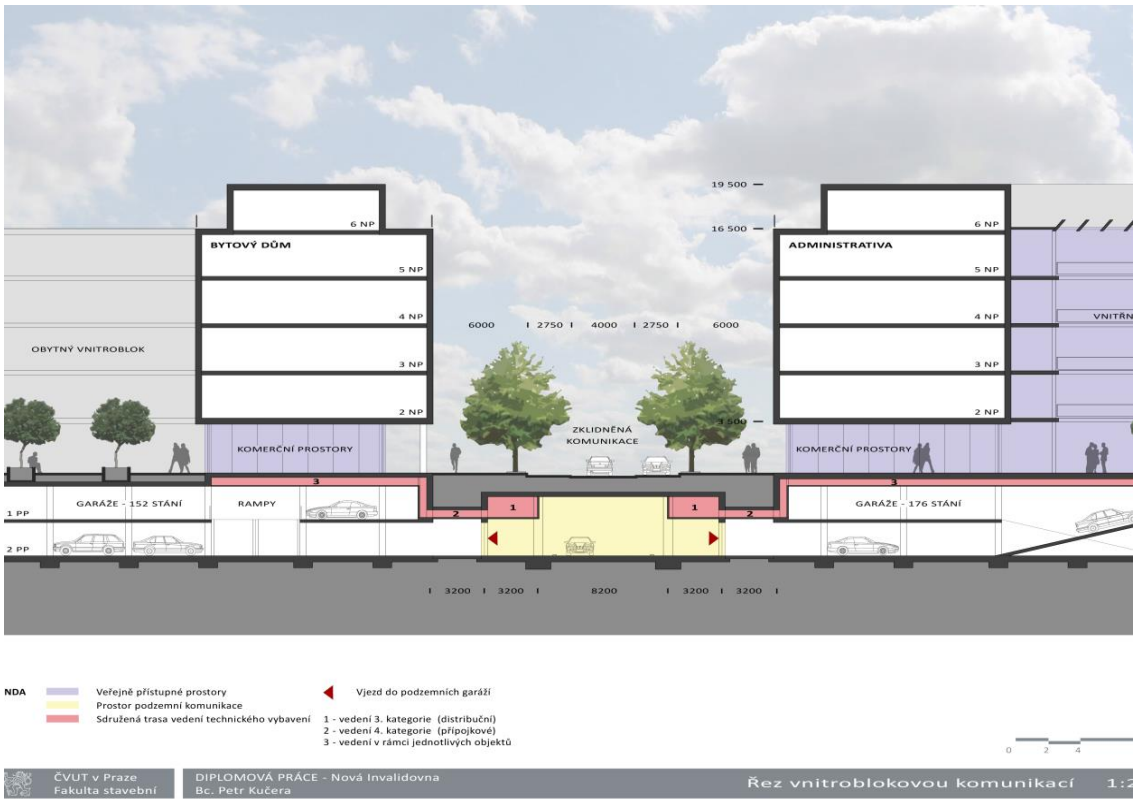
Obr. 6a. Příklad technického kanálu typu BIRCO (výstavní exponát), zdroj BIRCO GmbH (*www.birco.de*).



Obr. 6b. Příklad aplikace technického kanálu typu BIRCO (princip řešení z firemního podkladu), zdroj BIRCO GmbH (www.birco.de).



Obr. 7. Příklad použití technologie mikrotunnelling (plně mechanizovaného štítování) pro realizaci kolektoru užitím trubního prefabrikátu DN 1600 ze sklolaminátu HOBAS.



Obr. 8. Schéma příkladu aplikace řešení užitím *technicko-komunikačního koridoru* (červeně podbarveny plochy technologických profilů sdružených, přípojkových a propojovacích tras IS).

2. SOUHRN POZNATKŮ PRO METODIKU ŘEŠENÍ PROBLEMATIKY

Z metodického hlediska jsme si to mohli konkrétně odzkoušet, jak postupovat v případě plnění požadavku garance udržitelného stavu a vývoje řešení VTV/IS i celého veřejného prostoru, všech jeho funkcí zejména v případě města Tábor [6]. - Aby to bylo dle zadání kdekoliv a kdykoliv zvládnutelné, tak je především třeba mít k dispozici dostatečné podklady a informace (co do přesnosti, úplnosti a kvality). Cesta pro zajištění takovýchto podkladů a informací se ukazuje schůdná prostřednictvím prosazení několika preventivních, progresivních kroků: *zavedení/zajištění nezávislé databáze Facility Management* VTV/ IS a veřejných prostorů zájmového území (např. buď prostřednictvím samostatné společnosti *technických služeb*, zřízené městským či obecním úřadem nezasahujícím do jeho činnosti apod.). To pak nabízí i adekvátní informace pro zpracování aktualizovaných územně-plánovacích podkladů/ÚPP a územně plánovacích dokumentací/ÚPD a dále též adekvátní zpracování podkladů k zajištění splnění požadavku garance udržitelného stavu a rozvoje VTV/IS daného sídla. Metodicky jsme si to

odzkoušeli pro podstatnou část ul. Budějovické v Táboře a současně doporučili totéž v ucelené podobě provést pro všechny místní komunikace, veřejná prostranství, brownfieldy sídla a jejich okolí.

3. METODIKA ŘEŠENÍ

Zajištění zpracování variantních návrhů týmem odborníků a jejich vyhodnocení metodou *Asset Analyse*/AA (*Asset Management*/AM [7,8], včetně zpracování návrhu *všech návazností výsledných variant v prostorách jejich vzájemného napojení včetně harmonogramu potřebných činností, programu akcí postupného dosažení hlavního cíle i všech dalších potřebných návazností.* Např. využít též poznatků dlouhodobě získaných *působením v terénu*, v mnoha sídlech, např. i ve městě Tábor, viz [6] atp.

Důležité je též alespoň rámcově nabídnout zpřehlednění metodiky řešení rozhodujících problémů včetně adekvátního uplatnění bezvýkopových technologií/BT na konkrétním příkladu. Využít lze např. též poznatků dlouhodobě získaných *působením v terénu*, v mnoha sídlech, např. též ve městě Tábor [6] atp.

4. NÁVRH POSTUPU ŘEŠENÍ

Především je nutné v rámci přípravné fáze udělat aktuální důslednou inventuru stavu uceleného koncepčního řešení celého zájmového území (včetně inventury stavu provozní kontroly , kompletace, výměny/obnovy a modernizace VTV/IS). Aby to bylo dle důsledného zadání kdekoliv a kdykoliv zvládnutelné, tak je především třeba mít k dispozici dostatečné podklady a informace (co do přesnosti, úplnosti a kvality; chybějící podklady a informace je třeba operativně doplnit s využitím moderních technologií). Cesta pro zajištění takovýchto podkladů a informací se ukazuje prostřednictvím prosazení několika preventivních, progresivních kroků: zavedení/zajištění nezávislé databáze Facility Management VTV/ IS a veřejných prostorů zájmového území (např. prostřednictvím samostatné a nezávislé společnosti technických služeb). To pak nabízí i adekvátní informace pro zpracování aktualizovaných územně-plánovacích podkladů/ÚPP a územně plánovacích dokumentací/ÚPD a dále též adekvátní zpracování podkladů k zajištění splnění požadavku garance udržitelného stavu a rozvoje VTV/IS daného sídla. Pečlivě to je třeba provést v ucelené podobě pro všechny místní komunikace, veřejná prostranství i brownfieldy sídla a jejich okolí. Žádoucí je současně usilovat o dostatečně kompaktní podobu struktury města, která umožní aktivně usilovat též o optimální geometrickou strukturu všech IS, všech vedení technického vybavení/VTV včetně uplatnění kvalitních způsobů ukládání IS/VTV a BT. Jakákoliv improvizace a nedůslednost v tomto ohledu pak následně neumožňuje prokazovat splnění požadavku garance udržitelného rozvoje.

Následuje zajištění zpracování variantních návrhů týmem vybraných kvalitních odborníků a jejich vyhodnocení metodou Asset Analyse/AA a Asset Management/A), [6-8], včetně zpracování návrhu všech návazností výsledných variant v prostorách jejich vzájemného napojení a včetně harmonogramu potřebných činností, programu akcí postupného dosažení hlavního cíle i všech dalších potřebných návazností. - V případě plánovaní rozsáhlých investičních akcí se evidentně dostávají do vzájemných zájmových střetů dnes již prakticky intenzivní doprava (působící též produkcí hluku, emisí, otřesů a vibrací, …), bydlení, služby, žádoucí funkce TI, především VTV, městská zeleň, další žádoucí aktivity odehrávající se ve veřejném prostoru apod. Z dostupných podkladů pak vyplývá, že nebyla a není ve většině sídel též zatím adekvátně zohledněna nutnost důsledného řešení transformace stávajícího systému jednotné kanalizace na systém důsledně oddílný.

Analogicky chybí aktuální ucelená strategie a koncepce řešení zásobování energiemi a adekvátní strategie obsluhy tohoto území prostřednictvím subsystémů sítí elektronických komunikací (včetně subsystémů operátorů radiotelekomunikačních služeb), též včetně adekvátní strategie nakládání s odpady. To se pak obvykle promítá celkovým podceněním řešení (řešitelnosti) tohoto sektoru technické obsluhy na adekvátní úrovni v rámci přípravy investičních akcí. Územní plány většiny sídel pak nepočítají obvykle s využíváním dopravně exponovaných ulic jako součásti ploch veřejných prostranství. Není např. též obvykle v disponibilních podkladech nabízena informace ohledně způsobu řešení subsystému koncovky odvodňovacího systému sídla [12]. V takových případech pak existuje značné riziko, že subsystém místních komunikací zafunguje při extrémních srážkách krajně negativně. I to je tedy nezbytné prověřovat. Žádoucí by pak měla být např. snaha učinit dopravu svým režimem plynulejší např. též zřízením podchodů či nadchodů pro chodce apod.

Rekapitulace rozhodujících podmínek pro návrh variantních řešení IS/VTV, jejich kontrola a vyhodnocení:

1. Šířka uličního prostoru často vyvolává potřebu důsledně oboustranného trasování souboru prakticky všech VTV, vedení 3.a 4. kategorie dle ČSN 73 6005. Musí tak být umožněno též optimalizovat délkový rozsah

přípojkových vedení, vedení 4. kategorie včetně maximální max. snahy chránit hlavní dopravní prostor.

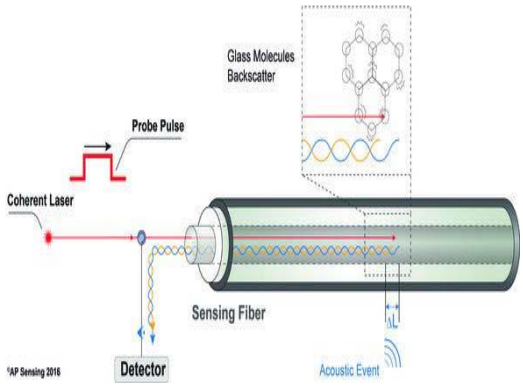
2. Výskyt prakticky souvislé uliční fronty (prakticky kontinuální zástavby) po obou stranách ulic po prověření pravděpodobně umožňuje (např. po prověření suterénů všech objektů po obou stranách ulic) aplikovat pro přípojková vedení progresivní řešení, tj. realizovat příslušný společný soubor přípojkových vedení ve sdružené trase pro několik navzájem sousedících domů/objektů (zajištění napojovacích rozvodů do sousedních objektů s využitím jejich suterénního prostoru, tj. použití efektivního i technicky možného řešení v rámci jejich technického zařízení budov/TZB).
3. Podmínka realizace adekvátního řešení umožňující programovou transformaci systému jednotné kanalizace na systém důsledně oddílný (v dané ulici i postupně v ulicích navazujících, výše i níže situovaných).
4. Podmínka realizace adekvátního řešení i v případě programově prosazovaného a adekvátně zkoordinovaného hospodaření se srážkovou vodou, tj. též i na pozemcích jednotlivých nemovitostí včetně případné realizace podzemních retenčních nádrží adekvátně technologicky vybavených ve vhodných místech.
5. Podmínka maximální ochrany dnes obvyklé hlavní funkce dané ulice, tj. ochrany její dopravní funkce včetně zajištění kvalitní MHD v tomto úseku a v úsecích navazujících.
6. Podmínka nepřerušení obsluhy prostřednictvím IS/VTV v průběhu realizace investiční akce, v případě Tábora [6], akce *Stavební úpravy ul. Budějovická*. - To by mohlo být zajištěno např. užitím stavebnice mobilní sdružené trasy/SMST IS/VTV [13].
7. Podmínka usnadnění transformace a modernizace řešení veřejného osvětlení/VO všech ulic dle připravovaných záměrů.
8. Podmínka sjednoceného koncepčního řešení pro síť na sebe navazujících ulic.
9. Podmínka garance udržitelného stavu a rozvoje IS/VTV.
10. Podmínka optimálních investičních nákladů dané akce a akcí navazujících.
11. Podmínka optimálních provozních nákladů IS/VTV.
12. Podmínka adekvátní životnosti IS/VTV po celou dobu opakovaných cyklů jejich životnosti.
13. Podmínka adekvátního splnění kritérií ideálního způsobu ukládání IS/VTV [14].
14. Podmínka optimální doby realizace aktuální investiční akce a akcí navazujících.
15. Další podmínky (po jejich odůvodněném doplnění; např. případné umožnění plošné plynofikace ev. též teplofikace v dané ulici a jejím okolí).

Důležité je též zohlednit hledisko bezpečnosti VTS/IS vůči vnějším atakům, především vůči atakům úmyslného či i nahodilého poškození apod. Na to pak reagují (jsou povinni reagovat) též nositelé *záchranného systém státu*. Budiž však řečeno, že v případě VTS/IS je případný útočný akt relativně snadný zejména z hlediska *přístupnosti* k zařízením VTS/IS a dále též k obvykle neúměrnému rozsahu struktury chráněných tras, objektů a zařízení VTS/IS, což v případě IS vyplývá z jejich základní struktury jako struktury spojitých rovinných grafů. Tzn., že již základní poznatky *teorie grafů* mohou pomoci posílit jejich základní schopnost provozu a jejich bezpečnost.

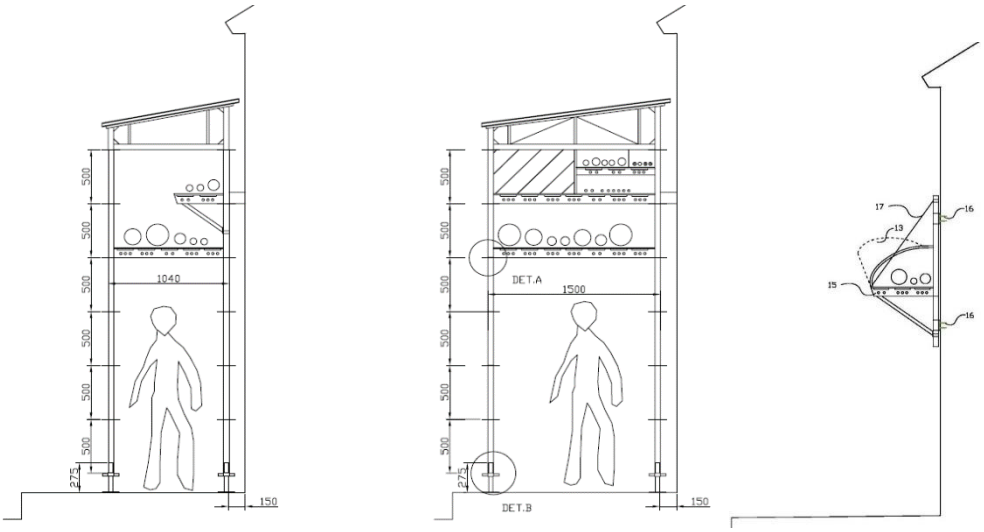
Výrazně lepší situace se však nabízí v případě použití ochranných konstrukcí VTS/IS zejména použití nabízejících se *konstrukcí sdružených tras* VTS/IS. V případě specifických tras IS, např. utajovaných telekomunikačních kabelů bezpečnostních složek státu, bylo vyvinuto a aplikováno řešení v podobě v paralelní trase instalovaných specifických optických kabelů schopných operativně identifikovat hluk a vibrace způsobené vstupem potencionálních narušitelů do prostoru tras chráněných kabelů či jiných vedení a objektů, obrázek 9 [15]. Takové řešení může být též kombinováno s kamerovým systémem.

Jde však o řešení relativně ekonomicky náročné včetně provozní náročnosti. Navíc jde o řešení, které může být ne vždy stoprocentně fungující. Zatím se však s tím odpovědná pracoviště a jednotlivci smiřují a dohlíží na jejich instalaci a provoz, nikoliv však se stejným či adekvátním úsilím.

V případech, kdy bude třeba důsledně a systémově prosadit ucelené změny koncepčních řešeních, právě se snahou o zajištění splnění požadavku garance udržitelného stavu a rozvoje VTS/IS, pak je nezbytné počítat s rozsáhlejšími investičními akcemi a to si též vyžaduje adekvátní nástroje, např. odpovídající dovybavení a dovednosti *Hasičského záchranného sboru* či i jiných složek, a následně profesionální použití i dalších opatření a nástrojů pro udržení kontinuálního provozu VTS/IS. Takovým nástrojem by mohla být též např. *stavebnice mobilní sdružené trasy* IS [13], obrázek 10



Obr. 9. Fiber optic based security system, www.optokon.com.



Obr.10. Příklady struktury a základních aplikací *stavebnice mobilní sdružené trasy/SMS IS* dle užitného vzoru [13], využívající dnes disponibilních systémů modifikovaných lešení.

Jde tedy o příklad nástroje k usnadnění postupu transformace IS/VTV do udržitelného stavu či i např. nástroje zkvalitnění zásahů HZS (Hasičského záchranného sboru).

5. ZÁVĚR

Závěrem lze již jen stručně potvrdit, že je opravdu již nezbytně nutné co nejdříve začít poctivě zabezpečovat plnění podmínky garance udržitelného stavu a rozvoje sídel prostřednictvím jejich TI, zejména pak IS/VTV, přestat improvizovat, přestat riskovat, respektovat veřejný zájem. Návod, *jak na to*, nabízí daný příspěvek, příspěvek techniků, respektujících realitu.

LITERATURA

[1] WILKINSON, D. *Trenchless Technology Guidelines.* London: ISTT 1989, 685 p.

[2] ŠRYTR P. A KOL. *Sdružené trasy inženýrských sítí v urbanizovaných územích.* ISBN 978-80-01-04289-2. Praha: ČVUT, 2010, 173 p.

[3] ŠRYTR P. Bezvýkopové technologie jako nástroj integrace zájmů všech síťových odvětví ve prospěch udržitelného rozvoje. *Sborník referátů 19. NO-DIG.* ISBN 978-80-904551-4-6. Litomyšl: CzSTT 2014, 10 p.

[4] ŠRYTR P. Bezvýkopové technologie, veřejný prostor s městskou zelení a revize ČSN 73 6005. *Sborník referátů odborného semináře MENDELU v Brně 26.-27.1.2015. Stromy ve městech-hodnotit nebo kácet?*, www.nature.cz
[5] LHOTSKY, M. (ed). *Zásady pro využití bezvýkopových technologií v oboru vodovodů a kanalizací.* ISBN 978-80-87140-07-9. Praha: Medim s.r.o. 2008, 144 p..
[6] AQUA PROCON. *Stavební úpravy ul. Budějovická v Táboře*. Studie proveditelnosti pro úsek Křižíkovo nám. – křižovatka s ul. Havlíčkova. Praha: ČVUT 2018-2020.
[7] WOLF, F. *Hodnotová analýza ve stavebnictví.* Praha: SNTL 1982, 279 p.
[8] KADLČÁKOVÁ, A. *Ekonomika ve stavebnictví – Hodnotový management.* ISBN 978-80-01026-052. Praha: ČVUT 2002, 203 p..
[9] BERAN, V. a kolektiv: *Městské inženýrství, Stavební kniha 2011.* ISBN 978-80-87438-09-1. Praha: Academia 2011, 180 p.
[10] DLASK P., ŠRYTR P. Objektivizace rozhodování při přípravě aplikací bezvýkopových technologií. *Sborník referátů konference NO-DIG CzSTT.* ISBN 978-80-904551-2-2. Luhačovice: CzSTT 2012, 8 p.
[11] ÚSTAV ÚZEMNÍHO ROZVOJE. *Pravidla a principy územního plánování. Technická infrastruktura* Brno: Ústav územního rozvoje 2019. www.uur.cz
[12] ZAVADIL J. Zkoumání změn odtokových poměrů v urbanizovaném území způsobených dopravními stavbami. *Doktorská disertační práce.* Ostrava: FAST VŠB-TU, 130 p.
[13] ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ. Užitný vzor *Stavebnice mobilní sdružené trasy IS.* Osvědčení o zápisu užitného vzoru č. 19323 ze dne 16.2.2009. www.upv.cz.
[14] ŠRYTR P. A Kolektiv. *Městské inženýrství.* ISBN 80-200-0802-0. Praha: Academia 1998, 404 .
[15] POSPÍCHAL, P. Lokalizace a klasifikace vibrací pomocí rozprostřeného vláknového senzoru. *Sborník odborné konference ČTS Měření a údržba sdělovacích kabelů XLIX.* Tábor: ČTS 2018, 41 p.

METODIKA SESTAVENÍ PLÁNU ÚDRŽBY PAROGENERÁTORU

METHODOLOGY OF COMPILING A STEAM GENERATOR MAINTENANCE PLAN

Karel Vidlák

ČEZ, a.s., Jaderná elektrárna Temelín, 373 05, Temelín, karel.vidlak@cez.cz

Abstrakt: Parogenerátor v jaderné elektrárně je navržen tak, že fyzicky odděluje primární okruh obsahující radioaktivní látky od sekundárního okruhu, který je již neobsahuje. Parogenerátor je zařízení kategorie 1, a proto je nutné minimalizovat jeho poruchy. Z tohoto důvodu je zvolena strategie péče o zařízení, která zajišťuje vysokou spolehlivost, tj. minimalizuje výskyt poruch a netoleruje funkční poruchy mezi stanovenými cykly údržby. Z ekonomických důvodů je program preventivní údržby řízen údržbou položek, které nejvíce přispívají k poruše parogenerátoru. V příspěvku uvádíme postup, kterým jsme připravili plán pro proaktivní preventivní údržbu parogenerátoru.

Klíčová slova: Jaderná elektrárna, riziko, technické dílo, bezpečnost, zdroje rizik, havárie, proaktivní preventivní údržba.

Abstract: The steam generator in nuclear power plant is designed in such a way that it physically separates the primary circuit that contains radioactive substances from the secondary circuit, which no longer contains them. The steam generator is a category 1 device, and therefore, it is required to minimize its breakdowns. Therefore, a device care strategy is chosen that ensures high reliability, i.e. minimizes the occurrence of failures and does not tolerate functional failures between established maintenance cycles. From economic reasons, the preventive maintenance program is controlled by the maintenance of the items that contribute mostly to the failure of the steam generator. In the paper, we show procedure by which we prepared steam generator maintenance plan for proactive preventive maintenance.

Key words: Nuclear Power Plant, risk, technical facility, safety, sources of risks, crush, proactive preventive maintenance.

1. ÚVOD

Pro zajištění bezpečnosti jaderné elektrárny je nutné za všech podmínek dodržet limity, které byly stanoveny v projektu pro prvky, komponenty, systémy a jejich rozhraní. V předloženém příspěvku se zaměřujeme na kritické zařízení jaderné elektrárny, a to na parogenerátor. Parogenerátor je navržen tak, že fyzicky odděluje primární okruh obsahující radioaktivní látky od sekundárního okruhu, který je již neobsahuje. Jeho úkolem je zajistit provoz reaktoru v přípustném rozsahu teplot a tlaků pomocí řízeného chlazení vody v primárním okruhu, která má vysokou teplotu a vysoký tlak.

Jaderná elektrárna Temelín má reaktor typu VVER 1000. Parogenerátor je horizontální výměník tepla s velkou teplosměnnou plochou tvořenou svazkem "U" trubek. Je dimenzován pro maximální provozní hodnoty, a to u teploty na 320 °C a u tlaku na 16 MPa [1]. Odvádí teplo, které vzniká v jaderném reaktoru do napájecí vody v sekundárním okruhu. Teplotní a tlakové poměry v parogenerátoru jsou nastaveny tak, aby na povrchu potrubí docházelo k intenzivní tvorbě páry, která proudí přes parní kolektor a parní potrubí do turbíny, kde slouží k pohonu turbogenerátoru.

Základní součást parogenerátoru tvoří tlaková nádoba, která má řadu příslušenství. Pro udržení optimálního výkonu celého systému je nutné provádět kvalitní údržbu jednotlivých zařízení systému a jejich propojení podle velikosti rizik. Nejzranitelnější příslušenství parogenerátoru jsou: armatury; potrubí; těsnění; svary atd. Při návrhu jaderné elektrárny projektant stanovil plány údržby jak pro tlakovou nádobu, tak pro její příslušenství. Provoz v jaderné elektrárně Temelín však ukázal, že vzhledem k místním podmínkám a novým poznatkům o provozu výměníků tepla ve světě jsou tyto plány zastaralé. Program údržby je proto postupně modernizován tak, aby byl hospodárným způsobem minimalizován výpadek celého zařízení [2].

Parogenerátor patří do zařízení kategorie 1, a proto je nutné minimalizovat jeho poruchy. Z tohoto důvodu je zvolena strategie péče o zařízení, která zajišťuje vysokou spolehlivost, tj. minimalizuje výskyt poruch a netoleruje funkční poruchy mezi stanovenými cykly údržby. Program údržby je založen na principu odstupňovaného přístupu k zařízení [3,4]. Základním požadavkem pro realizaci efektivní strategie preventivní údržby je znalost stavu a výkonnosti provozovaného zařízení. Na základě znalosti těchto parametrů je program údržby optimalizován tak, aby bylo dosaženo požadované úrovně bezpečnosti, výkonu a spolehlivosti [5,6].

Program proaktivní preventivní údržby [7] je založen na údajích o:
- konstrukci parogenerátoru,
- významu parogenerátoru pro bezpečnost jaderné elektrárny,
- významu parogenerátoru pro výrobu elektřiny
- a provozních zkušenostech.

Předkládaná metodika sestavení programu údržby parogenerátoru vychází z konceptu proaktivní preventivní údržby u konkrétních položek.

2. SOUHRN ZNALOSTÍ O ÚDRŽBĚ JADERNÝCH ZAŘÍZENÍCH

Již v 80. letech 20. století se objevovaly různé nedostatky a závady, které komplikovaly rozhodování o konstrukčních a provozních otázkách, a to kvůli neznámým, nejasným nebo chybějícím informacím o změnách konstrukce, které vznikaly během provozu. Implementace, účinnost a přiměřenost opatření údržby byla nepříznivě ovlivňována touto skutečností, ke které přispívaly i nedostatečně podrobné návrhy. Některé nepříznivé dopady těchto nedostatků přetrvávají v důsledku neadekvátních procesů, které jsou pod kontrolou vlastníků/provozních organizací (např. jejich programy, postupy, kultura a zdroje), zatímco některé, jako je přerušení vztahů s externími dodavateli, nikoli [8].

Z bezpečnostních důvodů se úloha údržby neustále zvyšuje, jak ukazují publikace [5,8-14]. V jaderných zařízeních se používají typy údržby dle [14]:
- periodická,
- preventivní
- a prediktivní.

Forma periodické údržby se sestává ze servisu, výměny dílů, dohledu nebo testování v předem stanovených časových intervalech, provozní doby nebo počtu cyklů. Provádí se akce, které detekují, vylučují nebo zmírňují degradaci funkční struktury, systému nebo součástí za účelem udržení nebo prodloužení jejich životnosti řízením degradace a poruch na přijatelnou úroveň.

Preventivní údržbou může být pravidelná údržba, plánovaná údržba nebo prediktivní údržba. Preventivní údržba se provádí buď nepřetržitě nebo v intervalech řízených pozorovaným stavem zjištěným monitorováním, diagnostikou nebo dle trendu indikátorů, které informují o stavu konstrukce, systému nebo součásti. Její výsledky ukazují současnou a budoucí funkční schopnost nebo povahu a harmonogram plánované údržby. Důležité úkoly údržby lze rozdělit do čtyř oblastí, a to:
- řízení údržby,
- management lidských zdrojů,
- hodnocení stavu zařízení
- a podnikatelské prostředí.

Funkcí údržby je zachovat a obnovovat vlastní bezpečnost, spolehlivost a dostupnost struktur podniku, systémů a komponent pro spolehlivý a bezpečný provoz.

Údržba v jaderných zařízeních má z důvodu velkého důrazu na bezpečnost specifické vlastnosti, které kladou velké nároky na způsob organizace a provádění činností údržby. Tyto příznačné znaky přispívají ke vzniku vážných následků, technické složitosti a opožděných dopadů údržby. To znamená, že systém řízení jaderné elektrárny (dále JE) zahrnuje dle [18] také činnosti:
- údržby,
- testování,
- dohledu
- a inspekcí.

To znamená, že systém řízení jaderné elektrárny obsahuje:
- detailní údaje o postupech údržby, testování, dozoru a inspekce,
- vymezení typů zařízení, která vyžadují kalibraci, dohled a údržbu,
- kritéria a orgán, kterému jsou nesrovnalosti hlášeny,

- formát záznamů a dokumentace,
- seznam zařízení, která jsou zahrnutá do ovládání konfigurace JE,
- kontroly záloh,
- analýzy sledování stavu zařízení v průběhu času,
- požadavky na provádění monitorování stavu
- a zpětnou vazbu v provozu.

Všechny uvedené činnosti musí provádět kvalifikovaný personál.

Plánování údržbářských prací musí respektovat:
- povolení pracovních sekvencí,
- povolení k izolaci zařízení,
- povolení k práci v radioaktivním prostředí,
- požadavky z oblasti neradiační bezpečnosti,
- požadavky na vyloučení cizích materiálů,
- požadavky na drenáž zařízení,
- požadavky na větrání,
- požadavky na ochranu před vnitřními a vnějšími hrozbami,
- zařízení pro izolaci mechanických a elektrických částí,
- a řízení úprav JE.

Důležitá je koordinace práce mezi jednotlivými týmy údržby:
- mechanické části,
- elektrické části,
- části řídicího systému
- a občanské vybavenosti.

Doporučuje se používat kontrolní seznam [18,19], aby se na nic nezapomnělo a činnosti probíhaly v logickém sledu.

To znamená, že program údržby musí zahrnovat:
- definici rolí a odpovědností,
- pochopení pro vyloučení cizích předmětů a chemikálií,
- vyjmenování všech součástí a systémů, které budou předmětem údržby,
- definice pracovních postupů,
- požadavky na koordinace prací
- a dokumentaci.

Tento program zahrnuje všechna preventivní a nápravná opatření k udržení všech projektem požadovaných funkcí konstrukcí, systémů a komponent na přijatelné úrovni. Činnosti údržby zahrnují seřizování, generální opravy, opravy a přemisťování dílů. Mohou také zahrnovat testování, kalibraci a provozní kontroly.

Optimalizovaná údržba pomáhá zajistit, aby úkoly byly prováděny správným vybavením ve správný čas. Cílem optimalizace údržby je snížit nerovnováhu mezi požadavky na údržbu a použitými zdroji a zajistit zlepšování na základě získaných zkušeností.

Optimalizace programu údržby je zásadní pro řízení aktiv [5]. Její typické cíle jsou:
- bezpečnost,
- spolehlivost,
- optimalizace nákladů,
- dostupnost
- a vylepšování technologie.

Optimalizační nástroje a metody musí být vybírány a posouzeny jak z hlediska kritičnosti zařízení, tak z hlediska nákladů na údržbu.

Typická hodnocení se zaměřují na pět hlavních oblastí procesu údržby:
- identifikace práce,
- zvládnutí práce,
- provedení práce,
- vyhodnocení práce
- a celkový program údržby.

V souladu s [5] se v praxi [15,16] pro klasifikaci stavu zkoumaných položek používá škála uvedená v tabulce 1.

Tabulka 1. Stupnice pro určení stavu položky / míry rizik.

Úroveň stavu položky / míra rizika	**Závěr z hodnocení položky**
1 – velmi dobrý ⬇ míra rizika je nízká	Položka je v perfektním fyzickém stavu a plní zamýšlené funkce. Náklady na údržbu jsou v souladu se standardy a normami. Položka je nová nebo byla nedávno obnovena. Nároky na provoz položky odpovídají projektu, položka nevykazuje provozní problémy. Celý program je implementován efektivně a účinně.
2 – dobrý ⬇ míra rizika je střední	Položka je fyzicky v dobrém stavu a plní zamýšlené funkce. Náklady na údržbu technického vybavení jsou v souladu se standardy a normami, ale postupně se zvyšují. Položka je zhruba v polovině své životnosti. Nároky na provoz položky odpovídají provedení a provozní problémy položky jsou jen občasné. Veškerý program je plněn přijatelně.
3 – přijatelný ⬇ míra rizika je vysoká	Položka vykazuje známky opotřebení a má nižší výkon, než byl zamýšlen. Některé části položky jsou nedostatečné. Náklady na údržbu položky přesahují částky stanovené standardy a normami a zvyšují se. Položka byla dlouhodobě používána nebo pracovala v nepříznivých podmínkách, a je tedy v poslední fázi své životnosti. Nároky na provoz položky odpovídají provedení, má časté provozní problémy. Celý program je z větší části naplněn, ale objevují se neúčinné a neefektivní způsoby implementace.
4 – špatný ⬇ míra rizika je velmi vysoká	Položka vykazuje značné známky opotřebení a plní zamýšlené funkce na nízké úrovni. Mnoho částí položky je nevyhovujících. Náklady na údržbu položky výrazně převyšují částky ze standardů a norem. Položka se blíží ke konci své životnosti. Nároky na obsluhu položky převyšují údaje v návrhu a provozní problémy položky jsou zřejmé. Celý program je naplňován jen ve velmi omezené míře.
5 – kritický ⬇ míra rizika je extrémní	Položka je ve špatném stavu a nepracuje tak, jak má. Je vysoká pravděpodobnost jejího selhání. Náklady na údržbu položky jsou ve srovnání se standardy a normami vysoce nepřijatelné, rekonstrukce položky není nákladově efektivní. Je nutná výměna. Nároky na provoz položky jsou výrazně vyšší než projektové; provozní problémy položky jsou vážné a trvalé. Stanovený program není naplněn.

3. KONCEPT PROAKTIVNÍ PREVENTIVNÍ ÚDRŽBY

Pro zajištění bezpečnosti a dlouhodobého provozu jakéhokoli technického zařízení je nutné řídit rizika všeho druhu, příklad je uveden v práci [16]. Pro dosažení cíle bezpečného, ekonomického a spolehlivého provozu je nezbytný program řízení životnosti elektrárny, který identifikuje všechny požadavky na celkový životní cyklus jaderné elektrárny. Takový účinný program zajišťuje, že jaderné elektrárny integrují své provozní, údržbářské, inženýrské, regulační, environmentální a ekonomické plánovací činnosti tak, aby zajistily materiálový stav elektrárny a zároveň aby zajistily bezpečný a dlouhodobý provoz.

Za bezpečnost jaderné elektrárny organizace provozující jadernou elektrárnu. Kromě aktivit provozovatele zacílených na bezpečnost, k bezpečnosti přispívá i nezávislý regulační orgán dohled prostřednictvím inspekční činnosti, a v případě potřeby i pomocí vynucovacích opatření. Bezpečnostní standardy MAAE, vypracované na základě mezinárodního konsensu, se zabývají všemi aspekty bezpečnosti provozu jaderných elektráren a regulačních činností. Zahrnují požadavky na řízení bezpečnosti, a organizační a technické aspekty bezpečnosti během životního cyklu jaderných elektráren. Doporučují prováděcí pokyny pro všechny hlavní typy zařízení, a od r. 2000 se soustřeďují zejména údržbu [5,8-14].

Údržba zahrnuje preventivní a nápravná opatření, která zajišťují, že konstrukce, systémy a komponenty jsou schopny plnit funkce, které jim byly předepsány projektem. Typické činnosti údržby zahrnují generální opravy, opravy a výměny součástí systému a jsou rozšířeny o testování, kalibrace a provozní kontroly [16,17].

Na zařízení se pravidelně provádí preventivní údržba, aby se snížila pravděpodobnost selhání. Údržba se provádí, když je zařízení funkční, aby se zabránilo poruchám, opravám nebo výměně. Preventivní údržba je program pro stanovení údržby podle plánu založeného na datech a doporučení výrobce. Efektivní programy preventivní údržby

umožňují organizacím docílit zlepšení celkových provozních nákladů a obchodních procesů. Ty mohou zahrnovat zvýšenou produktivitu, méně odpadu, lepší provedení a snížení poruchovosti zařízení.

Preventivní údržba je jednoduchá strategie údržby, kterou lze implementovat a provádět. Obvykle se začíná tím, že se dodržují doporučení výrobce a následně se vytvoří plán údržby pro kritická zařízení, který je místně specifický, protože místní podmínky ovlivňují stárnutí konstrukcí i jejich funkce [15,16]. Preventivní údržba pomáhá podniku vyhnout se poruchám a ztrátám ve výrobě, a také snížit skutečné náklady na údržbu. Typickým problémem plánů preventivní údržby je neúplná údržba majetku, protože frekvence plánované údržby zařízení bývá často nedostatečná. Kvalitní preventivní údržba tomu může zabránit, a proto se provádí analýzy situace a optimalizace programu preventivní údržby.

Metody používané pro podporu prediktivní údržby [18-20] jsou založeny na určení stavu zařízení s cílem odhadnout, kdy by měla být naplánována a provedena údržba. Pravidelné opotřebení bez pravidelné údržby může způsobit nižší účinnost stroje. Preventivní údržba zvyšuje životnost zařízení. Plánovaná preventivní údržba se proto plánuje tak , aby se předešlo překážkám ve výrobě a prostojům způsobeným poruchou zařízení.

Prediktivní údržba zajišťuje, že zařízení vyžadující údržbu je vyřazeno z provozu pouze tehdy, když je údržba nutná, obvykle před poruchou. To vede ke snížení celkového času a nákladů vynaložených na údržbu zařízení. Zařízení pro monitorování stavu potřebné pro prediktivní údržbu může být nákladné. Nároky na úroveň dovedností a technických zkušeností, které jsou potřebné k přesné interpretaci údajů z monitorování stavu, jsou vysoké. Monitorování stavu zařízení může mít pro organizace vysoké počáteční náklady. Správná strategie prediktivní údržby je nákladově efektivní, protože údržba se na zařízeních provádí pouze tehdy, když je to potřeba.

Především z ekonomických důvodů je plánování a rozvrhování kritickou součástí optimalizace údržby podniku. Podle [18-20] musí optimalizační program zvážit:

1. Pokročilé strategie údržby: Tyto strategie řeší, jaké přístupy údržby budou přijaty, aby se program údržby posunul z reaktivního na plánovaný. Mezi takové přístupy patří optimalizace základny údržby, implementace programu prediktivní údržby a vývoj živého proaktivního programu údržby.
2. Pracovní proces: Tato část procesu optimalizačního programu údržby se zabývá tím, jak je údržba prováděna. Zkoumá pracovní proces od zahájení práce, přes plánování po provedení práce, dokončení práce, a nakonec až po pokračující zlepšování.
3. Lidé: Dovednosti, pracovní kultura, management: Aby byla optimalizace údržby úspěšná, vyžaduje dobře vyškolenou pracovní sílu, dobrý management a organizační strukturu. Pracovní kultura, která odpovídá novým nápadům. Tento aspekt přístupu k programu údržby optimalizace se zaměřuje na to, kdo práci vykonává.
4. Nástroje/Technologie: Tato kategorie programu údržby optimalizace se zaměřuje na nástroje potřebné pro podporu personálu.

Proaktivní preventivní údržba [20] je proces poučení se z minulých problémů údržby s cílem omezit budoucí údržbářské práce u a zlepšit spolehlivost zařízení. Analýza kořenových příčin je formální metoda k určení nejzákladnější příčiny problému a doporučení účinných nápravných opatření. Analýza hlavních příčin je přirozenou součástí procesu proaktivní údržby. Tato směrnice [20] byla vyvinuta ve spolupráci s několika americkými a evropskými společnostmi. Osvědčené postupy v těchto společnostech byly shrnuty v tomto pokynu.

Proaktivní preventivní údržba je každodenní proces, který doplňuje pracovní proces údržby a proces prediktivní údržby. Tři hlavní kroky proaktivní údržby jsou:
- přezkoumávání,
- analýza
- a následná kontrola.

Proaktivní preventivní údržba je jak typem úkolu, tak procesem podniku, kterým se řídí bezpečnost [20], a proto se úkoly údržby také nazývají projektové úkoly. Proces údržby zahrnuje činnosti spojené se zlepšením nebo výměnou zařízení, nikoli pouze o opravu nebo renovaci. Proces údržby je jak denní, tak roční. Stejně jako jiné podnikové procesy, proces údržby má nároky na lidi, postupy a nasazení. Na denní bázi je práce přezkoumávána, analyzována a implementována.

Každoročně je práce shrnuta, a dlouhodobé faktory působící na stav zařízení jsou posuzovány. Proaktivní proces je více než jen klasická údržba, neboť v něm jde o snížení četnosti selhání důležitých zařízení. Proto sleduje otázky provozu, inženýrství a řízení. Proaktivní proces má tři kroky:
- určení událostí, které mají být přezkoumány personálem údržby nebo provozu
- určení událostí, které mají být analyzovány inženýry nebo manažery

- a stanovení doporučení pro pracovníky údržby, provozu, techniky nebo managementu.

Proaktivní preventivní údržba [20] vyžaduje správné nastavení procesu údržby a včasnou diagnostiku zařízení pro predikci poruch. Tím se zajistí:
- potřebná péče o zařízení,
- monitorováním stavu zařízení se doplní informace o stavu zařízení a zajistí se včasná predikce poruchy
- a provedou se akce k odstranění kořenových příčin poruch.

Proaktivní řízení údržby musí být implementováno na všech úrovních údržby.

Zařízení, které má být zahrnuto do rozsahu programu údržby zařízení, musí být podrobné a mít stanoveny priority [5,13,19-21]. Tento výběr musí být založen na analýze záznamů o údržbě, o poruchách a požadavcích na údržbu, jakož i na dalších faktorech. Musí vzít v úvahu:
- položky s vysokými náklady na údržbu,
- komponenty, které jsou pro podnikání nejdůležitější,
- kritické a nekritické systémy.

Vzhledem k dynamickému vývoji musí být každá údržba živým programem.

4. ÚDAJE O ÚDRŽBĚ PAROGENERÁTORU V JADERNÉ ELEKTRÁRNĚ TEMELÍN

Parogenerátor (dále PG) v jaderné elektrárny Temelín byl podrobně popsán v [17,22]. Původní program údržby byl nastaven dle doporučení výrobcem [23]. V průběhu provozu byla tato šablona údržby několikrát upravena na základě provozních zkušeností a provedených kontrol, které se zahrnuly do hodnocení stárnutí komponenty [24-26].

Speciální hodnocení stárnutí komponenty spočívá v průběžném pravidelném hodnocení vlivu degradačních mechanismů v závislosti na provozním režimu a provozních podmínkách. Provádí se za účelem zjištění fyzického stavu zařízení z hlediska stárnutí a zajištění toho, aby během provozu nedocházelo k čerpání bezpečnostních rezerv, případně ke znalosti míry absorpce bezpečnostních rezerv za určitých specifických provozních podmínek [27]. Na základě zkušeností a nových poznatků využívá od roku 2012 preventivní údržba dle pokynů a formulářů EPRI pro preventivní údržbu [2].

Na základě výše uvedeného se u parogenerátoru udržuje 256 položek [28]. Aktuální program údržby rozlišuje, zda jsou položky:
- kritické nebo nekritické,
- pro normální nebo obtížné podmínky,
- pro nízké nebo vysoké pracovní cykly
- a zda se jedná o vybrané zařízení nebo podléhají jiným vyhláškám nebo nařízením.

Podle klasifikace se používají plány údržby [28] pro položky:
- jednou za směnu,
- jednou denně,
- jednou týdně,
- jednou za 2 měsíce,
- jednou za 4 měsíce,
- jednou za rok,
- jednou za 3 roky,
- jednou za 4 roky,
- jednou za 6 let
- a jednou za 8 let.

Opatření údržby [28] se provádí na základě:
- sledování výkonnosti,
- vizuální kontroly obsluhujícím personálem,
- vizuální kontroly prováděné systémovým inženýrem,
- výsledků nedestruktivních zkoušek,
- vnitřní kontroly a čištění nebo doplňování maziv nebo provozních kapalin,
- závěrů zkoušek těsnosti při provozním tlaku,
- závěrů pevnostní tlakové zkoušky,
- rekonstrukcí či výměnou.

5. METODIKA PRO PROAKTIVNÍ PREVENTIVNÍ ÚDRŽBU PAROGENERÁTORU

Abychom splnili náš cíl, kterým je přechod od preventivní údržby k proaktivní preventivní údržbě [20], která je pokročilejší, musíme přesněji zvládat rizika. Znamená to mít postup pro stanovení rizika každé položky a provádět údržbu založenou na velikosti rizik, zejména v případech plánu údržby, která je spojena s výměnou jaderného paliva v reaktoru.

Předkládaná metodika sestavení programu údržby parogenerátoru vychází z konceptu proaktivní preventivní údržby u konkrétních položek. Stav položek je hodnocen v pětistupňové škále (tabulka 1):
- velmi dobrý stav,
- dobrý stav,
- přijatelný stav,
- špatný stav
- a kritický stav.

Pomocí výsledků testů jsou u každé položky posouzeny míry rizik. Velikosti dopadů a četnosti výskytu dopadů jsou stanoveny podle údajů v návrhu položek a v provozních protokolech. U kritických položek je navíc stanovena míra integrálních rizik pomocí výsledků všech provedených nedestruktivních testů pomocí specifického systému pro podporu rozhodování (decision support system – DSS) [7]. Podle získaných hodnot je určen nejzazší čas, kdy musí být provedena zásadní údržba nebo výměna kritické položky parogenerátoru. Z ekonomických důvodů je program údržby řízen údržbou položek, které nejvíce přispívají k poruše celého parogenerátoru.

Pro klasifikaci podmínek položek parogenerátoru používáme stupnici uvedenou v tabulce 1. Reálnou míru rizika každé položky určujeme podle výsledků testů, které jsou stanoveny normami [28]. V prvním kroku jsou skutečné míry rizika podle testu klasifikovány následujícím postupem:
- výsledek testu nesplňuje požadavky norem – stav položky je špatný nebo kritický a míra rizika je velmi vysoká nebo extrémní,
- výsledek testu má maximální povolenou odchylku podle požadavků norem – stav položky je přijatelný a míra rizika je vysoká,
- výsledek testu splňuje požadavky norem – stav položky je dobrý.

Jelikož normy jsou založeny na spolehlivosti, tak soulad s normami nemusí vždy zajistit bezpečnost položek. Proto u kritických položek (tj. položek, které zajišťují bezpečnost nebo k zajištění bezpečnosti přispívají) následuje druhý krok, ve kterém posuzujeme stav položek podle provozních zkušeností v provozním záznamu [29]. Pro rozhodování o riziku používáme systém pro podporu rozhodování [7], který zohledňuje:
- frekvenci provozních problémů,
- velikost dopadů selhání položky,
- náklady na údržbu.

Při hodnocení míry rizika používáme stupnici 1–3 [7] s konceptem „čím vyšší, tím horší“ [30]. Pokud je výsledek posouzení:
- 3, stav položky je velmi dobrý a míra rizika nízká,
- mezi 3 a 6, stav položky je dobrý a míra rizika střední,
- vyšší než 6 a stav položky je přijatelný a míra rizika vysoká.

V posledním případě u kritických položek parogenerátoru v rámci proaktivního přístupu je nutné provést korekce nebo připravit opatření pro nápravu v případě náhlé změny stavu.

U kritických položek zvažujeme také skutečnost, že příčinou selhání kritických položek je často kombinace malých chyb a že každá jednotlivá nedestruktivní kontrola má schopnost odhalit pouze některé dílčí dopady rizika na položku [16]. Proto hodnotíme také míru celkového (integrálního) rizika pro každou kritickou položku s ohledem na výsledky všech kontrol. K jeho určení používáme tabulku 2.

Celá stupnice pro klasifikaci stavů položek parogenerátoru pro proaktivní preventivní údržbu pro všech 256 položek je v [7]. Její příklad je v tabulce 3. Pokud je úroveň rizika v tabulce 3:
- nižší než 25 %, stav položky je velmi dobrý,
- mezi 25 % a 45 %, stav položky je dobrý
- mezi 45 % a 70 %, stav položky je přijatelný,
- míra rizika je vyšší než 70 %, stav položky je špatný.

Proto je v případě kritických položek a v rámci proaktivního přístupu nutné provést nápravu nebo připravit vhodná protiopatření.

Tabulka 2. Hodnotová stupnice pro stanovení míry rizika; $r = sr/N$, kde sr je součet míry rizik jednotlivých testů a N je celkový počet testů.

Míra rizika	**Hodnoty *r* v %**
Velmi vysoká	Vyšší než 70 %
Vysoká	45 – 70 %
Střední	25 – 45 %
Nízká	Nižší než 25 %

Tabulka 3. Klasifikace stavu položek parogenerátoru. L – nízká míra rizika, M – střední míra rizika, H – vysoká míra rizika, V – velmi vysoká míra rizika.

Položka	**Použité testy**	**Popis poškození**	**Stupnice míry rizika pro položku na základě všech testů**	**Použité normy [28,31]**
Obvodový svarový spoj kroužku 1 pláště parogenerátoru	Vizuální kontrola Magnetická kontrola Ultrazvuková kontrola	Koroze Trhliny Nelineární vady	L < 3,75 M = 3,75- 6,75 H = 6,75- 10,5 V > 10,5	Vyhláška č. 358/2016 Sb., ČSN EN 13927, ČSN EN ISO 6520-1, ČSN EN ISO 3059, ČSN EN ISO 3452-1, ČSN EN ISO 3452-2, ČSN EN ISO 6520-1, ČSN EN ISO 17640, ČSN EN ISO 3059, ČSN EN ISO 9934-1, ČSN EN ISO 9934-2, 4-JL-000451
…….				
Teplosměnné trubky HK	Metoda vířivých proudů	Netěsnost Deformace Koroze Trhliny Nelineární vady	L < 2,5 M = 2,5 – 4,5 H = 4,5 – 7,0 V > 7,0	Vyhláška č. 358/2016 Sb., ČSN EN 13927, ČSN EN ISO 6520-1, ČSN EN ISO 15549
Svarový spoj 1. parního kolektoru	Vizuální kontrola Ultrazvuková kontrola Magnetická kontrola	Koroze Trhliny Lineární vady	L < 3,75 M = 3,75 – 6,75 H = 6,75 – 10,50 V > 10,50	ČSN EN 13927, ČSN EN ISO 6520-1 ČSN EN ISO 3059, ČSN EN ISO 3452-1, ČSN EN ISO 3452-2, ČSN EN ISO 6520-1 ČSN EN ISO 17640 ČSN EN ISO 3059, ČSN EN ISO 9934-1, ČSN EN ISO 9934-2 4-JL-000451, PK 1514-72
……..				

HSS rozvodu napájecí vody uvnitř parogenerátoru	Vizuální kontrola Kapilární kontrola Ultrazvuková kontrola Ultrazvuková kontrola – Phased Array	Koroze Trhliny Lineární vady	L < 2,5 M = 2,5 – 4,5 H = 4,5 – 7,0 V > 7,0	ČSN EN 13927, ČSN EN ISO 6520-1, ČSN EN ISO 3059, ČSN EN ISO 3452-1, ČSN EN ISO 3452-2, ČSN EN ISO 6520-1, ČSN EN ISO 17640, ČSN EN ISO 13588, ČSN EN ISO 3059, ČSN EN ISO 9934-1, ČSN EN ISO 9934-2, 4-JL-000451, PK 1514-72
……..				
Svarový spoj nátrubku havarijního napájení k plášti parogenerátoru	Vizuální kontrola Kapilární kontrola	Koroze Trhliny Lineární vady	L < 2,5 M = 2,5 – 4,5 H = 4,5 – 7,0 V > 7,0	ČSN EN 13927, ČSN EN ISO 6520-1, ČSN EN ISO 3059, ČSN EN ISO 3452-1, ČSN EN ISO 3452-2, ČSN EN ISO 6520-1, 4-JL-000451, PK 1514-72
……..				
Senzor tlaku	Vizuální kontrola Input test Konfirmace Kalibrace	Mechanické poškození Chybné měření Neprostupnost signálu	L < 5 M = 5 – 9 H = 9 – 14 V > 14	ČSN 33 2000, ČSN 370640, 4-JL-000451, TPVŽ 1000/80, MR001

6. PLÁN PROAKTIVNÍ PREVENTIVNÍ ÚDRŽBY PAROGENERÁTORU

Plán proaktivní preventivní údržby parogenerátoru [7] obsahuje:
- seznam všech položek a systémů parogenerátoru ,
- postupy pro posuzování podmínek položek parogenerátoru podle metody popsané v tabulce 2,
- definice pracovních postupů údržby jednotlivých položek,
- způsob koordinace prací údržby parogenerátoru ,
- stanovení odpovědností za jednotlivé práce údržby a za celou údržbu,
- dokumentaci prací údržby.

Za plán údržby parogenerátoru, a to denní, roční a při odstávkách odpovídá manažer parogenerátoru [28]. Manažer parogenerátoru koordinuje práce vedoucích pro strojní, elektrickou a I&C části [17]. Každý dílčí manažer má tým kritických osob, které plní reálné práce podle harmonogramu [28] a posuzují stav kritických položek [29] – příklady v tabulce 3. Každá kritická osoba zajišťuje dokumentaci ve formátu stanoveném [28].Pokud je stav kritické položky podle jedné zkoušky ohodnocen stupněm vyšším než 6, musí vedoucí parogenerátoru a dílčí manažeři neprodleně uplatnit vhodná protiopatření.

Pokud je míra rizika kritické položky na základě všech testů vyhodnocena jako vysoká nebo velmi vysoká, musí manažer parogenerátoru a dílčí manažeři zvýšit pozornost a začít připravovat řešení, protože oprava není v mnoha případech jednoduchá. Z článku [22] vyplývá, že náprava některých závad není jednorázová. Má dvě fáze:
- v první se provede rychlá korekce
- a ve druhé je implementováno konečné nápravné řešení po komplexním posouzení rizik tohoto řešení.

7. ZÁVĚR

Na základě současných poznatků shrnutých v [16] potřebujeme odolný ekonomický výkon parogenerátoru a celé jaderné elektrárny. V současné době jaderná elektrárna Temelín aplikuje preventivní údržbu parogenerátoru . V

příspěvku je ukázán postup, kterým jsme připravili plán údržby parogenerátoru pro proaktivní preventivní údržbu, která je dalším zlepšením údržby, která vede jak k vyšší bezpečnosti, tak k prodloužení životnosti kritických položek. Základem použité metody je:

- posouzení rizik kritických položek posouzením jejich stavu při hlavní údržbě během pravidelných odstávek reaktoru specifickým způsobem; příklad je uveden v tabulce 3,
- uplatnit protiopatření tak, aby míra rizika kritických částí parogenerátoru byla při provozu stále přijatelná.

Prezentace naší strategie získala podporu odborníků z jaderných elektráren a odborníků jaderného dozoru.

Poděkování: Autor děkuje za vedení práce, návrhy a připomínky doc. RNDr. D. Procházkové, CSc. DrSc.

LITERATURA

[1] CENCINGER, F. *Primární část JE WWER 1000*, část I. Brno: ABN 2008, 301 p.
[2] EPRI. *Preventive Maintenance Basis Database (PMBD) v7.0.* Palo Alto: EPRI 2022.
[3] ČEZ ETE, Dokument JE ČEZ_ME_0225. *Archiv*. Temelín: ČEZ ETE 2021.
[4] ČEZ ETE, Dokument JE ČEZ_ME_0678. *Archiv*. Temelín: ČEZ ETE 2016.
[5] IAEA. *Maintenance Optimalization Programme for Nuclear Power Plants, NP-T-3.8.* ISBN 978-92-0-110916-3, Vienna: IAEA 2018.
[6] IAEA. *Guidance For Optimizing Nuclear Power Plant Maintenance Programmes*. IAEA-TECDOC-1383, ISBN 978-92-0-112703-0, Vídeň 2003.
[7] VIDLÁK, K. Údržba parogenerátoru založená na rizicích v jaderné elektrárně Temelín. *Rukopis disertační práce*. Praha: ČVUT 2023.
[8] IAEA. *Design Basis Reconstitution for Long Term Operation of Nuclear Power Plants.* TEC-DOC-2018. ISBN 978-92-0-.103923-1. Vienna: IAEA 2023, 86 p.
[9] IAEA. *Safety Related Maintenance in the Framework of the Reliability Centered Maintenance concept*. TECDOC-658. Vienna: IAEA 1992, 199 p.
[10] IAEA. *Good Practices for Cost Effective Maintenance of Nuclear Power Plants*. TECDOC-928. Vienna: IAEA 1997, 141 p.
[11] IAEA. *Advances in Safety Related Maintenance*. TECDOC-1138. Vienna: IAEA 2000, 234 p.
[12] IAEA. *Guidance for Optimizing Nuclear Power Pland Maintenance Programme*. TECDOC-1383. Vienna: IAEA 2003, 148 p.
[13] IAEA. *Safety Culture in the Maintenance of Nuclear Power Plants*. ISBN 92–0–112404–X. Vienna: IAEA 2005, 62 p.
[14] IAEA. *Maintenance, Testing, Surveillance and Inspection in Nuclear Power Plants*. SSG-74. ISBN 978-92-0-136522-4. Vienna: IAEA 2022, 112 p.
[15] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů*. ISBN 978-80-01-05771-1. Praha: ČVUT 2015, 208 p.
[16] 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
[17] VIDLÁK, K., PROCHÁZKOVÁ, D. *Risk Management Plan for Steam Generator Maintenance at Nuclear Power Plan*. Doi:10.3850/978-981-18-5183-4_R18-01-043-cd, 2022
[18] EPRI. *Predictive Maintenance Program*. Palo Alto: EPRI 1998, 570 p.
[19] EPRI. *Best Practice Guideline for Maintenance Planning and Scheduling. Technical Report*. Palo Alto: EPRI 2000, 84 p.
[20] EPRI. *Guideline on Proactive Maintenance. Technical Report*. Palo Alto: EPRI 2001, 82 p.
[21] IAEA. *Implementation Strategies and Tools for Condition Based Maintenance at Nuclear Power Plants*. TECDOC-1551. Vienna: IAEA 2007, 187 p.
[22] VIDLÁK, K., PROCHÁZKOVÁ, D. *Increase of Safety of Steam Generator by Reconstructing the Water Supply Pipe*. Doi:10.3850/978-981-18-20 16-8_126-cd, 2021.
[23] ČEZ ETE. Dokument JE 4-001300-1. *Archiv*. Temelín: ČEZ ETE 1999.
[24] KUSÍN, L. *C4-JL-000619, rev. 1*. Ostrava 2008.
[25] ČEZ ETE. Inspekční zprávy JE Temelín. *Archiv*. Temelín: ČEZ ETE 2015.
[26] ČEZ ETE. Dokument JE ČEZ_ME_1170. *Archiv*. Temelín: ETE 2015.
[27] ČEZ ETE. Dokument JE ČEZ_ME_1170. *Archiv*. Temelín: ČEZ ETE 2015.
[28] ČEZ ETE. *Údržba parogenerátoru*. Archiv Temelín: ČEZ ETE 2023.
[29] ČEZ ETE. Protokoly z NDT kontrol PG. *Archiv* Temelín: ČEZ ETE 2022.

[30] KEENEY R. L., RAIFFA H. *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*. New York: J. Wiley & Son 1976, 1993, 368 p.
[31] ČVUT. *Soubor norem pro zajištění bezpečnosti technických objektů.* Praha: ČVUT 2023.

DŮLEŽITOST ÚDRŽBY PRO PRODLOUŽENÍ ŽIVOTNOSTI SOUČÁSTÍ

IMPORTANCE OF MAINTENANCE TO EXTEND THE LIFE OF PARTS

Karel Vidlák

ČEZ, a.s., Jaderná elektrárna Temelín, 373 05, Temelín, karel.vidlak@cez.cz

Abstrakt: Prodloužení životnosti a údržba jakéhokoli produktu, stroje nebo systému jsou klíčovými aspekty, které vyžadují odbornou pozornost a přístup. Efektivní údržba a správné prodloužení životnosti nejenže zvyšují dobu provozuschopnosti, ale také maximalizují výkonost a snižují celkové náklady. Předmětná údržba zahrnuje pravidelné kontroly, diagnostiku a opravy, které mohou identifikovat a řešit potenciální problémy dříve, než se stanou vážnými.

Klíčová slova: Údržba, životnost, prodloužení životnosti, bezpečnost, šablona údržby.

Abstract: Extending the life and maintenance of a single product, machine or system are key aspects that require professional attention and approach. Effective maintenance and proper service life extension not only increase uptime, but also maximize performance and reduce overall costs. Maintenance in question includes regular inspections, diagnostics, and repairs that can identify and address potential problems before they become serious.

Key words: Maintenance, service life, service life extension, safety, maintenance template.

1. ÚVOD

Údržba a správná péče o jakékoliv zařízení, systém, komponentu jsou klíčové pro jeho dlouhodobé využití a prodloužení životnosti. Pravidelná kontrola, diagnostika a preventivní údržba mohou eliminovat předčasné výpadky zařízení, včas odhalit potenciální poruchy, což v důsledku vede ke snížení nákladů na opravy nebo nákup nových zařízení. Kromě toho pravidelná údržba přispívá k efektivitě a produktivitě komponenty, zařízení nebo systému, protože kvalitně udržované zařízení funguje optimálně a má tak tendenci spotřebovat méně energie.

Údržba součásti je nezbytnou strategií každé péče o zařízení. Správně nastavená a provedená údržba zajistí dostupnost zařízení a minimalizuje vznik poruch. Pravidelně vykonávaná údržba a kontroly zařízení jsou nezbytné pro dlouhodobé zachování funkce komponenty, systému, ať se jedná o tlakovou nádobu, klimatizační systém nebo automobil [1,2]. Dodržování doporučení výrobce pro údržbu zajistí správnou funkci zařízení, jeho optimální nastavení a napomáhá včasnému odhalení případných problémů dříve, než se stanou závažnými. Například v případě armatury může pravidelná údržba zahrnovat mazání a kontrolu ucpávky [3]. Tyto rutinní úkony údržby mohou zabránit vzniku závažnějších problémů a v konečném důsledku prodloužit životnost celého systému.

U složitějších prvků, zařízení, komponent a systémů však nestačí pravidelná údržba, protože jejich opotřebení není v čase rovnoměrné a je ovlivněno změnami v provozu a změnami vnějších podmínek. Proto u důležitých položek se používá údržba založená na monitoringu stavu položek a řízení rizik [1]. Preventivní údržba [2,4] vychází z posuzování stavu kritických položek při pravidelných kontrolách a opatření provádí předem s cílem zabránit selhání.

Pokrokovějšími přístupy údržby jsou prediktivní údržba a proaktivní preventivní údržba. Prediktivní údržba určuje stav položek na základě dat z monitoringu stavu položek pomocí vícerozměrných prediktivních metod [5]. Proaktivní preventivní údržba [6] propojuje data z monitoringu stavu položek s místními inženýrskými poznatky o chování položek v provozu. Je založena na hledání příčin poruch, analýze kořenových příčin poruchy a na kontrole účinnosti přijatých opatření s cílem omezit údržbářské práce a zlepšit spolehlivost zařízení [7-9].

Výměna opotřebovaných nebo poškozených součástí je dalším klíčovým aspektem údržby, který může výrazně prodloužit životnost systému [7-10]. Pravidelnou kontrolou zařízení a identifikací součástí, které vykazují známky opotřebení nebo poškození, mohou jednotlivci tyto díly vyměnit dříve, než selžou a způsobí závažnější problémy. Tento přístup je často označován jako preventivní údržba a může pomoci předejít nákladným opravám a prostojům zařízení [10]. Proaktivní výměnou komponent mohou jednotlivci zajistit, že jejich zařízení bude fungovat optimálně a prodloužit jeho životnost.

Celkově je správně nastavená údržba zásadní pro prodloužení životnosti komponent v jakémkoli systému. Pravidelné kontroly, identifikace potenciálních problémů a výměna opotřebovaných nebo poškozených součástí mohou pomoci zabránit vzniku závažnějších problémů a vyhnout se nákladným opravám a nedostupnosti zařízení [1,7,8]. Dodržováním doporučení výrobce a implementací strategií proaktivní údržby můžeme zajistit, že dané zařízení funguje optimálně a prodloužit jeho životnost.

Možnost prodloužení životnosti zařízení je v dnešní době atraktivní způsob vyrovnávání se s konkurencí na poli hospodářské soutěže.

2. SOUHRN ZNALOSTÍ O ÚDRŽBĚ V JADERNÝCH ELEKTRÁRNÁCH

Pro zajištění efektivity údržby je vhodné pomocí screeningu [1,11] rozdělit systémy na „kritické“ a „nekritické“. Dále jsou kritické systémy klasifikovány dle své povahy do jednotlivých kategorií I a II. Do kategorie I spadají systémy, které nejsou technicky nahraditelná a kategorie II, které nejsou ekonomicky nahraditelná. Každý kritický systém se skládá z mnoha částí, jako jsou potrubí, armatury, podpěry, čerpadla, nádrže atd. Pečlivým přezkoumáním se identifikují komponenty v kritických systémech na základě analýz bezpečnosti a databázi poruch.

Abychom mohli zjistit, že zařízení pracuje správně a údržba na zařízení je prováděna optimálně, můžeme pro toto srovnání použít seznamy vytvořené pro tyto účely, např. seznamy poskytnuté EPRI [12]. Srovnání nebo benchmarking přizpůsobíme specifickým podmínkám prostředí, ve kterém je zařízení umístěné [1] a také provozními zkušenostmi. Kvalitativní údaje slouží jako kontrolní seznam potenciálních podmínek, které mohou ovlivnit výkonost podniku. Kvantitativní údaje o selhání poskytují náhled na potenciál pro vylepšení a pomáhají určit místo, kde je nejlépe vhodné provést zlepšení

V případě, že je četnost selhání součástí mnohem nižší, než uvádí obecná data [1,12], lze z toho vyvodit závěr, že stávající plán údržby je účinný a bude velmi obtížné dosáhnout dalších zlepšení spolehlivosti součástí. Na druhou stanu lze vysokou spolehlivost přičíst k nadměrnému programu údržby, která vede k velké nedostupnosti a bude vyžadovat úpravu postupů údržby.

V dokumentu [12] byly přezkoumány podrobné údaje o poruchách v období 5 let. Toto období není náhodné, protože se doporučuje revidovat údaje trendů výkonosti pravidel údržby právě v tomto období. Pokud je četnost poruch podstatně vyšší, něž jsou uvedeny obecné četnosti poruch v seznamu, nebo příspěvek hodnoceného systému ke ztrátě dostupnosti zařízení výrazně překračuje obecné hodnoty, může být zapotřebí výměna zařízení nebo zásadní změna postupů údržby. Předpokládá se, že pokud klesne výkon spolehlivosti zařízení, systému pod určitou úroveň, je vyžadováno ke splnění výkonnostních kritérií pravidel údržby zapotřebí velké úsilí údržby. Nakonec je třeba zvážit výměnu nebo úpravu součástí, systému [8,9].

3. PRAVIDLA ÚDRŽBY V JADERNÉ ELEKTRÁRNĚ

Primární úlohou údržby je zajistit dostupnost a spolehlivost zařízení, systému a využít všechny funkce nezbytné pro bezpečnou hospodárnou výrobu. Volba údržby musí být vyvážená, aby byla optimalizována spolehlivost zařízení a četnost údržby [1,11,13].

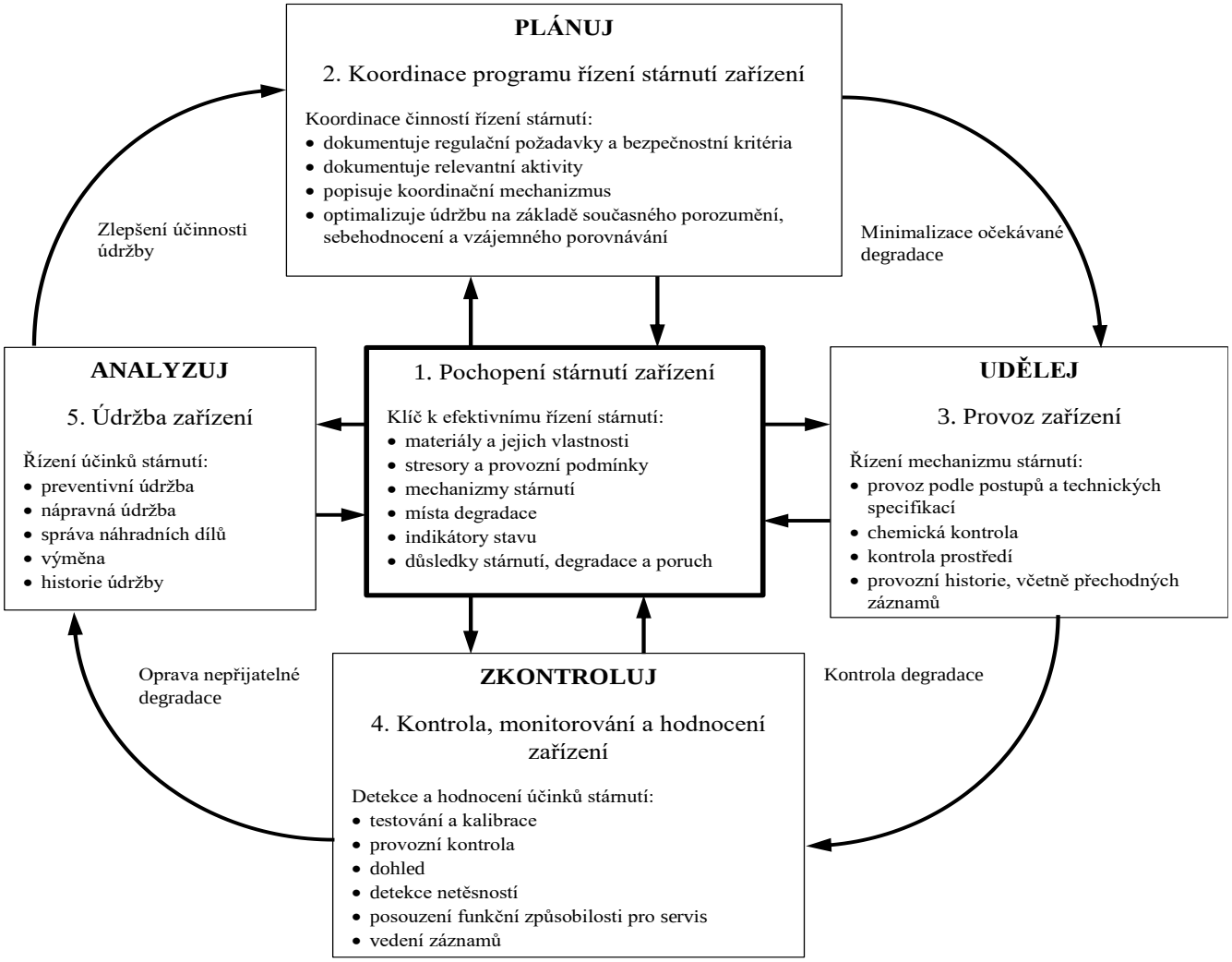
Například pro jaderné elektrárny jsou v dokumentu 10CFR50.65(a)(1), *Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Plants* [14] uvedeny následující požadavky:

> „Každý držitel povolení k provozování jaderné elektrárny podle § 2 odst. 1 písm. 50.21(b) nebo 50.22 musí monitorovat výkon nebo stav konstrukcí, systémů nebo komponent oproti stanoveným cílům držitele licence způsobem dostatečným k poskytnutí přiměřené jistoty, že takové struktury, systémy a komponenty, jak je definováno v odstavci (b), jsou schopny plnit své zamýšlené funkce. Tyto cíle musí být stanoveny úměrně bezpečnosti a tam, kde je to praktické, musí brát v úvahu provozní zkušenosti z celého odvětví. Pokud výkon nebo stav konstrukce, systému nebo součásti nesplňuje stanovené cíle, musí být přijata vhodná nápravná opatření.“

Na systémy se uplatňují kritéria spolehlivosti a dostupnosti [11,12] a dále se podle těchto kritérií shromažďují data pro monitorování výkonu zařízení. Použitelnost pravidel údržby je vždy místně specifická [1] a liší se mezi jednotlivými podniky na základě jejich konfigurace. V souladu s těmito specifickými údaji shromážděné pro účely pravidel údržby jsou tyto údaje přínosné také pro účely plánování prodloužení životnosti součástí.

4. ŠABLONY ÚDRŽBY

Pro optimalizaci údržby sledovaného zařízení se doporučuje pro testování, kontroly a údržbu program založený na výkonu [12]. Frekvence spojená s každým úkonem je nastavená jako počáteční cílová frekvence. Tyto cílové frekvence by měly být pravidelně revidovány dle Demingova cyklu [15], obrázek 1, na základě výsledků v jednotlivých podnicích. Pro komponenty, které jsou identifikovány jako zdroj největšího přírůstku k poruše se vytvoří seznam, který je pravidelně vyhodnocován [11].



Obr. 1. Demingův cyklus Plánuj–Udělej–Zkontroluj–Analyzuj pro údržbu [15].

4.1. Sestavení a zhodnocení historie provozu a výkonosti zařízení.

Současný stav, stáří a prostředí mají vliv na výběr plánování řízení životnosti. Důkladné posouzení stávajícího zařízení ve spojení s kontrolou výkonu má hlavní význam pro realistické rozhodnutí o zvolení výběru strategie údržby. Pro úplnou kontrolu stavu konstrukce, systému a komponenty je zapotřebí několika prvků. Mezi tyto prvky paří následující položky [12]:

1. Záznamy o pravidelných vizuálních kontrolách.
2. Diagnostické testy a data z monitorování zařízení.
3. Výsledky všech testů povedeny na zařízení.

4. Výsledky z použité prediktivní technologie.
5. Úpravy provedené na zařízení.
6. Pracovní příkazy.
7. Údaje o renovaci zařízení.

Důkladná revize historie údržby prováděná každých 3–5 let zpět slouží k vytvoření jasného obrazu výkonnosti zařízení. Tato historie údržby je většinou zachycena v pracovních příkazech, které bývají uloženy v počítačových systémech podniku, a které zároveň slouží k řízení údržby [11,12]. Pracovní příkazy jsou převážně určeny pro pravidelnou údržbu nebo pro opravnou údržbu. Jsou zde implementovány i jiné činnosti, jako je změna konfigurace, výměna či rekonstrukce.

Nejdůležitější pracovní příkazy související s řízením životnosti jsou ty, které řeší nápravná opatření v důsledku nenadálých poruch zařízení, vylepšení výkonu nebo změn konfigurace. Často obsahují informace týkající se kořenové příčiny selhání, aby bylo zajištěno, že nápravná opatření jsou dostatečně účinná, zda se jedná o opakující se příčinu selhání, náklady a pracovní hodiny potřebné k opravě zařízení a důvod, proč nebyla porucha včas diagnostikována [2,8,9,12]. Tyto informace jsou velmi důležité pro identifikaci dalších činností plánované údržby, vylepšení současného programu údržby nebo potřeby jeho výměny nebo přepracování. Základním předpokladem je, že výkon zařízení, systému lze zlepšit pouze předcházením poruch. Z tohoto důvodu je důležité identifikovat dřívější příčiny selhání a určit nápravná opatření, která tomuto selhání dokáží zabránit.

4.2. Zhodnocení aktuálního programu údržby

Přezkoumání pracovních příkazů [2,8,9,12] poskytuje dále informace o poruchovosti součástí. Tyto četnosti poruch lze porovnat s obecnými údaji, uvedenými např. v katalogu EPRI [12], aby se zjistilo, jestli existuje potenciál pro významné snížení četnosti poruch. Tato skutečná poruchovost je také využívána pro ekonomické modelování plánů údržby a výpočet nákladů na opravnou údržbu v důsledku selhání komponenty. Přezkoumání pracovních příkazů se dále používá k vývoji ročních činností nápravné údržby a určení, zda se poruchy zařízení zvyšují nebo snižují a jaká další nápravná opatření by mohla být vhodná pro dosažení pozitivní změny [2,8,9,11,12].

4.3. Posouzení výkonu systému

Přehled aktuálních plánů údržby lze použít pro plánování prodloužení životnosti komponenty specifické pro daný podnik mnoha způsoby. Data lze použít pro trendování a projekci výkonu nebo poruch do budoucnosti [2,8,9,11,12]. Pokud se jedná o nové zařízení, údaje o poruchách poskytují indikaci poruch, které lze očekávat v průběhu stárnutí komponenty a ukazují potenciální indikace problémů, které je třeba předvídat. Nejdůležitější je srovnání údajů s generickými údaji o výkonosti, které může naznačit oblasti, ve kterých by mohli existovat velké příležitosti k dosažení ekonomických a technických zlepšení [12].

Kroky zahrnuté v benchmarkingu [12] lze shrnout:

1. Na systémové úrovni se porovná podíl zpráv o událostech provozovaného systému k počtu zpráv o událostech jiných provozovatelů takového systému. To poskytne určité posouzení současného a minulého stavu systému a ukáže, zda systém pracuje na, nad nebo pod průmyslovým průměrem.
2. Na úrovni komponenty se porovnají poruchy komponent v provozovaném systému a obecnými údaji o poruchovosti těchto komponent pro diagnostiku a identifikaci potenciálně nepřijatelného výkonu součástí.
3. Porovnání periodické údržby systému s doporučením uvedeným v obecné databázi k přidání nebo odstranění aktivit periodické údržby a úprav souvisejících intervalů úkolů. Pokud výkon systému překračuje standardy a četnost poruch je podprůměrná, měly by se změny programu preventivní údržby provádět opatrně a s přijatelným důvodem. Na druhé straně, pokud výkon se systému výrazně odchyluje od doporučení, mely by být odchylky důkladně přezkoumány a identifikovány příčiny k jakékoli příležitosti ke zlepšení.
4. Přezkoumání provozních postupů pro zjištění výkonosti systému v rámci jednotlivých konstrukčních specifických hodnot a typových údajů poskytnutých výrobcem.
5. Kontrola nápravných pracovních příkazů a vyhodnocení hlavních příčin poruch systému pro zjištění, zda příčiny poruch odpovídají obecným zkušenostem.

6. Vytvoření databáze režimu detekce selhání z kontroly nápravného pracovního příkazu a určení, zda je schopen program periodické údržby detekovat degradaci a počínající poruchy.
7. Zajištění pro plán dlouhodobé údržby, aby zahrnoval důkladnou a kritickou kontrolu v souvislosti se stárnutím a stanovení míry selhání systému, předpokladu použití náhradních dílů, potenciální modernizací nebo renovací.

4.4. Posouzení generického stárnutí

Kontrola řízení stárnutí je nedílnou součástí plánování životnosti součástí [2,7,8,9,11,12]. Kromě dlouhodobého stárnutí pasivních součástí jsou aktivní součásti systému náchylné na opotřebení nebo degradaci. Tato degradace musí být řešena preventivní údržbou včetně generální opravy nebo výměny součástí. Vzhledem k rozmanitosti komponent používaných v různých konfigurací je důležité z obecných údajů získat určitý přehled o načasování selhání související s komponentami. Periodickou údržbu nebo nápravnou údržbu spojenou s výměnou opotřebovaných dílů lze řešit pomocí změny programu údržby.

Mnoho systémů je náchylné k technické zastaralosti, zejména systémy s elektronickým vybavením. Nutnost výměny součástí může být způsobena nedostupností náhradních dílů [8,10,12]. V takových případech je pravděpodobnost a načasování výměny systému nebo komponenty určené rychlosti selhání nebo degradace součásti a dostupnosti náhradních dílů z jiných zdrojů. V důsledku toho je třeba zvážit proveditelnost, náklady na reverzní inženýrství zastaralých komponent.

Pro zjištění systému náchylnému k technickému zastarávání můžeme použít kritéria dle [12]:

1. Komponenty nejsou jedinečné a jsou k dispozici i v budoucnu.
2. Komponenty vyrábí několik společností.
3. Poruchovost systému je dostatečně nízká, aby umožnila plánování nákupu a instalaci nových komponent bez ohrožení dostupnosti systému.

Pro pasivní systémy by mělo hodnocení stárnutí zahrnovat dle [10,12]:

1. Zvážení důležitosti netěsného dílu z hlediska funkčnosti systému.
2. Atributy návrhu, jako je materiál, prostředí atd.
3. Stáří komponenty.
4. Skutečný stav komponenty ve srovnání s očekávaným stavem.
5. Příčina poruch.
6. Zbývající životnost zařízení.
7. Náklady na celkovou opravu.

5. ZÁVĚR

Po posouzení stárnutí a spolehlivosti systému, komponenty se identifikují potenciální alternativní plány pro prodloužení životnosti [2,7-10,11,12]. Cílem je prozkoumat, zda existují potenciálně lepší způsoby řešení řízení stárnutí systému, konstrukce a komponent. Vstupy do hodnocení by měly pocházet nejen od zaměstnanců podniku, ale také by měly být požadovány od externích odborníků a srovnány s obecními požadavky srovnatelných projektů.

Závěrem lze říci, že význam údržby při prodlužování životnosti systému, komponent nelze podceňovat. Pravidelná údržba a kontroly jsou zásadní pro identifikaci a prevenci potenciálních problémů, stejně jako pro výměnu opotřebovaných nebo poškozených dílů. Zanedbání údržby může vést k nákladným opravám nebo dokonce úplnému selhání součásti. Proto je klíčové upřednostňovat takovou údržbu, aby byl zajištěn optimální výkon a životnost zařízení.

Poděkování: Autor děkuje za vedení práce, návrhy a připomínky doc. RNDr. D. Procházkové, CSc. DrSc.

LITERATURA

[1] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Řízení rizik procesů spojených s provozem technických zařízení po dobu jejich životnosti*. Doi:10.14311 /BK.9788001066751, 2019.

[2] EPRI. *Preventive Maintenance Basis Database (PMBD) v7.0.* Palo Alto: EPRI 2022.

[3] ROČEK, J., Průmyslové armatury. ISBN 859-4-315-0120-6. INFORMATORIUM 2008. 256 p.

[4] IAEA. *Guidance For Optimizing Nuclear Power Plant Maintenance Programmes*. IAEA-TECDOC-1383, ISBN 978-92-0-112703-0, Vídeň 2003.

[5] MELOUN, M., MILITKÝ, J. *Statistické zpracování experimentálních dat.* ISBN 80-200-1254-0. Praha: Academia 2004, 928 p.

[6] EPRI. *Guideline on Proactive Maintenance. Technical Report*. Palo Alto: EPRI 2001, 82 p.

[7] EPRI. *Demonstration of Life Cycle Management Planning for Systems, Structures, and Components.* Palo Alto: EPRI 2001, 208 p.

[8] EPRI. *Life Cycle Management Plan for Main Generators and Exciters at Diablo Canyon Power Plant.* Palo Alto: EPRI 2003, 174 p.

[9] EPRI. *Life Cycle Management Planning at Wolf Creek Generating Station.* Palo Alto: EPRI 2001, 288 p.

[10] EPRI. *Cathodic Protection System Application and Maintenance Guide.* Palo Alto: EPRI 2006, 260 p.

[11] OECD. *Status report on Nuclear Power Plant life management*. OECD 2000, 136 p.

[12] EPRI. *Plant Support Engineering: Life Cycle Mangement Planning Sourcebooks.* Palo Alto: EPRI 2008, 334 p

[13] BRIŠ, R., GUEDES SOARES, C. & MARTORELL, S., eds. *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362 p.

[11] 10CFR50.65. *Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Plants*. Office of the Federal Register. National Archives and Records Administration. U.S. Government Printing Office. Washington, D.C.

[15] IAEA. *Implementation and Review of Nuclear Power Plant Ageing Management Programme.* Safety Report Series No. 15. Vienna: IAEA 1999, 45 p.

OBRANA PROTI RIZIKŮM SPOJENÝM S OTEVŘENOU TECHNOLOGIÍ

DEFENCE AGAINST OPEN TECHNOLOGY RISKS

Tomáš Volf

ČEZ, a.s., Jaderná elektrárna Temelín, 373 05, Temelín, toma.volf@cez.cz

Abstrakt: Článek se zabývá problematikou ochrany společnosti ČEZ proti padělaným položkám, které v současné době představují velká rizika pro jaderné elektrárny. V zájmu zajištění bezpečnosti jaderných elektráren společnost ČEZ vytvořila speciální systém. Článek popisuje bezpečnostní aspekty a také cíle zmíněného systému.

Klíčová slova: Padělky, cizí materiály, jaderná elektrárna, rizika, bezpečnost, vyloučení cizích materiálů.

Abstract: The article deals with the issue of protecting the ČEZ against counterfeit items, which currently pose great risks to nuclear power plants. In order to ensure the safety of nuclear power plants, the ČEZ created a special system. The article describes the security aspects as well as the objectives of the system.

Key words: Counterfeits, foreign materials, nuclear power plant, risks, safety, exclusion of foreign materials.

1. ÚVOD

V současné době je velká pozornost Mezinárodní agentury pro atomovou energii [1], World Association of Nuclear Operators [2] věnována ochraně strategického průmyslu a objektům kritické infrastruktury před vnikem cizích předmětů do technologie. Existují případy, kdy cizí předměty v kritických zařízeních jaderných elektráren způsobily závažné nehody. Proto má ČEZ systém, který zajišťuje ochranu zařízení jaderných elektráren před vnikem cizích předmětů, a tím je FME [3].

2. SOUHRN POZNATKŮ O PROBLÉMU

Předměty, které zvenčí vniknou do technologických systémů elektrárny, nebo části zařízení, které se uvolní ze své projektové pozice, mohou během provozu nepříznivě ovlivnit funkci technologie, mohou způsobit poškození komponent a důležitých systémů. Důsledkem událostí s těmito předměty, které jsou označovány jako předměty „cizí“, může být:

- neplánovaná údržba (prodloužení plánované odstávky),
- zahájení odstávky neplánované,
- ohrožení bezpečného provozu,
- zvýšená radiační expozice personálu.

Cizí předmět je jakýkoliv předmět v technologii, který není součástí zařízení dle projektu nebo není na svém projektovém místě, a mohl by nežádoucím způsobem ovlivnit bezpečný nebo spolehlivý provoz technologických zařízení a jaderného paliva.

Otevřená technologie označuje stav výrobního technologického zařízení a navazujících systémů včetně částí těchto systémů (tj. strojní, elektro, měření a regulace) a včetně zařízení mimo projektovou pozici, kdy je možnost nekontrolovatelného vniknutí (pádu) cizích předmětů s rizikem poškození technologie nebo ztráty požadované funkce zařízení.

Systém FME (Foreign Material Exclusion – vyloučení cizích materiálů) je důležitý prvek v jaderném průmyslu, jeho cílem je:

- zajistit bezpečnost, spolehlivost a kvalitu výroby,
- předvídat a eliminovat nebo minimalizovat vnikání cizích předmětů do technologie, a to po celou dobu životnosti jaderné elektrárny.

Z pohledu jaderné i celkové bezpečnosti jaderných elektráren i jaderného průmyslu cizí předměty v technologii mohou způsobit:
- omezení chlazení jaderného paliva,
- poškození mechanických částí zařízení,
- zkrat na elektrickém zařízení,
- aktivaci nečistot v primárním okruhu.

Všechna tato poškození mohou vést ke zhoršení jaderné bezpečnosti nebo k ekonomickým ztrátám.

3. CÍL PROGRAMU FME

Cílem programu FME, který zavedl ČEZ [3] je stanovení opatření pro minimalizaci rizika nekontrolovatelného vniknutí cizích předmětů do otevřené technologie a stanovení pravidel při nálezu cizích předmětů. Základní předpoklady pro efektivní program zabránění vniknutí cizích předmětů do technologie jsou:
- identifikace rizik vniknutí cizích předmětů do otevřené technologie na daném zařízení,
- využívání technických a organizačních opatření k minimalizaci rizika vniknutí cizího předmětu do otevřené technologie,
- efektivní školení všech zaměstnanců o správném chování při přípravě a provádění prací na otevřeném technologickém zařízení,
- kontrolní mechanismy FME při provozu a údržbě zařízení elektrárny,
- zavedení a sledování klíčového ukazatele (KPI) programu FME,
- stanovení požadavků na dodavatelský řetězec.

4. OPATŘENÍ PROGRAMU FME

Opatření projektu FME zahrnují pravidla pro přípravu, realizaci, přerušení a ukončení prací. Patří do nich zejména:
- vymezení a označení FME pracoviště,
- kontrola vstupujících osob,
- kontrola stavu nářadí a materiálu, případná evidence vnášeného/vynášeného materiálu,
- všechen vnášený materiál musí být FME bezpečný (svými rozměry neumožňuje vnik do otevřené technologie, případně je proti vniknutí do otevřené technologie zabezpečen pevným úvazkem),
- nevnášení předmětů nepotřebných pro práci,
- důraz na čistotu a uspořádání pracoviště,
- při přerušení práce zabezpečení otevřené technologie (včetně demontované) proti vniku cizích předmětů (návleky, zátkami, plachtami, …),
- zajištění provedení kontroly na nepřítomnost cizích předmětů před uzavřením technologie,
- v případě vniku cizího předmětu nebo podezření na vnik do technologie informování odpovědné osoby, provedení vyjmutí cizího předmětu z technologie, kontroly čistoty, evidování nálezu.

5. ZÁVĚR

Systém FME představuje důležitý faktor v jaderném průmyslu, kde jsou bezpečnost a kvalita klíčovými faktory. Efektivní implementace zásad a pravidel FME přináší snížení rizika událostí způsobených vnikem cizích předmětů do technologie a pomáhá tak zvýšit úroveň bezpečnosti. Je důležité, aby provozovatelé jaderných elektráren věnovali pozornost systému FME a investovali čas a zdroje do školení personálu a zajištění odpovídajících technologií.

LITERATURA

[1] IAEA. *IAEA-TECDOC-1970. Foreign Material Management in Nuclear Power Plants and Projects.* ISBN 978-92-0-124221-1. Vienna: IAEA 2021, 244 p.

[2] WANO. *Guideline WANO GL 2009-01(Rev-1). Guidelines for Achieving Excellence in Foreign Material Exclusion (FME).* London: WANO 2012.

[3] ČEZ. *Zásady pravidel práce na otevřeném technologickém zařízení JE.* Praha: ČEZ 2023

ZDROJE RIZIK SPOJENÉ S POVRCHOVÝM KALENÍM LITIN LASEREM

SOURCES OF RISKS ASSOCIATED WITH LASER SURFACE HARDENING OF CAST IRON

Ladislav Záhon, Jiří Kuchař, Jakub Horník

ČVUT v Praze, Fakulta strojní, Technická 4, 166 07, Praha 6; ladislav.zahon@fs.cvut,cz

Abstrakt: Článek pojednává o rizicích spojených s procesem povrchového kalení vybraných druhů litin. Ve článku je zmíněn obecný princip povrchového kalení, dále je zde popsána problematika kalení laserem včetně jednotlivých faktorů, které zvyšují rizika vzniku kalené struktury s nevhodnými mechanickými vlastnostmi.

Klíčová slova: Povrchové kalení, laser, litiny, ADI, ferit, perlit, ausferit

Abstract: The article discusses the risks associated with the process of surface hardening of selected types of cast irons by laser. The general principle of surface hardening is mentioned in the article, then the problems of laser hardening are described, including individual factors that increase the risk of formation of hardened structure with unsuitable mechanical properties.

Key words: Surface hardening, laser, cast irons, ADI, ferrite, pearlite, ausferite.

1. ÚVOD

Litiny jsou přes svou poměrně dlouhou historii stále nezastupitelným materiálem ve slévárenském průmyslu. To je dáno především jejich vlastnostmi, které souvisí s jejich metalurgií. Nejběžnější jsou litiny, jejichž stupeň eutektičnosti (S_c) je blízký jedné, tak aby dvoufázové pásmo (rozdíl mezi křivkami likvidu a solidu) bylo co nejmenší. Další výhodou litin (grafitických) je expanze grafitu, při kterém dochází ke kompenzaci zmenšování objemu litiny při tuhnutí. Tento faktor vede ke značnému snížení rizika vzniku staženin, které by znehodnotily odlitek [1,2].

Z výše zmíněných důvodů je i v současné době kladen velký důraz na výzkum a rozvoj litin. Velmi progresivním materiálem jsou izotermicky zušlechtěné litiny. Tepelným zpracováním grafitických litin lze docílit typické ausferitické struktury [3,4]. Takové litiny dosahují vysoké pevnosti (mez kluzu $R_{p0,2}$ = 1300 MPa), současně však mají poměrně vysokou houževnatost, která je spojená s vysokouhlíkovým austenitem obsaženým ve struktuře [3,5]. Dalším předmětem výzkumu je v současné době použití laseru pro kalení různých druhů litin. Povrchové kalení laserem má řadu specifik a zdrojů rizik, které je potřeba při tomto procesu uvažovat [3-6].

2. POVRCHOVÉ KALENÍ

Povrchové a objemové kalení se ve své podstatě příliš neliší. V obou případech spočívá proces v ohřátí materiálu do oblasti austenitu (austenitizace) [7,8]. Poté následuje rychlé ochlazení, s tím je spojena martenzitická transformace austenitu. Hlavním cílem povrchového kalení je zvýšení tvrdosti povrchu a současné zachování původní houževnatosti jádra součásti. Zvýšení tvrdosti má pak značný význam pro odolnost povrchu proti opotřebení. Při martenzitické transformaci dochází také k nárůstu objemu (až 4 %), tím dochází ke vzniku tlakových napětí v povrchových vrstvách součásti. Tato napětí pak přispívají ke zvýšení únavové pevnosti, dochází totiž k omezení vzniku a šíření únavových trhlin [7-10].

Zásadními prvky procesu povrchového kalení je intenzita ohřevu povrchu a odvod tepla do jádra součásti. To způsobuje vznik tepelného gradientu, protože společně s rostoucí rychlostí ohřevu roste i tepelný gradient. Příliš intenzivní ohřev zvyšuje riziko znehodnocení povrchu (spálení nebo přehřátí). Důležité je tak kontrolovat rychlost ohřevu, která ovlivňuje tepelný gradient a hloubku zakalené vrstvy. Pomalejší ohřev vede k menšímu tepelnému gradientu a větší tloušťce zakalené vrstvy. Další faktor, který je potřeba uvažovat a který může zvyšovat riziko vzniku nevhodné struktury po zakalení je změna teploty fázových přeměn v závislosti na rychlosti ohřevu. S rostoucí rychlostí ohřevu se posouvá interval fázových přeměn do vyšších teplot. Při povrchovém kalení se tak obvykle používají výrazně vyšší teploty než při kalení objemovém [7-10] .

Pokud je austenitizační teplota pro danou rychlost ohřevu příliš nízká, zvyšuje se riziko, že dojde k nedostatečné homogenizace austenitu. Tento jev následně vede ke zhoršení mechanických vlastností. Naopak příliš vysoká austenitizační teplota způsobuje značné hrubnutí zrna a dochází ke zvyšování podílu zbytkového austenitu v zakalené vrstvě, a tím jsou opět nepřijatelně ovlivněny mechanické vlastnosti [7-10].

3. POVRCHOVÉ KALENÍ LASEREM

Laser je velmi výkonný zdroj energie. Rychlost dodávání tepla do povrchových vrstev je výrazně vyšší než rychlost odvádění tepla do chladného jádra [8,13]. Vzniká tak značný tepelný gradient. Povrch součásti dosáhne působením laseru velmi rychle austenitizační teplotu. Následným pohybem paprsku do jiné oblasti dochází k odvodu tepla z ohřátého místa do jádra součásti a rychlé ochlazení způsobí zakalení struktury. Toto je jedna z největších výhod použití laseru pro kalení. Při použití konvenčních metod povrchového kalení (kalení plamenem nebo indukční kalení) totiž nevzniká tak výrazný tepelný gradient. Pro dostatečně rychlé ochlazení povrchu je při těchto metodách využíváno vodní sprchy, případně ponoru [7,8]. Současně je nutné při konvenčních metodách upravit nástroj (hořák nebo induktor) dle konkrétního tvaru povrchu součásti [7,8,11-13].

Pro omezení rizik, jejichž zdroje jsou v okolním prostředí na laserem zpracovávaný povrch je možné využít ochranných plynů, které toto působení omezí [13]. Laserem zakalený povrch obvykle dosahuje lepších mechanických vlastností v porovnání s povrchy konvenčně kalenými. To je dáno vysokou rychlostí ohřevu a vyšší nukleací austenitu; vznikající martenzit je tak výrazně jemnější [7,8,11-13] .

Mezi hlavní nevýhody laserového kalení lze zařadit pořizovací a provozní náklady [7]. Dalším problémem může být relativně malá tloušťka zakalené vrstvy, která je ovlivněna kaleným materiálem a procesními parametry. S rostoucí intenzitou laseru roste i tepelný gradient, a proto austenitizace povrchových vrstev je tak omezena teplotou tání daného materiálu. Regulací výkonu paprsku do jisté míry lze korigovat požadovanou hloubku kalení, což současně však může zvyšovat riziko nedostatečného odvodu tepla z kaleného místa, a to následně může omezit martenzitickou transformaci v povrchových vrstvách [7,8,11-13] .

Při laserovém kalení je také nutné uvažovat rizika spojená s nevhodným tvarem součásti citace. Problém jsou komplikované součásti, především jejich hrany. Ostré hrany totiž mohou způsobit nerovnoměrný tepelný tok v povrchových vrstvách. Odvod tepla z povrchu tak může být omezen, a tím se zvyšuje riziko natavování materiálu [8,12] .

4. ZDROJE RIZIK SPOJENÉ S POHYBEM LASERU

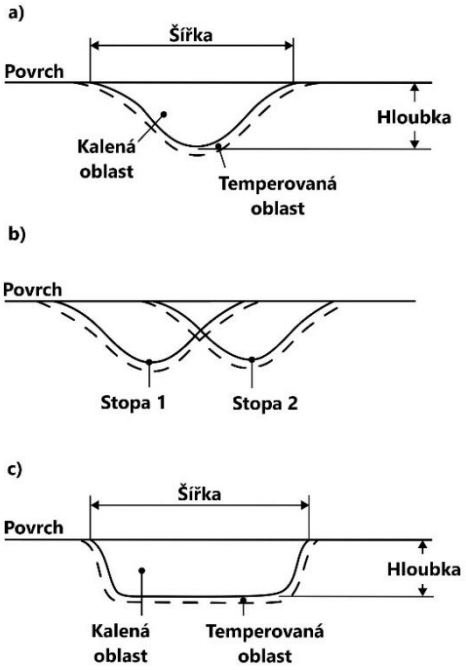
Zásadním faktorem pro laserové kalení je samotný pohyb laserového paprsku po kaleném povrchu. Nevhodným pohybem totiž může docházet k nežádoucímu a nepřijatelnému ovlivnění kalené struktury, a tím se následně zvyšuje riziko selhání povrchových vrstev při jejich pracovním zatížení [8,12]. Obecně je možné uvažovat několik základních variant procesu kalení, které jsou zobrazeny na obrázku 1, varianta „a“ znázorňuje samostatný průchod paprsku. Tímto je docíleno zakalení několika milimetrů širokého pásu, a z tohoto důvodu má tato varianta velmi omezené využití. Obvykle je totiž žádoucí zakalení mnohem větší plochy. Toho je možné docílit variantou „b“ (Obrázek 1). Zde dochází k postupnému kladení jednotlivých stop laseru paralelně. Při této variantě však vzniká zásadní problém [8,11,12,14-17] .

Při kladení stop paralelně totiž dochází k jejich vzájemnému ovlivnění. Teplo vnášené do materiálu při kladení další stopy může způsobit popuštění předchozí zakalené stopy. Tím dochází ke značnému lokálnímu poklesu tvrdosti (Obrázek 2 b, c). Pokles tvrdosti pak může značně zvyšovat riziko intenzivního opotřebení kaleného povrchu [8,12]. Ke zpětnému popuštění může také docházet u rotačních součástí, kdy dochází ke kontaktu počátku a konce stopy laseru [9,11,12,14-17] .

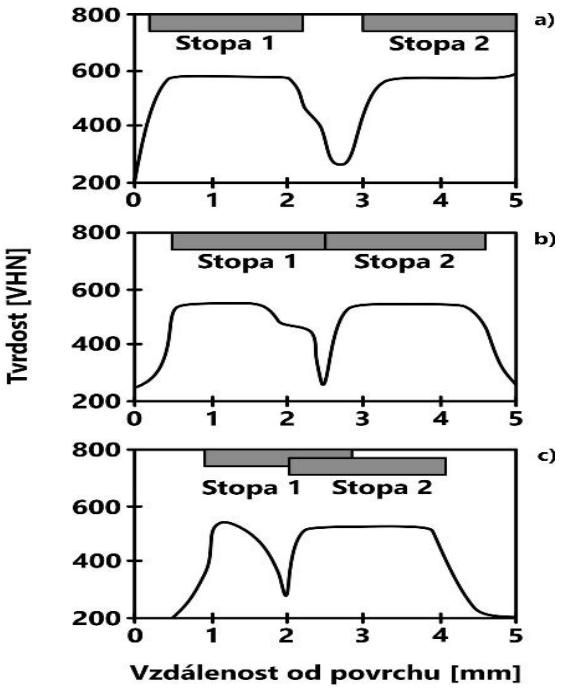
Pokles tvrdosti však nemusí být nutně nežádoucí [17]. Některé výzkumy [12,17] ukazují, že dochází ke zvýšení odolnosti proti opotřebení. Oblast s menší tvrdostí totiž může napomáhat efektivnějšímu mazání kontaktu, současně může zachytávat částice vznikající při opotřebení.

Zpětné popuštění a s tím spojené riziko zhoršení tribologických vlastností lze částečně eliminovat [13]. Používá se k tomu tzv. rozmítaný paprsek. Zrcadly je řízen pohyb laserového paprsku. Vysoká rychlost kmitajícího laseru následně způsobí relativně rovnoměrný tepelný tok. Tento případ je zobrazen na obrázku 1c, šířka takto vzniklé stopy je běžně několik desítek milimetrů. Tímto způsobem tak lze rovnoměrně, bez zpětného popuštění zakalit výrazně větší plochy, pokud je šířka této stopy větší než šířka kalené oblasti, tak nedochází ke zpětnému popuštění

vůbec [13,14]. Pokud je šířka kalené plochy větší, je zpětné popuštění nevyhnutelné a dochází tak k nárůstu rizika spojeného s nedostatečnou vlastností daného povrchu [8,11-17] .



Obr. 5. Možné varianty laserového kalení, upraveno autorem dle [11].



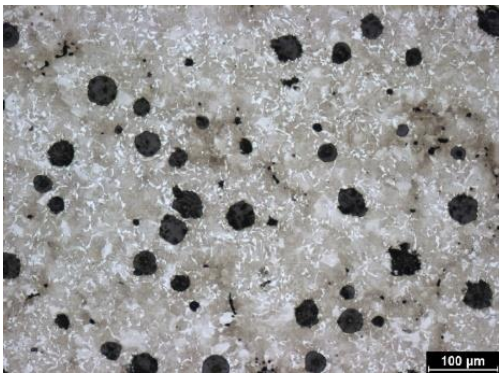
Obr. 6. Tvrdost kaleného povrchu pro různé varianty laserového kalení, upraveno autorem dle [18].

5. ZDROJE RIZIK SPOJENÉ S VÝCHOZÍ STRUKTUROU PŘI LASEROVÉM KALENÍ LITIN – EXPERIMENT

Jak již bylo zmíněno, proces laserového kalení se od konvenčního objemového kalení nijak zásadně neliší. Zásadním rozdílem je rozdílná rychlost ohřevu. Je tedy nutné uvažovat vliv výchozí struktury na austenitizaci, velmi důležitá je distribuce uhlíku. Žádoucí je získání austenitu s rovnoměrně rozloženým uhlíkem, tím totiž lze dosáhnout vyhovující martenzitické struktury. Výchozí struktura obsahuje uhlík, který je vázaný ve formě karbidů nebo grafitu. Austenitizací by měla být zajištěna redistribuce tohoto uhlíku, tak aby byla uhlíkem obohacena i místa, která byla původně feritická (ferit má značně omezenou rozpustnost uhlíku). Pro zajištění rovnoměrné distribuce uhlíku v austenitu je však nezbytný určitý čas. Vyšší teploty napomáhají difuzi uhlíku ve struktuře. Na základě současného poznání [7,8,11-13], problémovými strukturami mohou být například hrubá perlitická struktura nebo grafitická litina s feritickou matricí.

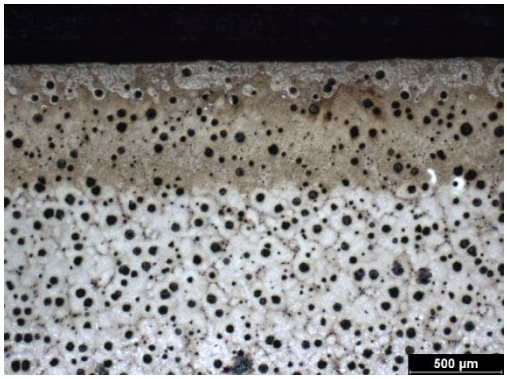
V experimentální části [19] bylo laserem zakaleno několik vybraných druhů litin. U některých typů litin je samotná struktura (zejména izotermicky zušlechtěné litiny – ADI, AGI). Vliv laseru v některých zmíněných případech není zcela jasný.

Na obrázku 3 je zobrazena litina jejíž výchozí struktura je převážně perlitická, jsou zde patrné i oblasti, které obsahují ferit, bainit, acikulární ferit a vysokohulíkový austenit. Litina byla podrobena pravděpodobně určitému izotermickému zušlechtění, nicméně při tepelném zpracování nejspíše došlo k nějakým problémům. Struktura je tak v podstatě perlitická, mohly tomu napomoci perlitotvorné prvky obsažené v této litině (Cu, Ni).



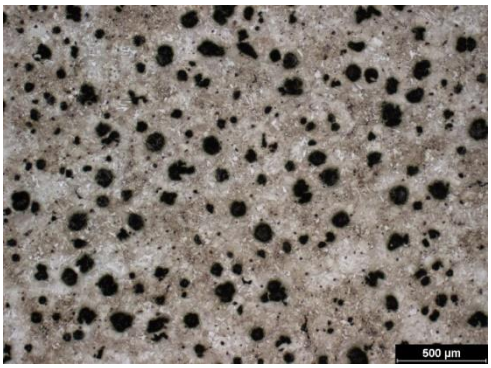
Obr. 7.Výchozí převážně perlitická struktura [19].

Vzhledem k výchozí perlitické struktuře, je distribuce uhlíku poměrně rovnoměrná. Při ohřevu povrchu laserem tak uhlík nemusí překonávat dlouhé difuzní vzdálenosti. Tímto je sníženo riziko heterogenit v zakalené vrstvě. Na obrázku 4 je patrné, že povrchovým kalením laserem vznikla souvislá martenzitická struktura. Při působení laseru došlo k částečnému natavení povrchu, a následným rychlým tuhnutí vznikla metastabilní karbidická struktura. Jedná se v podstatě o další metodu zpevňování povrchových vrstev laserem (laser glazing).



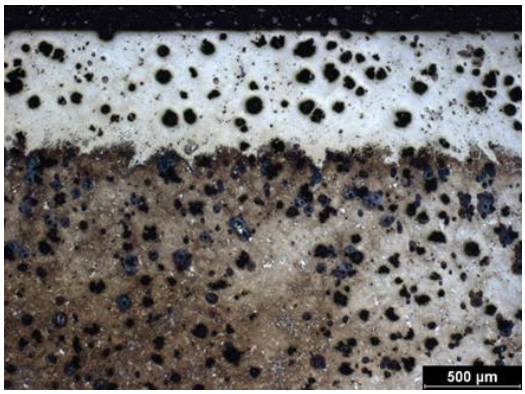
Obr. 8. Souvislá zakalená martenzitická vrstva s karbidickým povrchem [19].

Další typ litiny je zobrazen na obrázku 5, jedná se o izotermicky zušlechtěnou litinu s kuličkovým grafitem. Výchozí struktura je tedy ausferitická, tvoří ji acikulární ferit a vysokouhlíkový austenit. Tento typ litiny se získává tepelným zpracováním, které spočívá v austenitizace a následném rychlém ochlazení (litina se musí vyhnout oblastem perlitu a feritu). Grafitické litiny obsahují křemík, který mění aktivitu uhlíku a omezuje tvorbu karbidů, při izotermické výdrži rostou desky feritu z grafitických útvarů, jejich orientace je náhodná. Růstem feritu (má omezenou rozpustnost uhlíku) dochází k obohacení okolního austenitu o uhlík, tím dochází k jeho stabilizaci. V závislosti na teplotě izotermické výdrže se mění struktura a distribuce uhlíku. Tato problematika je však nejasná a je stále předmětem výzkumů.



Obr. 9. Výchozí ausferitická struktura [19].

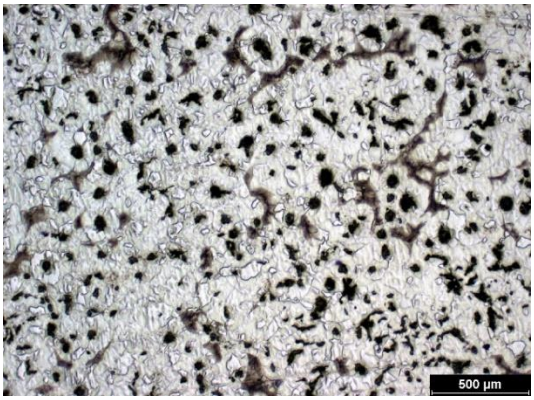
Uhlík je v ausferitické struktuře poměrně rovnoměrně rozložen (do jisté míry to však závisí i na zmíněné teplotě izotermického zušlechtění). Rovnoměrná distribuce uhlíku ve struktuře pak napomáhá získání souvislé martenzitické struktury (Obrázek 6) s vhodnými mechanickými vlastnostmi.



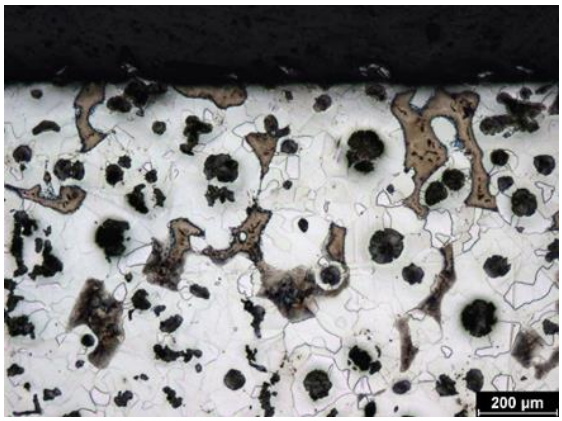
Obr. 10. Souvislá martenzitická vrstva s ausferitickým jádrem [20].

Na obrázku 7 je zobrazena litina s feritickou matricí. Ferit má obecně velmi malou rozpustnost uhlíku (do 0,02 %), feritická matrice tak obsahuje jen minimální množství uhlíku.

Při ohřívání povrchu laserovým paprskem dochází k difuzi uhlíku ve struktuře litiny. Uhlík difunduje z grafitických útvarů do okolní matrice. Příliš vzdálená místa zůstávají uhlíkem neobohacená. Při rychlém chladnutí materiálu dochází k martenzitické transformaci pouze v místech, kde je dostatečné množství uhlíku. Tímto způsobem se tak tvoří martenzitické oblasti obalující grafit (Obrázek 8). Laserem zpracovaná vrstva je výrazně nesouvislá. Heterogenní struktura, která je tvořena fázemi s tak odlišnými mechanickými vlastnostmi, značně zvyšuje riziko intenzivního opotřebení.

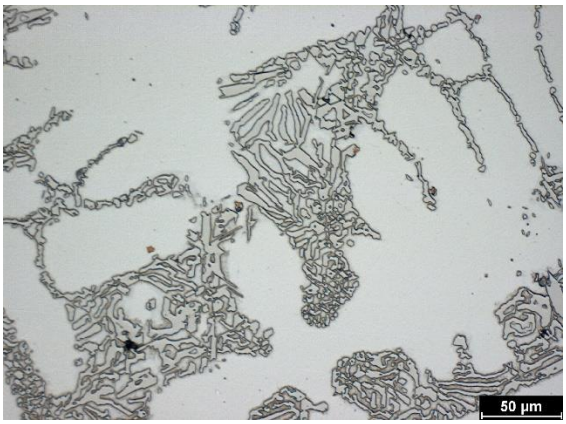


Obr. 11. Výchozí feritická struktura [19].



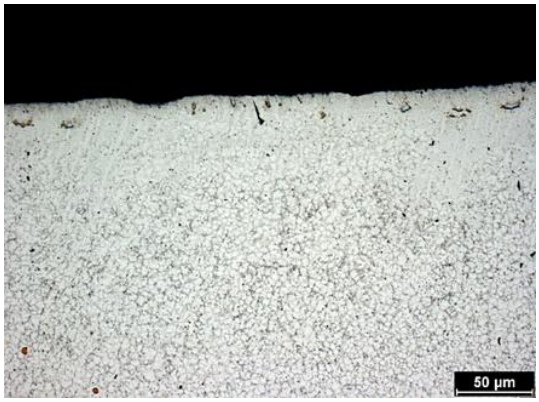
Obr. 12. Nesouvislá martenzitická vrstva s feritickými oblastmi [19].

Na obrázku 9 je zobrazena výchozí struktura vysokochromové karbidické litiny. Struktura je tvořena austenitem, martenzitem a jemnými eutektickými karbidy typu M_7C_3. Použití laseru pro úpravu povrchu tohoto typu litin je velmi neobvyklé, tato problematika skýtá řadu rizik [19,21] rozsáhlejší výzkumy zatím neexistují.



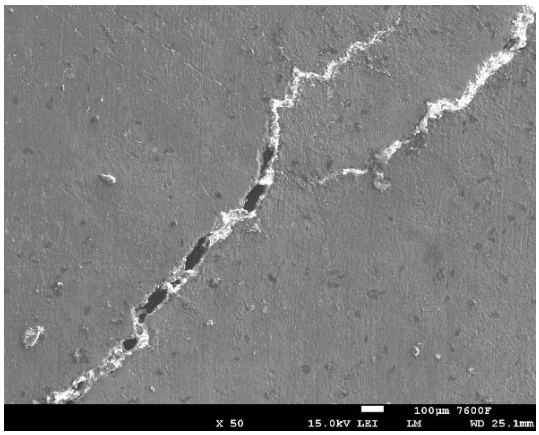
Obr. 13. Výchozí struktura vysokochromové karbidické litiny [19].

Na obrázku 10 je vyobrazen povrch, který byl vystaven laserovému paprsku. Na první pohled je patrná změna struktury. Působením laseru došlo k natavení povrchových vrstev. Tímto způsobem došlo k výraznému zjemnění struktury. I toto zjemnění má určitý vytvrzující efekt, nárůst tvrdosti kaleného povrchu proti nekalenému jádru však není příliš velký. Samotné vysokochromové litiny jsou vzhledem ke karbidické struktuře velmi tvrdé a používají se v různých tribologických aplikacích.



Obr. 14. Laserem zpracovaný povrch vysokochromové karbidické litiny [19].

Výchozí struktura vysokochromových litin má mnoho zdrojů rizik [19]. Vzhledem k obsahu velkého množství legur (tato konkrétní litina obsahuje 26,66 % Cr) a karbidické struktury, je tepelná vodivost těchto litin velmi nízká [21]. To je poměrně zásadní problém. Při kalení těchto litin hrozí porušení celistvosti povrchových vrstev litiny (Obrázek 11). Takový povrch je nezpůsobilý pro pracovní zatížení.



Obr. 15. Trhliny vzniklé na povrchu vysokochromové karbidické litiny [19].

6. ZÁVĚR

Povrchové kalení litin laserem je do jisté míry stále experimentální metodou, která může skýtat řadu zdrojů rizik. Celý proces je ovlivňován tvarem součásti, který může ovlivňovat odvod tepla z kaleného místa. Mění se tak tepelný gradient a může docházet ke vzniku nevhodné struktury kalené vrstvy. Dalším zásadním zdrojem rizik může být i zpětné popouštění kalené stopy. To lze částečně eliminovat výše zmíněným rozmítaným paprskem. Zásadním faktorem spojeným se zdroji rizik při povrchovém kalení litin laserem je samozřejmě struktura dané litiny, míra legování, případně distribuce uhlíku.

Poděkování: Článek byl podpořen projektem SGS22/156/OHK2/3T/12 (Vliv povrchových úprav na kvalitu výrobních technologií).

LITERATURA

[1] ROUČKA, J. *Metalurgie litin.* ISBN 80-214-1263-1. Brno: PC-DIR 1998, 165 p.

[2] NĚMEC, M., BEDNÁŘ, B., STUNOVÁ, B. *Teorie slévání*. 1. vyd. ISBN 978-80-01-04395-0. Praha: Česká technika – nakladatelství ČVUT 2009, 187 p.

[3] WANG, B., BARBER, G., QIU, F., ZOU, Q., YANG, H. A Review: Phase Transformation and Wear Mechanisms of Single-Step and Dual-Step Austempered Ductile Irons. *Journal of Materials Research and Technology*. (2020), pp. 1054–1069. Doi: 10.1016/j.jmrt.2019.10.074.

[4] MEIER, L., HOFMANN, M., SAAL, P., VOLK, W., HOFFMANN, H., In-situ Measurement of Phase Transformation Kinetics in AUSTEMPERED DUCTILE iron. *Materials Characterization*. ISSN 1044-5803. (2013), pp. 124–133. Doi: doi.org/10.1016/j.matchar.2013.09.005.

[5] WANG, B., QIU, F., BARBER, G., PAN, Y., CUI, W., WANG, R., Microstructure, Wear Behavior and Surface Hardening of Austempered Ductile Iron. *Journal of Materials Research and Technology*. 2020. Doi: 10.1016/j.jmrt.2020.06.076.

[6] MUSSA, A., KRAKHMALEV, P., BERGSTRÖM, J. Wear Mechanisms and Wear Resistance of Austempered Ductile Iron in Reciprocal Sliding Contact. Wear. ISSN 0043-1648. 2022, Doi: 10.1016/j.wear.2022.204305.

[7] PTÁČEK, L. *Nauka o materiálu*. 2. vyd. ISBN 80-7204-248-3. Brno: CERm 2002, 187 p.

[8] ASM. Heat Treating. *ASM Handbook.* ISBN 0-87170-379-3. Volume 4 - Materials Park: ASM International, 1991, pp. 286-295.

[9] JECH, J. Tepelné zpracování oceli: Metodická příručka. 4. vyd. Praha: SNTL 1983, pp 100-103.

[10] GADHE, P., BATHE, R. Laser Materials Processing for Industrial Applications. *Proceedings of the National Academy of Sciences*, India Section A: Physical Sciences. 2018. Doi: 10.1007/s40010-018-0523-5.

[11] RAJAN, T. V., SHARMA, C. P., SHARMA, A. *Heat Treatment: Principles and Techniques*. 2. vyd. ISBN 978-81-203-4095-4. New Delhi: PHI Learning, 2011, 153 p.

[12] STEEN, W. M., MAZUMDER, J. *Laser Material Processing*. 4th ed. ISBN 978-1-84996-061-8. London: Springer 2010, 315 p.

[13] READY, J. F. *Industrial Applications of Lasers.* 2nd ed. ISBN 0-12-583961-8. San Diego: Academic Press 1997, 380 p.

[14] GRUM, J. Laser Surface Hardening. In*: Encyclopedia of Tribology*. ISBN 978-0-387-92897-5. Boston, MA: Springer US 2013, pp. 1948–1962. Doi: 10.1007/978-0-387-92897-5_1007.

[15] GIORLEO, L., PREVITALI, B., SEMERARO, Q. Modelling of Back Tempering in Laser Hardening. *The International Journal of Advanced Manufacturing Technology*. 2011, pp. 969–977. Doi: 10.1007/s00170-010-3008-5.

[16] ANUSHA, E.; KUMAR, A., SHARIFF, S. Finite element Analysis and Experimental Validation of High-Speed Laser Surface Hardening Process. *The International Journal of Advanced Manufacturing Technology*. 2021. pp. 2403-2421. Doi: 10.1007/s 00170-021-07303-z.

[17] ZHANG, X.M., MAN, H.C., LI, H.D. Wear and Friction Properties of Laser Surface Hardened En31 Steel. *Journal of Materials Processing Technology*. ISSN 0924-0136. (1997), 1, pp. 162–166. Doi: 1016/S0924-0136(97)00011-3.

[18] BERGMANN, H. W. Laser Surface Melting Of Iron-Base Alloys. In: *Laser Surface Treatment of Metals.* ISBN 978-94-009-4468-8. Springer Netherlands, 1986, pp. 351–368. Doi: 10.1007/978-94-009-4468-8_34.

[19] ZÁHON, L. Povrchové kalení litin a tribologická analýza kaleného povrchu. *Diplomová práce ČVUT v Praze*. Praha: ČVUR 2023. https://dspace.cvut.cz/handle/10467/ 111428.

[20] MORES, A., HORNÍK, J., MAZÁČOVÁ, V., KRČIL, J., SKRBEK, B., NĚMEC, M. Povrchové laserové kalení odlitků s kuličkovým a lupínkovým grafitem po izotermickém kalení. *Sborník přednášek z 57. slévárenských dnů*. 1. vyd. Brno: Česká slévárenská společnost, z.s., člen ČSVTS Praha, 2021. https://www.slevarenskedny.cz/sborniky/sborn%C3%ADk_57_slevarenske_dny_ final.pdf.

[21] LAIRD, G.; GUNDLACH, R.; ROHRIG, K. *Abrasion Resistant Cast Iron Handbook.* 3. vyd. ISBN 978-0-87433-224-7. Schaumburg: American Foundry Society 2000, 53 p.

Titul:	Řízení rizik procesů, zařízení a složitých technických děl zacílené na a bezpečnost 2023
Editor:	Doc. RNDr. Dana Procházková, CSc., DrSc.
Recenzenti:	Doc. Ing. Hana Bartošová, CSc. Dr.h.c. Doc. Ing. Branislav Lacko, CSc. RNDr. Jan Procházka, Ph.D.
Vydavatel:	ČVUT v Praze
Forma	Elektronická DSPACE
Počet stránek:	236
Rok vydání:	2023

Odborné připomínky k článkům od recenzentů i editora vypořádali autoři ve spolupráci s editorem. Editor dále provedl formální úpravy, uspořádání textu a základní jazykové korekce.

ISBN 978-80-01-07239-4

Doi: https://doi.org/10.14311/BK.9788001072394