Česká společnost pro jakost, Novotného lávka 5, 110 00 Praha 1

Aktivity ČR v rámci European Safety and Reliabitily Assocation

Materiály ze 73. semináře Odborné skupiny pro spolehlivost
konaného dne 4. 12. 2018 v Praze

Odborný garant semináře:
prof. Ing. Zdeněk VINTR, CSc., dr.h.c.

Obsah

ESRA-Evropská asociace pro bezpečnost a spolehlivost

prof. Ing. Radim Briš, CSc.

Fakulta elektrotechniky a informatiky, Vysoká škola báňská – Technická univerzita Ostrava

radim.bris@vsb.cz

1 Anotace

ESRA - European Safety and Reliability Association, oficiálně existuje se svým zvoleným vedením od roku 1993 jako legální nezisková evropská organizace, která je v souladu s evropskou legislativou, se sídlem v Bruselu. V přednášce jsou prezentovány informace o současné působnosti této asociace v Evropě i ve světě. Jsou zmíněny základní cíle působnosti této asociace, aktivity, informace o technických komisích, sponzoring, jak se stát členem atd.

2 Hlavní cíle

Cílem je propagace a aplikace technik bezpečnosti a spolehlivosti a dále management rizika ve všech oblastech technologií. ESRA je nezisková organizace a rovněž se zdržuje politických aktivit.

ESRA dlouhodobě provozuje tyto cíle:

- Zajišťuje vedení informační sítě mezi členskou základnou a různými průmyslovými, akademickými, či profesionálními organizacemi a dalšími zainteresovanými osobami;
- Podporuje a prosazuje dobré zkušenosti v aplikacích bezpečnostních a spolehlivostních technik a v managementu rizika;
- Podporuje spolupráci mezi národními profesionálními asociacemi, průmyslovými skupinami nebo asociacemi zajišťujícími vzájemnou výměnu informací v oblasti bezpečnosti a spolehlivosti;
- Podporuje formování profesionálních společností (sdružení) nebo asociací v EU, kde ještě neexistují;
- Podporuje roli národních společností nebo asociací, jak na národních, tak i na mezinárodních úrovních;
- Podporuje kontakty s organizacemi aktivními v této oblasti (bezpečnost a spolehlivost), jak uvnitř, tak i vně zemí EU. Mezinárodní skupiny a profesionální společnosti (asociace) mající podobné anebo doplňkové zájmy jako ESRA se mohou přidružit k těmto aktivitám formou součinnosti přes ESRA sekretariát atd;
- Podporuje významná vzdělávací a technická školení v této oblasti a harmonizuje získané zkušenosti.
- Garantuje konference typu Esrel – organizační a vědecká úroveň (prostřednictvím ESRA Board a TC), schvalování a výběr hlavního pořadatele, finanční záležitosti, atd.

3 Členství v ESRA (institucionální) – stav 2018

Organizace vyžadující členství musí kontaktovat generálního sekretáře ESRA, kterým je v současnosti Roger Flage; roger.flage@uis.no

Stávající instituce: 67

Odcházející instituce: 8 (6)

Bez odezvy: 49

Nové členské instituce: 6

Celkově stávající + noví: 73

Roční poplatek za členství v ESRA:

Akademické instituce: €115

Profesionální organizace: € 345

Komerční organizace: € 575

Příjmy za poplatky: cca 8.000 € /rok

Další příjmy: z konferencí Esrel, cca 5-15.000 € / rok.

Důvody pro členství v ESRA

- Sleva cca 100 € na jednoho účastníka Esrelu (z částky 600 €), který pochází z členské instituce ESRA.
- Možnost účasti v technických komisích (TC): monitorovat nejnovější poznatky v daných oblastech, živé diskuse a výměny poznatků a zkušeností v rámci TC
- Organizace workshopů, seminářů a „webinars“ v důležitých tématech – možnost žádat o podporu (až 3000 € ročně)
- Poskytuje síť pro výzkum v daných oblastech.

4 Hospodaření ESRA

Majetek je přibližně 230.000 €. Největší výdaje jsou na podporu tematicky orientovaných workshopů a seminářů, cca 16-18.000 €/rok, což přibližně odpovídá ročním příjmům.

5 Vedení ESRA - ESRA Board

Chairman	Marko Čepin	University of Ljubljana, Slovenia
Vice-Chairman	Luca Podofillini	Paul Scherrer Institute, Switzerland
Treasurer	Stefan Bracke	University of Wuppertal, Germany
General Secretary	Roger Flage	University of Stavanger, Norway

Vedení je voleno vždy na období 2 let tajně (1 funkcionář může být zvolen na maximálně 2 období) generálním shromážděním ESRA (zástupci členských institucí), které probíhá každoročně při příležitosti konference ESREL.

Web adresa ESRA: http://esrahomepage.eu/

Oficiální znak:

Obr. 1: Oficiální znak ESRA

6 Časopisy spojené s ESRA

ESRA Newsletter

http://esrahomepage.eu/home.aspx?lan=230&tab=2767&itm=2832&pag=1679

Pro účely základní komunikace mezi vedením ESRA a členskou základnou. Časopis je jen v elektronické verzi, má svoji ediční radu, která přispívá vším, co se děje okolo ESRA: úvodník od prezidenta ESRA, blížící se konference s tematikou ESRA, změny v členských institucích, změny v komisích TC, účelově orientované články, občas i nové úspěšné dizertace pokrývající tematiku ESRA, atd.

Journal of Risk and Reliability (IF 1.373 Q2)

Časopis The *Journal of Risk and Reliability* je oponovaný časopis pro výzkumníky i aplikátory, kteří jsou zainteresováni do oblasti rizikových analýz a spolehlivostního inženýrství. Časopis publikuje články vysoké kvality pokrývající všechny teoretické i praktické otázky spojené s návrhem spolehlivosti a s bezpečným provozem inženýrských systémů z jakéhokoliv průmyslového sektoru.

Reliability Engineering and System Safety (IF 4.139, Q1, D1)

Je mezinárodní časopis věnovaný výzkumu, vývoji i aplikacím metod pro zlepšení bezpečnosti a spolehlivosti komplexních technologických systémů, jako jsou jaderné elektrárny, chemické podniky, řešení nebezpečných odpadů, vesmírné, či námořní systémy, ropné plošiny, dopravní systémy, kritické infrastruktury, atd. Časopis normálně publikuje pouze články, zahrnují analýzu zásadních problémů vztažených ke spolehlivosti komplexních systémů, nebo prezentuje techniky nebo významné teoretické výsledky, přispívající k řešení problematiky spolehlivosti. Významným cílem je dosažení rovnováhy mezi akademickými výsledky a praktickými aplikacemi.

Tematicky je orientován na taková témata, která se řeší v rámci technických komisí ESRA a na konferencích ESREL.

7 Technické komise - ESRA Technical Committees

Metodologicky orientované komise:

Název komise	*Vedení komise*
1. Accident and Incident Modeling	Stig Johnsen, Nicola Paltrinieri
2. Economic Analysis in Risk Management	Eirik B. Abrahamsen
3. Foundational Issues in Risk Assessment and Management:	Terje Aven, E. Zio
4. Human Factors and Human Reliability	Luca Podofillini, Chiara Leva
5. Maintenance Modeling and Applications:	Christophe Bérenguer, M. Fouladirad
6. Mathematical Methods in Reliability and Safety	John Andrews, Nicolae Brinzei
7. Prognostics and System Health Management	Piero Baraldi, Enrico Zio
8. Resilience Engineering	Ivonne Herrera, Eric Rigaud
9. Risk assessment	Marko Cepin, Henrik Hassel
10. Risk Management	Lesley Walls, David Vališ, Marcelo Hazin
11. Simulation for Safety and Reliability Analysis:	Nicola Pedronim, Edoardo Patelli
12. Structural Reliability	Jana Marková, Martin Krejsa
13. System Reliability	Gregory Levitin, Serkan Eryilmaz
14. Uncertainty analysis	Emanuele Borgonovo, Roger Flage
15. Innovative Computing Technologies in Reliability and Safety:	Radim Briš

Applikační sféra, případně technologické sektory

Název komise	*Vedení komise*
1. Aeronautics and Aerospace	Darren Prescott
2. Chemical and Process Industry	Valerio Cozzani, G. Landucci, N. Khakzad
3. Civil Engineering	Raphael Steenbergen
4. Critical Infrastructures	Giovanni Sansavini, Enrico Zio
5. Energy	Michalis Christou
6. Information Technology and Telecommunications	Elena Zaitseva, Ralf Mock
7. Land Transportation	Olga Fink, Bob Huisman
8. Manufacturing	Benoit Iung, François Peres
9. Maritime and Offshore technology	Jin Wang, Ingrid B. Utne, Mario Brito
10. Natural Hazards	Pieter van Gelder, Bas Kolen
11. Nuclear Industry	Sebastian Martorell, Francesco Di Maio
12. Occupational Safety	Ben Ale, Reniers Genserik
13. Security	Sissel H. Jore, Zdeněk Vintr, Genserik Reniers

Závěr

V oblasti výzkumu a aplikací metodologie technické bezpečnosti, spolehlivosti a rizik se Česká republika za posledních 25 let výrazně zviditelnila v rámci Evropy. Svědčí o tom nejen členství špičkových českých vzdělávacích institucí v organizaci ESRA, ale i působnost zástupců těchto institucí ve vedení ESRA, či vedení technických komisí ESRA. Za jeden z největších úspěchů za celé období pak lze považovat vítězství ČR ve výběrovém řízení ESRA pro uspořádání největší evropské konference (asi 400 účastníků) v této oblasti v Praze, která úspěšně proběhla v roce 2009.

Tradice a současnost konferencí ESREL

prof. Ing. Zdeněk Vintr, CSc., dr.h.c.

Fakulta vojenských technologií, Univerzita obrany, Brno

zdenek.vintr@unob.cz

1 Úvod

Patrně nevýznamnější odbornou konferencí v oblasti spolehlivosti a bezpečnosti, která se koná v Evropě, je konference ESREL – European Safety and Reliability Conference. Tuto konferenci každoročně pořádá Evropská asociace pro spolehlivost a bezpečnost – ESRA (Europian Reliability and Safety Association) [1,2]. Konference se pravidelně zúčastňuje celá řada odborníků z České republiky a nezanedbatelná je i jejich role v přípravě a organizaci konference.

Cílem tohoto příspěvku je seznámit čtenáře s historii konference, jejím zaměřením a zásadami uplatňovanými při přípravě a organizaci konference. V článku je také charakterizován podíl zástupců ČR na rozvoji konference a blíže je také představena konference ESREL 2018, která se konala v Norském Trondheimu.

2 Historie konferencí ESREL

Konference ESREL jsou pod tímto názvem pravidelně pořádány od roku 1992, avšak již v roce 1991proběhla ve Velké Británii mezinárodní RELB, která se díky získaným ohlasům a zkušenostem stala základním impulzem pro vytvoření konceptu konferencí ESREL. Zpočátku byly konference organizovány volným sdružením organizátorů, ale v roce 1993 byla oficiálně založena ESRA, jejímž hlavním cílem v té době bylo právě pravidelné organizování konference ESREL.

Zpočátku měla konference ryze evropský charakter a účastnili se jí téměř výhradně odborníci ze zemí západní Evropy. Teprve koncem 90. let minulého století konferenci „objevili“ zástupci zemí bývalého východního bloku a začali se jí nedříve zúčastňovat a později i aktivně zapojovat do přípravy a organizace konference. Určitý průlom z tohoto pohledu představovala konference v roce 2005, která se konala v Polsku. Od té doby se na území bývalých socialistických zemí konaly již tři další konference (2009 – Praha, 2014 – Wroclaw, 2017 Portorož).

Dnes již má konference globální charaktera a běžně se jí účastní mnoho odborníků z Asie, Severní i Jižní Ameriky, Afriky i Austrálie. V poslední době je dokonce v rámci ESRA vedena diskuse o možnosti konání konference jinde než v Evropě. Zcela jednoznačně se tak dnes konference ESREL řadí k nejvýznamnějším odborným setkáním v oblasti spolehlivosti a bezpečností na globální úrovni.

Význam konference také prohloubila spolupráce ESRA s Mezinárodní asociací pro pravděpodobnostní hodnocení a řízení bezpečnosti – IAPSAM (International Association for Probabilistic Safety Assessment and Management) [3]. Tato mezinárodní organizace s globální působností organizuje každé 2 roky konferenci PSAM (International Conference on Probabilistic Safety Assessment and Management) a vždy, když se tako konference koná v Evropě, je pořádána společně s konferencí ESREL. Bylo tomu tak v létech 1996 (Kréta), 2004 (Berlín) a 2012 (Helsinki) a bude tomu tak v roce 2020 (Benátky).

Tab. 1: Přehled míst konání konference ESREL

Rok	Místo konání	Rok	Místo konání
1991	Velká Británie	2006	Portugalsko, Estoril
1992	Dánsko, Lyngby	2007	Norsko Stavanger
1993	Německo, Munich	2008	Španělsko, Valenci
1994	Francie, La Baule	2009	Česká republika, Praha
1995	Velká Británie, Bournemouth	2010	Řecko Rhodos
1996	Řecko, Kréta	2011	Franci, Troyes
1997	Portugalsko, Lisbon	2012	Finsko, Helsinki
1998	Norsko, Trondheim	2013	Nizozemí, Amsterdam
1999	Německo, Munich-Garching	2014	Polsko, Wroclaw
2000	Velká Británie, Edinburgh	2015	Švýcarsko, Zurich
2001	Itálie, Torino	2016	Velká Británie, Glasgow
2002	Francie, Lyon	2017	Slovinsko, Portorož
2003	Nizozemí, Maastricht	2018	Norsko, Trondheim
2004	Německo, Berlín	2019	Německo, Hannover
2005	Polsko, Tri City	2020	Itálie, Benátky

3 Základní principy organizace konferencí ESREL

Místo konání konference a hlavní organizátor konference se vybírá vždy na generálním shromáždění ESRA dva roky předem. Pokud se přihlásí více zájemců o uspořádání konference, výběr probíhá v rámci tajné volby. Tak například v loňském roce neuspěla Žilinská univerzita v souboji s Leibniz University Hannover o pořádání konference v roce 2019.

Existuje podrobný manuál, který organizátorům přesně vymezuje to, jakým způsobem má být konference připravena a organizována. Vedení ESRA na průběh přípravy dohlíží a do řídících orgánů konference deleguje vlastní zástupce. Na recenzním řízení u zaslaných příspěvků se standardně podílí členové technických komisí ESRA.

Pro přípravu a řízení konference se obvykle ustanovuje předseda (zástupce pořádající organizace) a spolupředsedající (zástupce ESRA), programový výbor (zpravidla členové technických komisí ESRA) a organizační výbor (zástupci pořádající organizace).

Konference je vždy organizována jako čtyřdenní (pondělí – čtvrtek). Tradičně se však koná recepce na uvítanou den předem (v neděli večer). Další pravidelnou společenskou akcí je slavnostní konferenční večeře (zpravidla středa). Pravidelně v rámci konference také probíhá generální shromáždění generální shromáždění ESRA (hodnocení činnosti, volby funkcionářů, výběr organizátorů budoucích konferencí …) a v závěru konference plenární zasedání ESRA (zhodnocení konference, představení organizátora a místa konání příští konference).

Výběr příspěvků pro zařazení do sborníku a prezentaci na konferenci probíhá ve dvou kolech. V prvním kole jsou posuzovány zaslané abstrakty (termín odevzdání obvykle 10 měsíců před konáním konference). Ve druhém kole jsou posuzovány vlastní příspěvky (termín odevzdání článků cca 6 měsíců před konferencí). Termín pro odevzdání konečných verzí příspěvků (upravených dle požadavků recenzentů) je cca 4 měsíce před konáním konference. Recenzi zpravidla provádí nejméně dva recenzenti.

Přijaté články jsou zařazeny do sborníku konference, který v posledních létech obsahuje obvykle 350 – 450 článků. Původně byl sborník vydáván pouze v tištěné formě (2 – 3 díly), později v tištěné a elektronické podobě a v posledních létech je v tištěné podobě vydáván pouze sborník abstraktů a vlastní sborník je vydáván pouze v elektronické podobě. V letošním roce byl poprvé sborník vydán s otevřeným přístupem (open access).

Výše vložného je závislá ne místě konání konference a pohybuje se obvykle ve výši 600 – 800 EUR. Členové ESRA mají slevu (cca 10%) a studenti taktéž (40-50%). Ušetřit lze také včasnou úhradou vložného (early bird). Ve vložném je, mimo jiné, zahrnuta také účast na recepci, slavnostní večeři a obědy. Počet článků pro jednoho účastníka není omezen. Vždy je však požadováno, aby alespoň jeden z autorů článku vložné uhradil a konference se zúčastnil.

Každý den je jednání konference zpravidla zahájeno plenární přednáškou nějakého pozvaného význačného odborníka. Poté následuje jednání v sekcích. Paralelně je organizováno až 10 odborných sekcí, jejichž zaměření navazuje na zaměření jednotlivých technických komisí ESRA [1,2]. Jednání v sekcích je rozděleno do bloků po 4-5 příspěvcích, přičemž pro každý příspěvek je vyhrazeno 20 minut. Důsledně se dbá na dodržování časového harmonogramu tak, aby účastnici mohli přecházet mezi jednotlivými sekcemi a vyslechnout ty příspěvky, které je zajímají. Jednání v sekci vždy řídí pověřená osoba (zpravidla členové technických komisí)

Kromě standardních odborných sekcí bývají do programu zařazovány i další typy setkání, jakou jsou kulaté stoly, průmyslová setkaní, workshopy apod.

4 Aktivity zástupců ČR v rámci konferencí ESREL

První účastníci z ČR se na konferenci ESREL začali objevovat až koncem 90 letech minulého století a po dlouhá letá se jednalo jen o pár jednotlivců. Jisty zlom představuje až ESREL v roce 2005, kdy se na konferenci objevila přece jenom početnější skupinka účastníků z ČR a ve sborníku bylo publikováno celkem 9 příspěvků autorů z ČR. Velmi důležitým krokem však bylo především to, že přes kontakty na polské kolegy se poprvé do technického výboru konference prosadili lidé z ČR.

V následujících létech potom aktivy ČR postupně narůstaly. Velmi významného úspěchu ČR dosáhla tím, že přípravou konference v roce 2009 byla, díky aktivitě prof. Ing. Radima Briše, CSc., pověřena VŠB-TU v Ostravě. Konference ESREL v Praze je prozatím nejvýznamnějším úspěchem ČR v rámci konferencí ESREL. Její konání se stalo počátkem velmi aktívního

zapojování odborníků z ČR do aktivit souvisejících touto konferencí. V tabulce č. 2 jsou uvedeny některé faktické informace o zapojení ČR u vybraných konferencí ESREL.

Souhrnně lze konstatovat, že dnes si nelze konferencí ESREL, bez rozsáhlé účasti odborníků z ČR a bez jejich podílu na přípravě a organizaci konference, představit. Je to nezpochybnitelný důkaz vysoké úrovně odborné a vědecké činnosti, která je v oblasti spolehlivosti a bezpečnosti v ČR realizována.

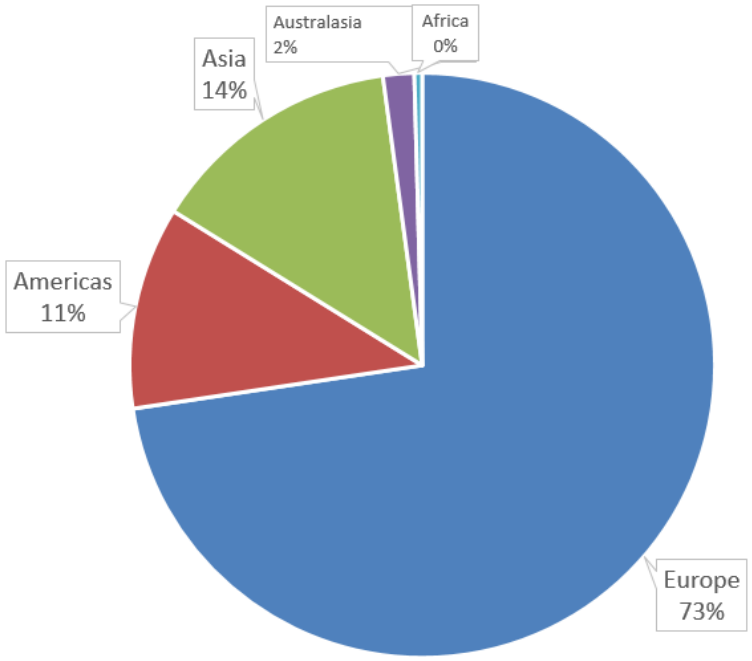
Tab. 2: Přehled o aktivitách odborníku z ČR na vybraných konferencích ESREL

Rok	Místo	Počet článků ve sborníku	Články autorů z ČR	Podíl článků	Podíl ČR na řízení konference
2000	Edinburg	228	2	0,9 %	-
2001	Torino	244	2	0,8 %	-
2003	Maastricht	234	2	0,8 %	-
2005	Tri City	287	9	3,1 %	4
2006	Estoril	371	11	2,9 %	2
2009	Praha	324	40	12,3 %	6
2010	Rhodos	335	27	8 %	1
2014	Wroclav	315	22	6,9 %	12
2016	Glasgow	420	26	6,2 %	1
2017	Portorož	455	34	7,5 %	5
2018	Trondheim	392	16	4 %	6

5 Konference ESREL 2018

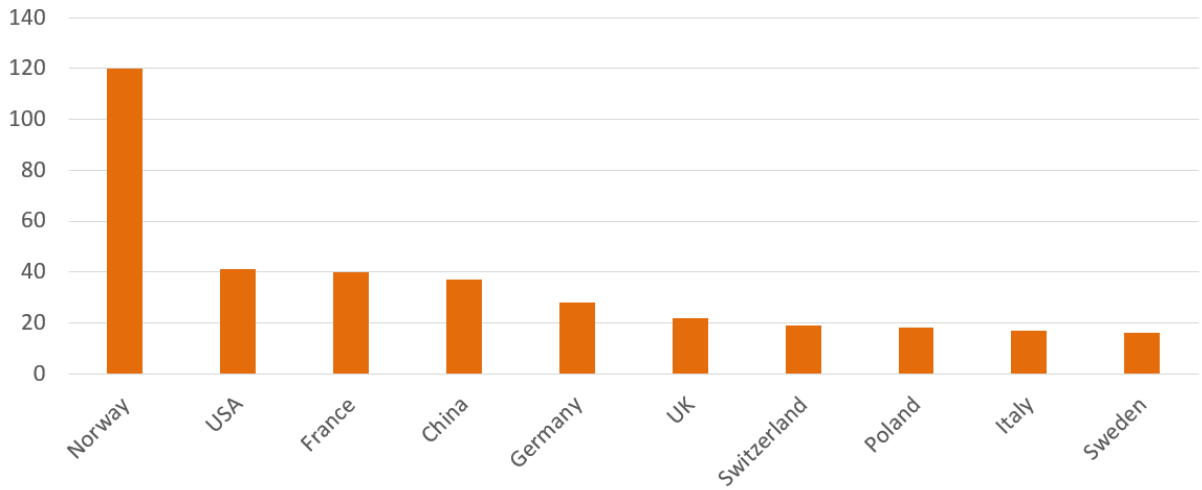
V letošním roce se konference ESREL konala v době od 17. do 21. června v Norském Trondheimu. Hlavním organizátorem byla Norská univerzita vědy a technologií – NTNU. V pořadí se jednalo již o 29. konferenci ESREL a třetí, která se konala v Norsku. Motem konference bylo „Safe Societies in a Changing World“.

Konference se zúčastnilo zhruba 400 účastníků ze 43 zemí světa. Na obr. 1 je znázorněn podíl účastníků z jednotlivých světadílů, který dokazuje, že ESREL není jen evropskou záležitosti, ale má skutečně globální rozměr.



Obr. 1: Zastoupení účastníků konference z jednotlivých světadílů

Nejpočetněji zastoupené země jsou uvedeny v obr. 2, ze kterého je také patrné, že jako obvykle byla nejpočetněji zastoupena pořádající země. Mezi deseti zeměmi s největší účastí chybí Česká republika, ze které bylo přítomno jen 10 účastníků. Rozhodně se však nejedná o zastoupení nevýrazné. To vyplývá z obr. 3, kde je počet účastníků vztažen k počtu obyvatel dané země. Z tohoto pohledu již ČR patří mezi nejaktivnější země.

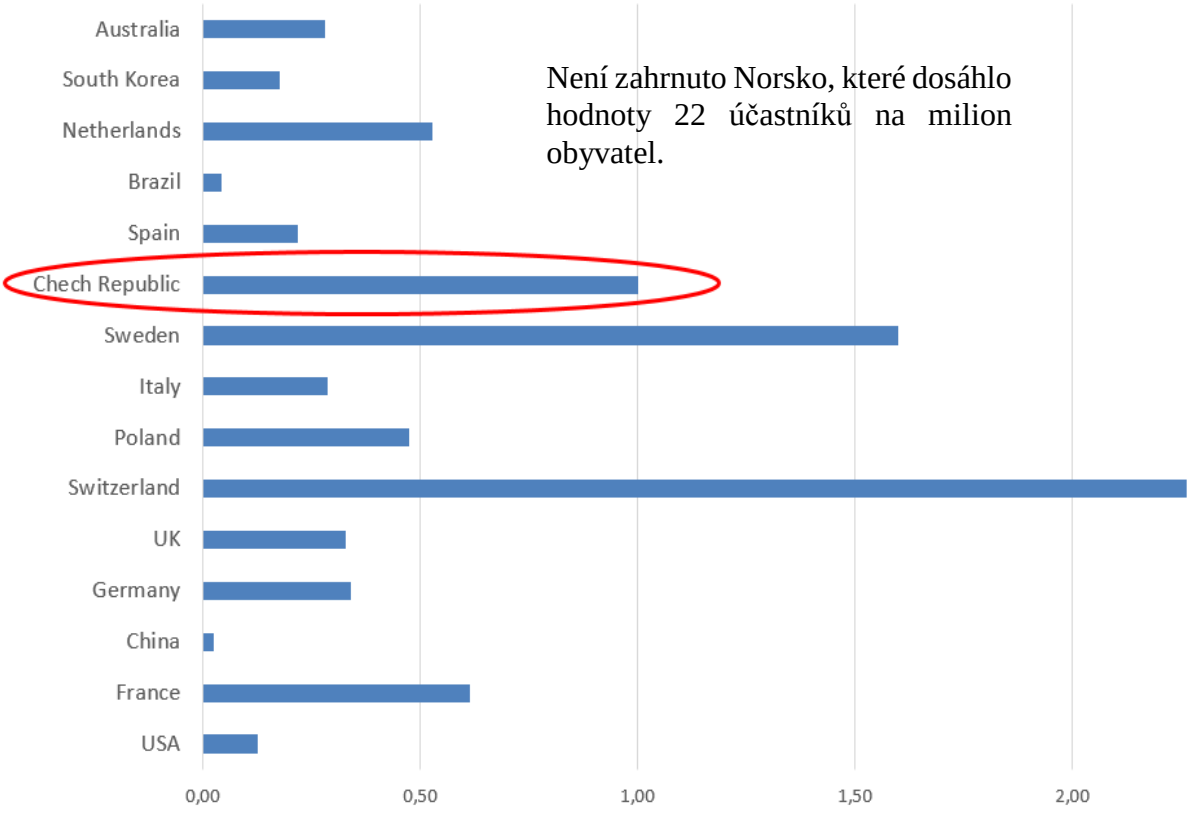


Obr. 2: Přehled zemí s nevyšším zastoupením na konferenci

Ve sborníku konference bylo zveřejněno celkem 392 příspěvků. Úplný sborník byl vydán pouze v elektronické podobě a je volně přístupný na Internetu v režimu Open Access [4]. Tematicky se konference jako obvykle věnovala širokému okruhu metodologických i aplikačních oblastí

spolehlivosti a bezpečnosti se zaměřením především na oblasti zahrnuté v následujícím přehledu:

- foundations of risk and reliability assessment and management,
- mathematical methods in reliability and safety,
- risk assessment,
- risk management,
- system reliability,
- uncertainty analysis,
- digitalization and big data,
- prognostics and system health management,
- occupational safety,
- accident and incident modeling,
- maintenance modeling and applications,
- simulation for safety and reliability analysis,
- dynamic risk and barrier management,
- organizational factors and safety culture,
- human factors and human reliability,
- resilience engineering,
- structural reliability,
- natural hazards,
- security,
- economic analysis in risk management.



Obr. 3: Počet účastníků vztažený na milion obyvatel dané země

V rámci konference proběhly čtyři plenární přednášky:

- Thon, R. (Norwegian National Security Authority): Cybersecurity – The Human Factor,
- Mosleh, A. (NTNU): Ask The Expert,
- Hudson, P. (Elft University of Technology): Redefining Risk And Safety – A Multi-Dimensional Approach,
- Mannan, M. S. (Mary Kay O'connor Process Safety Center): Perspectives on Ocean Energy Safety.

Byly zorganizovány dvě průmyslová setkání (Industry Sessions):

- Major accident collision risk management of DynPos (DP) marine operation,,
- Industry challenges for railway safety and reliability.

Proběhly také dva worshopy zorganizované sponzory konference:

- Aviation Academy: How much is your system capable of avoiding safety risk events? The SAREAC indicator,
- BQR Reliability Engineering Ltd & AEGIS Engineering Systems Ltd.: Cross domain safety standards overview with a practical RAMS lifecycle activities example.

Další informace o průběhu konference, včetně podrobného programu konference, sborníku abstraktů i celý sborník příspěvků lze nalézt na webových stránkách konference [5].

6 Závěr

Celkově lze konstatovat, že konference ESREL jsou dnes globálně respektovaná mezinárodní setkání expertů z oblasti bezpečnosti a spolehlivosti a každý odborník zajímající se o tuto problematiku by se o účast na konferenci, respektive o její výsledky (sborník) měl zajímat. Za pozitivní lze považovat, že se do přípravy, organizace a vlastního průběhu konference pravidelně zapojuje řada zástupců ČR.

Použité zdroje

[1] Briš, R. ESRA-Evropská asociace pro bezpečnost a spolehlivost. In *Aktivity ČR v rámci European Safety and Reliabitily Assocation – Materiály ze 73. semináře Odborné skupiny pro spolehlivost*. Praha ČSJ, 2018

[2] Europian Reliability and Safety Association. http://esrahomepage.eu/

[3] International Association for Probabilistic Safety Assessment and Management. https://www.iapsam.org/

[4] Haugen, S., Barros, A., Gulijk, C., Kongsvik, T., Vinnem, J. E. (Eds.) *Safety and Reliability – Safe Societies in a Changing World. Proceedings of ESREL 2018.* London: CRC Press, 2018. Dostupné na https://www.taylorfrancis.com/books/e/9781351174657

[5] ESREL 2018 – European Safety and Reliability Conference Trondheim, Norway, 17-21 June 2018. https://www.ntnu.edu/esrel2018

Informační výkon pro bezpečnost drážních systémů

Ing. Tomáš Kertis, doc. RNDr. Dana Procházková, DrSc.

Fakulta dopravní, České vysoké učení technické v Praze

kertitom@fd.cvut.cz

1 Úvod

Dnešní společnost je závislá na technických a kybernetických systémech, které přispívají k uspokojení základních potřeb lidí. Systémy potřebují pro svoji správnou funkci správné a včasné informace z reálného fyzického prostředí. Proto jsou informační a komunikační systémy používané k vytváření spojení mezi různými druhy systémů, protože v souladu s danými pravidly dokáží zpracovat informace rychleji než člověk.

Čím větší je úsilí lidí ke zlepšení a usměrnění procesů k jejich vyššímu ekonomickému užitku, tím je vyšší závislost lidské společnosti na informačních technologiích, a proto neustále vzrůstá potřeba vývoje uvedených technologií. Zlepšováním a usměrňováním procesů ve směru k ekonomickému užitku, zavádíme stále nová spojení, tj. vazby, a tím vytváříme systémy stále komplexnější, a tím i zranitelnější. Zranitelnosti vedou k selhání systémů v kritických podmínkách, které mají v mnoha případech dopady na bezpečí lidí, zajištění základních lidských potřeb a hlavních funkcí států. Proto také v oblasti informačních technologií hovoříme o kritické informační infrastruktuře, která je navíc propojena s ostatními technologiemi. Propojením uvedených elementů vznikají kritické kyber-fyzické systémy.

Pro zajištění bezpečí lidí potřebujeme zajistit zabezpečení a v mnoha případech také bezpečnostní kyber-fyzické systémy. K formování příslušných principů pro zajištění zabezpečeného a bezpečného kybernetického systému je zapotřebí použít teorii informací a konkrétně odvodit parametry, které ovlivňují informační výkon. Informační výkon je právě ta veličina, jejíž rozměr ovlivňuje kvalitu rozhodnutí, tj. čím vyšší je informační výkon, tím je vyšší pravděpodobnost správného rozhodnutí a naopak.

Dopravní infrastruktura a drážní systémy jsou komplexními systémy systémů, a svou povahou kyber-fyzickými systémy, které jsou závislé na informačních technologiích, ve kterých je řada zranitelností, které mohou vést k závažným dopravním nehodám. Proto předložená práce předkládá vybranou část teorie informace relevantní k informačnímu výkonu. Dále analyzuje dva příklady železničních nehod a na nich demonstruje význam informačního výkonu. Výsledkem práce je návrh kritérií, která určují informační výkon pro různá místa drážního kyber-fyzického systému.

2 Vliv informačních technologií na bezpečnost drážních systémů

Úroveň bezpečnosti na drahách ovlivňujeme zlepšováním jejích kvalitativních parametrů, jako je například přepravní rychlost, kapacita a množství přepraveného zboží a lidí, parametry RAM (bezporuchovost, dostupnost, udržovatelnost), LCC (náklady životního cyklu), interoperabilita. V některých případech kvalitativní parametry bezpečnost zlepšují, především tam, kde je bezpečnost závislá na bezporuchovosti a dostupnosti určité funkce. V ostatních případech jsou kvalitativní parametry v rozporu s bezpečností, například pokud zvyšujeme provozní rychlost a zkracujeme intervaly mezi vlaky s přepravou velkého počtu pasažérů, tak to vede k vyššímu nebezpečí s ohledem na lidi. Drážní bezpečnost má dlouhou tradici ve smyslu technologií, ale

stále je zde prostor pro zlepšení z hlediska zajištění bezpečí lidí (ang. Human security). Úroveň bezpečnosti je vždy limitována provozními podmínkami, ve kterých je systém provozován: jestliže jsou podmínky velmi odlišné od těch, na které byl systém navržen, anebo jsou překročeny jisté limity, systém se dostane do nebezpečného stavu, tj. do stavu, ve kterém ohrožuje sám sebe i své okolí, tj. okolní systémy, životní prostředí, ekonomické vazby, životy a zdraví lidí a další [1-3]. Bezpečnost drážního systému znamená, že drážní systém je schopen pracovat perfektně v širokém spektru podmínek. Jestliže je uvedený rozsah překročen, systém musí rozpoznat změny v podmínkách a musí přejít do jiného stavu řízení bezpečnosti, např. aplikovat opatření a aktivity v souladu s plány bezpečnosti, kontinuity aj. V současnosti je kladen velký důraz na vývoj zabezpečených drážních systémů [4, 24-26], a proto nároky jsou zaměřené především na bezpečnost technologické platformy, která je pro bezpečnost celku velmi důležitá, ale neřeší komplexní problémy (ve smyslu složité), tj. bezpečí lidí. Integrální bezpečnost zaměřená na bezpečí lidí je stále v praxi přehlížená. Množství investic do oblasti bezpečnosti a zabezpečení je totiž velmi zatíženo ekonomickými aspekty [5-8].

Informační systémy založené na informačních technologiích jsou implementované ve všech výše zmíněných oblastech, tj. zajištění kvality drážní dopravy, zabezpečení a bezpečnost drážních systémů. Informační technologie interpretují, pomáhají zvládat, anebo v případě automatizovaného provozu také řídit všechny uvedené kvalitativní a bezpečnostní parametry. Informační systémy a technologie jsou integrální částí drážního systému. Tabulka 1 ukazuje příklady, jak jsou informační systémy použité v různých oblastech drážní dopravy. Správné nastavení parametrů informačních systémů zajišťuje velikost jejich informačního výkonu, tj. kvalitu informace, která umožňuje systému efektivně reagovat na nepřijatelné podmínky. Tímto způsobem zlepšují bezpečnost drážních systémů, a to nejen za normálních, ale také za abnormálních a především kritických podmínek.

Tabulka 1. Příklady využití informačních systémů na drahách.

Řízení a plánování (management)	• vyhodnocování dat z provozu • tvorba jízdních řádů • rozpis služeb zaměstnanců • rozhodovací, ekonomické, účetní činnosti • komunikace se záchrannými složkami a s policií
Řízení provozu	• centrální dohledu a řízení, dispečerské činnosti • staniční a traťové technologie • sběr a zpracování dat na trase vlaků • komunikace mezi stacionárními a vlakovými systémy • zabezpečovací zařízení
Provoz vlaku	• řízení vlaku, vlakový počítač • datové přenosy mezi vlakovými zařízeními • sledování a řízení vlakových zařízení (dveře, klimatizace, vlakový rozhlas, energetická zařízení) • rozhraní technika – strojvedoucí
Cestující	• informační tabule • systémy odbavení cestujících • zábavná zařízení ve vlaku, Wi-Fi • navigační systémy – směrové tabule • navigační systémy pro hendikepované

3 Informační systémy a technologie, proces vzniku informace a zabezpečení informací

Níže uvedená teorie je založena na znalosti v oblasti informačních systémů, kyber-fyzických systémů, komplexních systémů a kritické infrastruktury [2,3,9-12].
Informace, informační systémy a technologie zahrnují velmi širokou oblast, která vytváří spojení mezi systémy. Informace jsou dnes vedle materiálních, energetických a finančních zdrojů řazeny k základním faktorům, které určují pokrok, a to nejen technologický, ale také pokrok v ostatních oblastech lidských aktivit. Informační toky v systémech vytváří důležitá spojení a spřažení elementů a celých systémů v komplexních technologických objektech. Bez jisté úrovně informace není možné vytvářet ani spravovat procesy v technických dílech a v lidské společnosti. Vznik informace je podmíněn sledováním jistých vlastností pozorovaného objektu nebo společných vlastností skupiny objektů. Každý informační systém sleduje vlastnosti entit použitím určitého jazyka, což slouží k vytvoření informace o pozorovaném objektu. Podle způsobu interpretace takto získaných informací se rozlišují typy informačních systémů: syntaktické informační systémy, které vytváří množinu informačních obrazů stavových veličin pozorovaného objektu; a procesní informační systémy, které reprezentují množinu procesů. Akční informační systémy pak zpětnou vazbou ovlivňují původní pozorovaný objekt, nebo vytváří model či další reálný objekt. V oblasti řízení provozu drah jsou aplikované především akční procesní informační systémy, proto se na ně dále předložená práce zaměřuje. Proces vzniku informace, informačního systému, proces vzniku nového objektu nebo modifikace objektu původního je složen z následujících podprocesů, respektive množiny vazeb a jejich relací, které jsou popsané tabulkou 2.

Tabulka 2. Proces vzniku informace a informační technologie.

	Podproces vzniku / množiny objektů	**Dotčené abstr. uzly**	**Použité inf. technologie**	**Vstupy procesu**	**Výstupy procesu**
1	Identifikace objektu	Objekt, pozorovatel	Fyzické receptory (senzory, čidla)	Pozorované stavové (fyzické) veličiny objektu	Signály
2	Pozorování	Pozorovatel, jazyk (syntaxe)	Vzorkování, kvantování, kódování/dekódování	Signály	Data
3	Komunikace mezi zdrojem a příjemcem zprávy	Jazyk (pozorovatele, resp. systému sběru dat), příjemce zprávy	Telekomunikační, přenosové a sdělovací systémy	Data	Data
4	Interpretační množina, vznik informace	Jazyk (pozorovatele, resp. systému sběru dat, nebo příjemce), množina informací (viz 6)	Ontologie, jazyk	Data	Informace
5	Vazby funkcí a strukturálního uspořádání objektu, ověření celistvosti (integrity)	Informace (viz 6), objekt	Akční člen systému, akční informační systém	Objektu, informace	Správnost informace, změna objektu
6	Množina informací v množině informačních systémů	Informační systémy	Informační systémy	Informace	Informace

7	Proces interpretace	Informace (viz 6), nový objekt	Signalizace a technologie reprezentace informace, umělá inteligence	Informace	Obraz objektu, nový objekt

Kvalitativní vlastnosti informačních systémů a technologií lze ovlivňovat vhodným nastavením jejich parametrů, kterými jsou např.: kvalita procesu vytvářející informační obrazy (na základě Fregeho konceptu); množství informace (viz vzorec 1); parametry přenosové matice (viz vzorec (4)). Uvedené parametry ovlivňují informační výkon (vzorce 5 a 6), a proto také schopnost rychlého a správného rozhodnutí informačního systému (vzorec 7). Fregeho funkční koncept vzniku informačního obrazu [11,12], který je složen z množin: $\boldsymbol{O_i}$ – množina stavových veličin na objektu; $\boldsymbol{P_i}$ – množina stavů (pozorovatelů); $\boldsymbol{\Phi_i}$ – množina syntaktických řetězců (tok dat); $\boldsymbol{I_i}$ – množiny informačních obrazů stavových veličin.
Vazby předmětných množin, které určují kvalitu v procesu vzniku informačního obrazu, jsou v souladu s [9] popsané následujícími parametry:

- $\boldsymbol{a_{OP}}$ – identifikace,
- $\boldsymbol{a_{PO}}$ – invazita (nebezpečí ztráty integrity stavových proměnných na pozorovaném objektu),
- $\boldsymbol{a_{P\Phi}}$ – projekce v množině symbolů a syntaktických řetězců,
- $\boldsymbol{a_{\Phi P}}$ – korekce a identifikace neurčitelnosti,
- $\boldsymbol{a_{\Phi I}}$ – interpretace, vznik informace,
- $\boldsymbol{a_{I\Phi}}$ – reflexe jazykových konstruktů,
- $\boldsymbol{a_{IO}}$ – relace funkčních a strukturální uspořádání,
- $\boldsymbol{a_{OI}}$ – verifikace integrity.

Míra informace je nejčastěji charakterizována Hartleyovou mírou informace pro binární systém symbolů (tj. pro většinu současných kyber-fyzických systémů). Vyjadřujeme ji vztahem:

$$I = \frac{1}{ln(2)} \cdot ln(N) \,, \tag{1}$$

ve kterém $\boldsymbol{N}$ reprezentuje počet možných zpráv (údajů):

$$N = S^n \,, \tag{2}$$

ve kterém $\boldsymbol{S}$ je počet znaků v abecedě $\underline{A}(A_1,A_2,...A_S)$ a $\boldsymbol{n}$ je počet prvků v množině znaků.
Procesní informační systémy charakterizujeme grafy přiřazenými relacím:

$$I_i \sim F[P(t), \Phi(t)]. \tag{3}$$

Předmětné přiřazení umožňuje strukturální interpretaci složitých informačních systémů, hodnocení zpětných vazeb a kvalitu převozu a zpracování informace v dílčích informačních systémech a jeho informační segment vychází z maticového vyjádření:

$$\underbrace{\begin{pmatrix} I_2 \\ \Phi_2 \end{pmatrix} \approx \begin{pmatrix} t_a t_b \\ t_c t_d \end{pmatrix} \cdot \begin{pmatrix} I_1 \\ \Phi_1 \end{pmatrix}}_{[\hat{T}_i]}, \tag{4}$$

ve kterém T_i je přenosová matice i-tého informačního segmentu (tj. segmentu informačního výkonu). V reálném systému ze vztahu (3) vyplývá, že informace nebo množina informací I_i je propojena s množinou stavů sytému a informačních toků v čase. Informační segment ze vztahu (4) můžeme přiřadit například systému sběru dat, kde I_1 jsou vstupní (počáteční) informace, ϕ_1 vstupní informační tok a na druhé straně na výstupu daného systému I_2 jako vstupní informace a přenesený informační tok ϕ_2. Parametry t lze získat jak kvantitativní tak i kvalitativním způsobem a v předmětném příkladu představují:

- t_a – schopnost interpretace (pro $t_a < 1$ má systém velmi malou znalost a schopnost interpretace, pro $t_a = 1$ má schopnost interpretace vlastností objektu v informačním systému, pro $t_a > 1$ se jedná o expertní systém se schopností reprezentace vlastních informací o objektu na základě získaných údajů a dat),
- t_b – schopnost filtrace (v případě $t_b < 1$ systém na svém výstupu interpretuje menší množství informací, než které získá na jeho vstupním informačním toku, pro $t_b > 1$ naopak),
- t_c – komunikativnost (schopnost poskytnout výstupní informační tok na základě vstupních informací),
- t_d – propustnost informačního systému (schopnost převést vstupní informační tok na jeho výstupní informační tok, v případě redundance je t_d mnohem větší než 1).

Kvalitativní parametry systémů systémů (tj. také drážních systémů), které ovlivňují bezpečí lidí, jsou: bezpečnost; integrita; bezporuchovost; kvalita; pohotovost; kontinuita; přesnost, a jsou přímo závislé na efektivnosti informačních systémů. Informační systémy totiž zajišťují požadovanou správnost a včasnost informace a v případě akčních informačních systémů také rychlost správného rozhodnutí. Úroveň efektivnosti informačního systému se vyjadřuje pomocí veličiny ***informačního výkonu:***

$$P_i(t) = I_i(t) \cdot \Phi_i(t), \quad (5)$$

kde $P_i(t)$ je okamžitý informační výkon. Informační výkon je také roven velikosti míry odstranění nejistoty E znalosti (tj. z fyziky množství práce) na jednotku času t:

$$P = I \cdot \Phi = \frac{E}{t}. \quad (6)$$

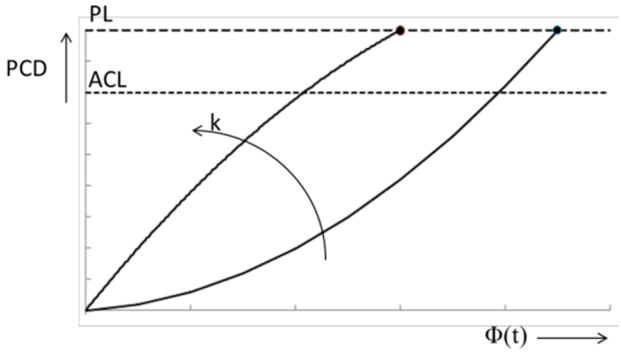
Pro zajištění bezpečnosti řídicích systému na drahách je proto důležité provozovat takové informační systémy, které poskytují co nejrychleji správné rozhodnutí, což úzce souvisí s informačním výkonem. Pravděpodobnost správného výběru variantního řešení z množiny řešení a pravděpodobnost správného rozhodnutí v provozu řídicího systému, tj. PCD (Probability of Proper Decision), je dána funkcí závislé na úrovně znalosti funkce „k“ a informačního toku v čase „$\Phi(t)$“ [11, 12]:

$$PCD = F[\Phi(t), k]. \quad (7)$$

Předmětný vztah je znázorněn na Obrázku 1, kde PL je maximální a ACL je akceptovatelná úroveň PCD.

Z uvedeného vyplývá, že řídicí systémy, které se opírají o vyšší úroveň znalostí, jsou schopné zajistit rychleji správné rozhodnutí při menší zátěži. Každý systém pracuje správně pouze za jistých předpokladů, tj. okolních podmínek. Proto musí mít kyber-fyzické systémy stanovené jisté limity a podmínky, které podmiňují jejich kvalitativní parametry; a mechanismy, které reagují na okolní podmínky systému. Pro velmi rozdílné podmínky musí mít připravené plány pro přechod na jiné aktivity, tj. provozní pravidla pro abnormální a kritické podmínky, které mohou nastat v případě výskytu pohromy. Navíc musí mít zajištěné plány pro případ, pokud okolní stav systému stanovené podmínky překročí, tj. pro kritické podmínky v případě výskytu

pohrom. Předmětnou problematikou se zabývají ***procesy zajištění informační bezpečnosti*** (přesněji zabezpečení, tj. anglicky security), které jsou založené na ochraně důležitých kybernetických aktiv způsobem, který pro důležité informace stanovuje požadovaný stupeň důvěrnosti, integrity a dostupnosti - CIA (anglicky Conifidentiality, Integrity and Availability).



Obr. 2: Pravděpodobnost správného rozhodnutí v provozu řídicích systémů [9].

4 Případové studie, společné kybernetické příčiny nehod

Pro zobrazení příčin dopravních nehod vlaků způsobených selháním kybernetické sítě uvedeme dva skutečné případy; první z České republiky a druhý ze Španělska.

4.1 Moravany 2008

Dne 19. května roku 2008 došlo ve 4 hodiny 48 minut na staniční koleji v Moravanech k závažné železniční nehodě, srážce nákladního vlaku s osobním vlakem s následným vykolejením.
Následkem nehody bylo jedno úmrtí, 4 lehce zranění a přímá finanční škoda 12 643 092,- Kč [13]. Zásadní příčinou byla ztráta kontaktu železničního vozidla na styku koleje s vozidlem. Zpráva z vyšetřování uvedené dopravní nehody uvádí následující bezprostřední příčiny: ztráta šuntu kolejového obvodu 1K žst. Moravany vlakem Os 5011; a nesprávná reakce staničního zabezpečovacího zařízení ESA 11 na neočekávanou změnu informace o volnosti 1. staniční koleje. Dalšími zásadními příčinami byly: nekompatibilita mezi drážními vozy a kolejovými obvody v oblasti izolujících emisí – pískování (pro zvýšení tření mezi koly a kolejnicí); dále vnitřní logika staničního zabezpečovacího zařízení ESA 11, konkrétně zpracování nové informace o volnosti koleje obdržené připojením výstroje kolejového obvodu po ukončení vysílání kódu traťovou částí vlakového zabezpečovače. Z hlediska systému řízení bezpečnosti zpráva uvádí [13]: provoz drážních vozidel nekompatibilních s kolejovými obvody bez odpovídajících bezpečnostních opatření.
Uvedená událost nebyla ojedinělá, zdroj [13] dále uvádí: „*29. srpna 2008 došlo v žst. Hulín k události se stejným pozadím, jako má mimořádná událost z 19. května 2008 v žst. Moravany. Po stejné závadě pískovacího zařízení hnacího drážního vozidla stejné řady stejného dopravce tam stejným postupem staničního zabezpečovacího zařízení stejného typu došlo v 17:46:55 hodin ke změně indikace stavu 3. staniční koleje na „volná“, ačkoliv byla stále obsazena stojícím osobním vlakem Os 4256. Tato událost se obešla bez následků jen díky příznivým okolnostem a reakci zúčastněných zaměstnanců.*“

Předmětná událost je ve smyslu společných kybernetických příčin [1] kombinací dvou příčin, a to zejména chybný SW a nedostatečný HW; porucha pískovacího zařízení, které bylo stále aktivní i po jeho vypnutí strojvedoucím – nedostatečná údržba (HW); použitím písku s větším zrnem došlo ke zkreslení informací zapříčiněné pískováním – organizační chyba (HW); indikace pískování strojvedoucímu nesignalizovala aktuální stav, pouze záměr, zda je vydán elektronický signál k pískování – nedostatečný návrh (SW/HW); signalizace obsazené koleje jako neobsazené – nedostatečný návrh (HW/SW); automatické nastavení cesty k obsazené koleji – nedostatečný design (HW/SW); absence systému vzdáleného zastavení vlaku – nedostatečný návrh (HW/SW); a nedostatečné komunikační zařízení (strojvedoucí nákladního vozu nereagoval na příkaz k zastavení) – nedostatečný návrh (HW) a organizační chyba.
Hlavní příčinou události je tedy fakt, že byla zkreslená informace jak kvůli pískování, tak také kvůli špatné reakci staničního zabezpečovacího zařízení, tj. chyba, která se vyskytla na rozhraní kybernetického a fyzického (kyber-fyzického) systému.

4.2 Santiago de Compostela 2013

Železniční nehoda v roce 2013 se stala několik kilometrů od španělské železniční stanice Santiago de Compostela, a byla nejhorší železniční nehodou ve Španělsku za posledních čtyřicet let. 24. července 2013 v 20 hodin 41 minut, v oblouku „Angrois“ vykolejil vysokorychlostní vlak osobní přepravy v rychlosti 179 km/h s předepsanou omezenou rychlostí 80 km/h. Po vykolejení většina vozů narazila na betonovou zeď vedoucí podél oblouku a došlo k požáru na hnacím vozidle. Následkem vykolejení vlaku bylo 80 mrtvých a 152 lidí zraněných, tj. téměř všichni pasažéři [14].
Příčinou nehody byla překročená rychlost vlaku a vyšetřovací komise v závěru obvinila strojvedoucího z nedbalosti a nedodržení drážních předpisů. Uvedené závěry vyšetřování, které jsou neveřejné, byly zpochybněny Evropskou Drážní Agenturou ERA. ERA ve svém dokumentu určenému EU [14] popisuje kořenové příčiny nehody, tj. odhalila také slabiny v celkovém řídicím systému drah. Stručně uvádíme závěry zprávy ERA [14] s připojenými poznámkami ze zkušeností z podobného vyšetřování nehod [14]:

1. Předmětem nehody byl vysokorychlostní vlak 150/151 řady Alvia Class 730, který je modifikací řady 130. Oba konce soupravy jsou vybaveny dieselovými motory (s naftovou nádrží). *Pozn.:* právě vylitá nafta je hlavní příčinou velkého požáru při železničních nehodách.
2. Souprava 150/151 byla složena z 13 vozů: dvou trakčních vozů doplněných motorovými vozy na každém konci; osmi vozů pro přepravu cestujících; a restauračního vozu. Hmotnost vlaku byla 382 tun. *Pozn.:* právě parametry vlaku mají přímý vliv na dopady a závažnost nehody.
3. Vlak byl vybaven dvěma zabezpečovacími zařízeními: ASFA Digital a ERTMS/ETCS. Kvůli poruchovosti a dostupnosti systému konfigurace ERTMS na předmětné trase byl provozovatelem schválen provoz s bodovým zabezpečovačem (BSL) ASFA Digital. *Pozn.*: právě neslučitelnost více systémů o různých stupních automatizace způsobuje narušení bezpečnosti a přispívá k vážným nehodám.
4. Předmětná trať je vybavena balízami (BSL), ERTMS/ETCS úrovně 1, s výjimkou jejího začátku a konce, a s podporou zabezpečovače ASFA Digital. *Pozn.*: právě přechod mezi různými řídicími systémy často vede ke zmatku zaměstnanců a k lidským chybám.
5. „Nízko-rychlostí“ oblouk (s maximální rychlostí 80 km/h) má navržený rádius 402 m a je umístěn na konci úseku tratě vybavené výhradní technologií ASFA Digital. *Pozn.*: ve sledovaný čas předmětný systém nepracoval s rychlostními limity a umožnil jízdu vlaku v nepřijatelné rychlosti, která zapříčinila vykolejení.

6. Podél oblouku je vybudována masivní betonová stěna. Maximální povolená rychlost 80km/h v daném úseku je označená tabulkou na dráze. *Pozn.*: takové tabulky nejsou v předmětných rychlostech příliš zřetelné, což přispívá k nehodě.
7. Signalizace a cesta pro vlak byly nastaveny v pozici indikující „volnou cestu“, tj. návěst „Volno“. *Pozn.*: právě nedostatky v automatickém řídicím systému, který umožňuje nesprávnou indikaci volnosti nebo obsazení tratě, příčinami nehod.
8. Značení změny rychlosti před obloukem na staničení (PK) 84+273 nebylo dostatečně výstražné. *Pozn*: tato zdánlivě maligní skutečnost je často příčinou dopravních nehod
9. Kabina strojvedoucího byla vybavena několika komunikačními systémy (tj. radiotelefon mezi vlakem a tratí, mobilní telefon (GSM-R)) pro podnikovou komunikaci v rámci vlaku a vně vlaku, uvedené systémy byly v provozu. *Pozn:* služební hovory a komunikace s dispečinkem spolu s dalšími úkoly řízení vlaků, zejména při změnách řídicích systémů, vedou k těžké pracovní zátěži strojvedoucích a přispívají k jejich chybám.
10. Jízdní řád v kabině pro strojvedoucího ukazoval změnu rychlosti: omezení rychlosti na 80 km/h na PK 84+230 (the Anrois curve). *Pozn.:* to je možná chyba strojvedoucího zapříčiněná přehlédnutím.
11. V souladu s pokyny měl strojvedoucí sám a včas zahájit brzdění a přizpůsobit rychlost, tj. z 200 km/h na 80 km/h, a to bez pomoci nějakých určitých technických systémů řízení. *Pozn.:* možné pochybení strojvedoucího.
12. V daném případě vlak měl 2-3 minuty zpoždění. *Pozn.*: v takových případech často zpoždění zvyšuje stres strojvedoucích, kteří se snaží o dodržení jízdního řádu.
13. Záznamy ukázaly, že asi 6 000 metrů před vjezdem do oblouku strojvedoucí reagoval na služební volání vlakového dispečera. Hovor trval 100 sekund. *Pozn.*: možná příčina přehlédnutí značky nabádající ke včasnému snížení rychlosti.
14. Technická analýza ukázala, že brzdy vlaku 150/151 nebyly dostatečně aktivovány pro dosažení požadovaného omezení rychlosti. *Pozn.*: to značí pozdní reakci strojvedoucího.

Závěr ERA konstatuje, že oficiální vyšetřování Komise pro vyšetřování železničních nehod ve Španělsku (CIAF - Comisión de Investigación de Accidentes Ferroviarios) nezvážilo při stanovení kořenové příčiny nehody všechna fakta, protože se opíralo o úzký pohled na věc, tj. strojvedoucí musí vždy reagovat kvalitně a nemůže se opírat o upozornění zabezpečovacích systémů, tj. musí ve správný čas brzděním upravit rychlost vlaku na požadovaných 80km/h [14].
Vyhodnocení dopravní nehody, které jsme provedli na základě závěrů ERA a poznámek k 14 oblastem na základě zkušeností z praxe [11,15], ukazuje, že k nehodě přispěla kombinace několika pochybení, a to především z důvodu složitosti (komplexnosti) systému řízení bezpečnosti provozu. Z hlediska kybernetických příčin dle [1] se jedná o: zkreslení dat z monitorování - kdy dle výpovědí strojvedoucího došlo k jeho zmatení o aktuální pozici; a nedostatečný HW - kde byla v nebezpečném úseku snížena úroveň zabezpečení, kvůli vypnutí zabezpečovacího zařízení ERTMS/ETCS úrovně 1, a tím nebyla kontrolovaná povolená traťová rychlost v daném úseku.

4.3 Společné kybernetické příčiny

Společné kybernetické příčiny jsou zřejmé z analýzy obou výše uvedených případů. Jedná se zejména o problémy na systémových rozhraních, které jsou navržené, implementované a provozované různými subjekty na různých úrovních jejich odpovědností. Jde o: problémy na rozhraní člověk – stroj; problémy na rozhraních systémů kyber-fyzických, problémy na rozhraních systémů socio-technických; stanovení odpovědností, a to nejenom mezi subjekty,

ale také mezi procesy systémů (vzájemná kompatibilita); problémy na rozhraních systémů s rozdílnou kritičností (stupně automatizace, úrovně zabezpečení, nebo úroveň integrity bezpečnosti).
Tyto problémy odpovídají nálezům z analýzy společných příčin železničních nehod v České republice [1], které jsou z hlediska kybernetiky: zkreslení dat z monitorování; chybný software, který nezvažuje všechny možné varianty provozních podmínek; a nedostatečně robustní hardware, který způsobí nesprávné nebo pomalé zpracování a vyhodnocování dat. V některých případech byly zaznamenané i hackerské útoky na řídící centrum dispečerského pracoviště.
Předmětnými společnými kořenovými kybernetickými příčinami jsou validita rozhodování systémů, tj. nízký informační výkon a míra informace v informačních systémech, tj. malé množství informace.

5 Metody konstrukce opatření zlepšující drážní bezpečnost

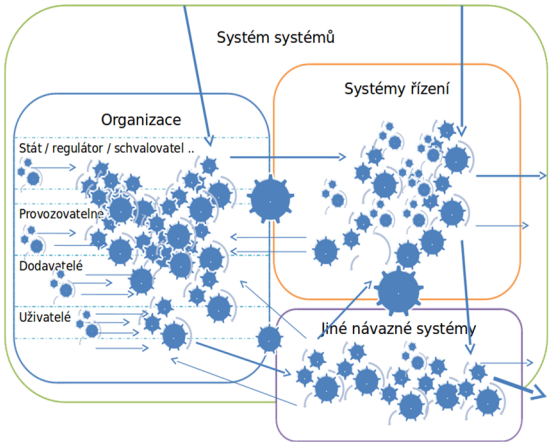
K dosažení co nejvyšší míry bezpečnosti drážního řídicího systému, tj. také informačního výkonu, musí všechny zúčastněné strany zavádět přístupy k řízení kvality TQM (z angličtiny Total Quality Management) [16], které berou v potaz integrální rizika. Uvedené přístupy musí být přizpůsobeny specifickým vlastnostem drážních systémů. Proto je nutné pro práci s riziky použít multikriteriální přístup. Protože některá kritéria k dosažení integrity bezpečnosti jsou konfliktní, optimální řešení musí být stanoveno v dostatečně širokém rozsahu podmínek pro použití při respektování jistých limitů [5,6,11].

6 Opatření zlepšující drážní bezpečnost

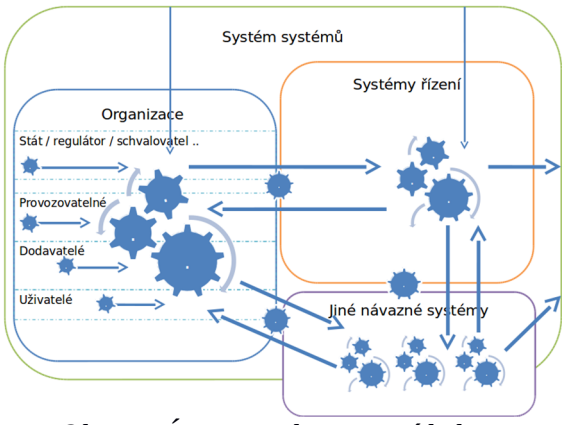
V předloženém případě jsme upravili výše popsaný přístup pro železniční informační systémy, které jsou charakterizovány výše. V souladu s [2] a s jistou úrovní abstrakce, obrázky 2 až 4 znázorňují postupnou změnu systému v průběhu implementace různých technik pro zvýšení informačního výkonu a zabezpečení systému. Obrázek 5 obsahuje legendu k obrázkům předchozím.

Obrázek 2 ukazuje otevřený systém systémů, ve kterém jsou implementované procesy a spojené z důvodu plnění jisté definované funkce. Se zvážením velkého množství systémových spojení a interakcí velkého množství entit, které jsou v systému zahrnuté, za normálních podmínek systém provádí požadovanou funkci, ale je náchylný na chyby, především v případě větších provozních odchylek a nerovnováhy ve vnějším prostředí systému.

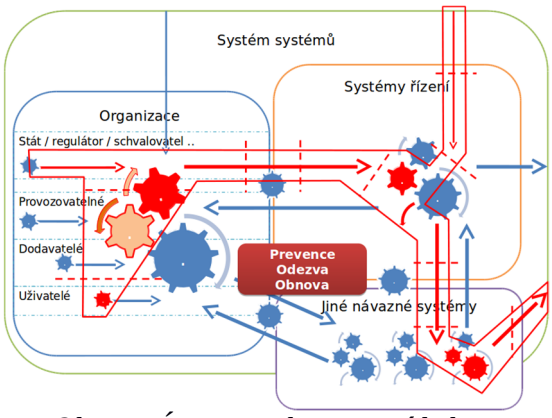
Obrázek 3 ukazuje systém systému s optimalizovaným informačním výkonem, který zvyšuje systémovou odolnost a udržovatelnost a tím i jeho zabezpečení. Optimalizací, tj. usměrněním toků a zlepšením parametrů informačního výkonu, dosáhneme toho, že je systém méně náchylný na vnitřní chyby v případě různých známých provozních odchylek a odchylek v okolí systému.



Obr. 3: Úroveň zabezpečení kyber-fyzického systému (společný systém systému).



Obr. 4: Úroveň zabezpečení kyber-fyzického systému (optimalizovaný s vyšším informačním výkonem).



Obr. 5: Úroveň zabezpečení kyber-fyzického systému (optimalizovaný s vyšším informačním výkonem).

Obr. 6: Legenda

Pro zvýšení informačního výkonu a minimalizace zdrojů, které jsou nezbytné pro tvorbu těchto systémů, lze v praxi využít řadu metod, např.: COBIT pro audit informačních systémů z hlediska vrcholového managementu [17]; ITIL pro řízení informačních systémů a služeb, jehož části jsou standardizované [18]; refaktoring, tj. změny v systému SW, které neovlivní vnější chování informačního systému, ale zlepší jeho vnitřní strukturu [9].

Zavádění systémů řízení [19,20] s podporou informačních systémů navržených pomocí výše uvedených metod, výrazně přispívá ke zlepšení informačního výkonu a parametrů přenosové matice v souladu se vztahem (4), ale to pouze v případě, pokud se kontext systému řízení zaměřuje na drážní systém jako celek, tj. s jednotnou terminologií a zaměřením na rozhraní systémů napříč všemi zúčastněnými, tj. dotčenými subjekty.

Obrázek 4 ukazuje řádně zabezpečený systém s optimalizovaným informačním výkonem, který získáme ochranou optimalizovaného systému (viz Obrázek 3) proti značným externím a interním vlivům, tj. zavádíme preventivní a zmírňující opatření, a připravujeme opatření na odezvu v případě incidentů, stejně tak jako opatření pro rychlou obnovu pomocí ověřených plánů kontinuity. V oblasti řízení a správy železničního systému a souvisejících organizací se

postupně zavádějí systémy a metody podle [21-23]. Musí být však implementovány všemi zainteresovanými subjekty, a především je potřeba se vyrovnat s problémy spojenými se systémovými rozhraními; tj. musí zvážit celý proces vzniku informace, použité informační technologie a kvality jejich parametrů podle kapitoly 3.

Zabezpečení předmětných systémů je dále zaměřeno na identifikaci a řízení důležitých aktiv. Protože nemůže být zajištěné vše, potřebujeme vybrat kritická aktiva, tj. kritické procesy, informační toky nebo další podpůrná informační a fyzická aktiva. Na základě jejich kritičností hodnotíme prioritní rizika a zavádíme příslušná preventivní opatření. V případě výskytu pohromy (včetně kyber-útoku) provádíme odezvu a obnovu v souladu se stanovenou politikou [2,3].

V souladu s principy bezpečnosti systémů systémů, celý drážní systému musí stavět na přístupu obrana do hloubky (ang. Defence-in-Depth) a zavádět rozdílné typy řízení bezpečnosti s reflektováním očekávaných provozních podmínek systému, a případně, pro závažné pohromy, mít také způsob řízení, který chrání také další (okolní) kybernetická, organizační a fyzická aktiva, tj. nejenom aktiva daného systému

7 Závěr

Příklady drážních nehod ukazují několik společných kybernetických příčin, které se skládají z kombinace několika chyb, zejména v návrhu systému řízení bezpečnosti a jeho informačních systémů. Úkolem aplikace informačních systémů je nejen zvýšit provozní hospodářský zisk, ale i úroveň bezpečnosti veřejných aktiv Evropského prostoru. Vzhledem k tomu, že dnešní procesy řízení železnic, tj. uvažované řízení bezpečnosti a dalších části železničního systému (řídicí systémy, infrastruktura, vozidla a zařízení), nemohou bez informačních systémů fungovat, je velmi důležité hledat selhání i v kybernetickém prostředí.

Analýza společných kybernetických příčin, provedená na základě dvou případových studií, poukazuje na problémy související s rozhraními systémů, které jsou v administraci různých subjektů nebo jsou odlišné fyzické povahy. Na základě výše uvedených výsledků a znalostí je zapotřebí použít vícekriteriální přístupy a navrhnout opatření pro zvládnutí zjištěných zranitelností, tj. zlepšení parametrů, které zvyšují informační výkon a zajišťují bezpečnost informací v kritických procesech systémů řízení železnic, jmenovitě v celém procesu vzniku informace a zpracování informací. V případě použití navržených zásad práce přispívá ke zvýšení bezpečnosti železnic.

Použité zdroje

[1] Kertis, T., Prochazkova, D. Railway accidents in the Czech Republic, causes of risks and their mitigation. Safety and Reliability—Theory and Applications: 1667–1673. London: Taylor & Francis Group, 2017.

[2] Kertis, T., Prochazkova, D. Cyber security of underground railway system operation. Smart City Symposium Prague, Prague: CTU Faculty of transportation sciences, 2017.

[3] Kertis, T., Prochazkova, D. Information power and cybernetic causes of rail accidents. Řízení rizik procesů spojených s technickými díly (ŘRTD) 2017. Praha: CTU Faculty of transportation sciences, 2017.

[4] ARTEMIS 2014. Project SESAMO: Security and Safety Modelling.

[5] Prochazkova, D. 2013. Krizové řízení pro technické obory. Praha: CTU.

[6] Kertis, T. 2015. Bezpečnostní plán vybrané stanice pražského metra (Diploma Thesis), Praha: CTU, Faculty of transportation sciences.

[7] Kertis, T. 2016. Porovnání přístupů pro řízení bezpečnosti v dopravě. Rizika podnikových a územních procesů a poznatky pro krizové řízení: 34–59. Praha: CTU.

[8] Kertis, T., Prochazkova, D. 2016. Risk management plan for metro station safe operation. Risk, Reliability and Safety: Innovating Theory and Practice: 1306–1314. London: CRC Press.

[9] Moos, P., Malinovsky, V. Information systems and technologies. Praha: ČVUT 2008.

[10] Prochazkova, D. 2012. Bezpečnost kritické infrastruktury. Praha: ČVUT.

[11] Prochazkova, D. 2015. Safety of complex technological facilities. Saarbruecken: Lambert Academic Publishing.

[12] Novobilsky, P., Kertis, T. & Prochazkova, D. 2016 Cyber security of metropolitan railway communication infrastructure. Risk of business and territorial processes: 78–91. Usti nad Labem: FVTM UJEP.

[13] ČR MD. Zpráva o výsledcích šetření příčin a okolností vzniku mimořádné události: Moravany (trať Česká Třebová—Praha—Libeň). Praha: Drážní Inspekce (MD) 2017.

[14] EU. Advice ERA/ADV/2015-6 OF THE EUROPEAN RAILWAY AGENCY FOR EUROPEAN COMMISSION REGARDING. Brussels: European Rail Agency 2015.

[15] Prochazkova, D. Zásady řízení rizik složitých technologických zařízení. Praha: ČVUT 2017.

[16] Zairi, M. Total Quality Management for Engineers. Cambridge: Woodhead Publishing 1991.

[17] Vitous, M. Cobit 5 v malých a středních firmách. IT Systems: specializovaný měsíčník o podnikové informatice. Brno: CCB 2000.

[18] ISO. ISO/IEC 20000: Information technology—Service management. Geneva: ISO 2011.

[19] ISO. EN ISO 9001: Quality management systems. Requirements. Geneva: ISO 2015.

[20] ISO. ISO/TS 22163:2017 Railway applications—Quality management system—Business management system requirements for rail organizations: ISO 9001:2015 and particular requirements for application in the rail sector. Geneva: ISO 2017.

[21] ISA. ANSI/ISA–62443-1-1 Security for industrial automation and control systems: concepts, terminology and models. Washington, DC: ANSI 2007.

[22] ISO. ISO/IEC 15408-1: Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model. Geneva: ISO 2009.

[23] ISO. ISO/IEC 27001: Information technology—Security techniques—Information security managementsystems—Requirements. Geneva: ISO 2013.

[24] CEN-CENELEC 2017. Rail Sector Forum: Railway in Future.

[25] EU 2020a. Project CertMILS: Compositional security certification for medium to high-assurance COTS-based systems in environments with emerging threats.

[26] EU 2020b. Project CITADEL: Critical Infrastructure Protection Using Adaptive MILS.

Nástroj ke snížení rizik při svařování specifických dílů motoru letadla

RNDr. Jan Procházka, Ph.D, Doc, RNDr. Dana Procházková, DrSc., Ing Šárka Marešová

Fakulta Dopravní, ČVUT, Praha

Japro2am@seznam.cz

7 Úvod

V leteckém průmyslu je na prvním místě bezpečnost. Proto je brán při výrobě leteckých komponent velký zřetel na preciznost a dokonalost provedení všech výrobních operací. Jde o odstranění příčin leteckých dopravních nehod způsobených chybami při výrobě, montáží a údržbě leteckých motorů [1]. Podrobný výzkum zacílený na zvýšení bezpečnosti byl proveden pro firmu GE Aviation Czech v Praze. Byl zaměřen na oblast výroby leteckého motoru, při které je třeba dodržovat technologické postupy a eliminovat lidský faktor, který ovlivňuje proces výroby.

V předloženém článku jsou uvedeny dílčí výsledky výzkumu. Výsledky jsou spojené s výrobou ochranného krytu, který je uvnitř leteckého motoru, je uchycen k jeho vnějšímu plášti, který obklopuje výkonovou trhlinu. Jeho úkolem je chránit letecký motor před úlomky lopatek, disků nebo z jiných částí. Na základě vyhodnocení informací z technických provozních deníků [2] jsme velkou pozornost soustředili na svařování základních komponent ochranného krytu.

Pro identifikaci a vyhodnocení rizik se používají metody rizikového inženýrství, a to procesní mapy, kontrolní seznamy a bezpečnostní audity [3]. Na základě technologického postupu výroby [4] a technické dokumentace výroby [5] jsme zpracovali podrobný kontrolní seznam pro bezpečnostní audit, který jsme dali k posouzení expertům z Technické rady podniku. Poté jsme zajistili bezpečnostní audit za pomocí předmětného kontrolního seznamu. Závěry pro jednotlivé položky kontrolního seznamu při bezpečnostním auditu jsme stanovili jako medián z hodnocení získaných od 3 specialistů (auditor firmy, vedoucí kontrolního úseku, státní inspektor). Vyhodnocením auditu jsme zjistili kritická místa procesu svařování. Následně jsme společně se specialisty navrhli opatření na zvýšení bezpečnosti výroby i výrobku.

8 Kultura bezpečnosti, prevence ztrát a procesní bezpečnost

Kultura označuje specifické materiální a duchovní hodnoty, které lidé vytváří svou činností a kterými obohacují život svůj i život celé lidské společnosti. Kultura společnosti je celistvý systém významů, hodnot a společenských norem, kterými se řídí členové dané společnosti a které prostřednictvím sdílení předávají dalším generacím. Je to sbírka hodnot, symbolů, podnikových hrdinů, rituálů a vlastních dějin, které působí pod povrchem a mají velký vliv na jednání lidí na pracovních místech [6].

Na základě právě uvedených definic pak kultura bezpečnosti znamená, že člověk ve všech svých rolích (řídící pracovník, zaměstnanec, občan či oběť pohromy) dodržuje zásady bezpečnosti, tj. chová se tak, aby sám nevyvolal realizaci možných rizik, a když se stane účastníkem realizace rizik, aby přispěl k účinné odezvě, stabilizaci chráněných zájmů a jejich obnově a k nastartování jejich dalšího rozvoje. Podle některých autorů jde o soubor postojů,

domněnek, norem a hodnot, které existují v dané entitě, který je odrazem toho, jak je podnik řízený, tj. jsou to všeobecné principy rozdělení pravomoci a odpovědnosti, zásady řízení a jistý poměr mezi důrazem na pracovní výsledky, autoritou, péčí o lidi, dodržování zásad bezpečnosti a zajištění funkčnosti dané entity [6].

Účinná kultura bezpečnosti je základním prvkem pro řízení bezpečnosti. Odráží koncepci bezpečnosti a vychází z hodnot, stanovisek a jednání vrcholových řídících pracovníků a z jejich komunikace se všemi zúčastněnými. Je zřetelným závazkem aktivně se podílet na řešení otázek bezpečnosti a prosazuje, aby všichni zúčastnění konali bezpečně a aby dodržovali příslušné právní předpisy, standardy a normy. Pravidla kultury bezpečnosti musí být zapracována do všech činností v území nebo jiné entitě. Jejich základem není koncentrace na potrestání viníků / původců chyb, ale poučení z chyb a zavedení takových nápravných opatření, aby se chyby nemohly opakovat nebo aby se alespoň výrazně snížila četnost jejich výskytu.

Principy kultury bezpečnosti [7]:

1. Přímý, otevřený přístup k slabým místům, jednání zaměřené na nalezení řešení.
2. Odklon od kultury připisování viny.
3. Pracovníci i vedení jednají odpovědně, samostatně s orientací na tým. „Kultura odpovědnosti“ je součástí jejich života.
4. Standardy bezpečnosti jsou akceptovány a integrovány do každodenní činnosti firmy.
5. Bezpečnost a ochrana zdraví tvoří významnou hodnotu jak pro pracovníky firmy, tak i pro celou organizaci

Úroveň kultury bezpečnosti je veličina, kterou není možno přímo a exaktně změřit, přesto má zásadní vliv na chování pracovníků, styl řízení i úroveň technologie. Definování slabých a silných stránek v jednotlivých oblastech bezpečnosti je důležité pro úroveň kultury bezpečnosti. Porovnání časové řady průzkumů umožní vyhodnotit účinnost korektivních opatření.

Kultura bezpečnosti pro společnost vyrábějící motor letadla znamená, že se společnost zavazuje provozovat výrobu s nejvyššími standardy bezpečnosti. Pro dosažení tohoto cíle je rozhodující mít zavedené účinné a bez zábran prováděné ohlašování (oznamování) všech nehod, incidentů, nahodilých událostí a případů, zkušeností, pochybností a dalších informací a údajů, které by mohly mít nepříznivý vliv na bezpečně vyrobený díl leteckého motoru. A nakonec každý jednotlivý zaměstnanec je nejen laskavě vybízen, ale i povinen ohlásit jakoukoli informaci, týkající se bezpečnosti. Ohlašování není předmětem jakéhokoli obviňování a následného odvetného opatření. Hlavním účelem ohlašování je řízení a ovládání rizika a předcházení incidentům a nehodám, nikoli přisuzování viny. Nebudou podnikány žádné kroky vůči zaměstnanci, který oznámí jakékoli údaje, týkající se bezpečnosti pomocí systému hlášení, pokud takové oznámení bez nejmenších pochybností neodhalí, že byl spáchán nezákonný čin, hrubá nedbalost nebo úmyslné a vědomé porušení předpisů nebo technologických postupů. Metoda sběru, zaznamenávání a šíření bezpečnostních informací zaručuje ochranu v celé šíři a objemu dle zákona, včetně ochrany totožnosti toho, kdo informaci, týkající se bezpečnosti ohlásil [7]. Jednotlivé pilíře kultury bezpečnosti jsou znázorněny na obr 1.

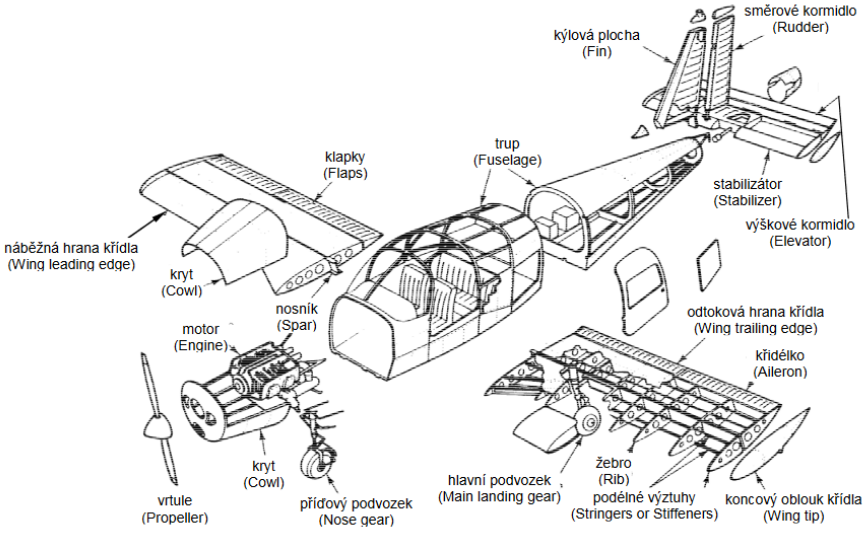
Obr. 1. Základní pilíře kultury bezpečnosti [8]. Je vítaná otevřená komunikace, důraz je kladen na prevenci a od vedoucích se vyžaduje rozhodovat ve prospěch bezpečnosti a jsou jim poskytovány zdroje pro budování bezpečnosti.

V souvislosti s kulturou bezpečnosti se často v současné odborné literatuře spojené s technologiemi používají pojmy prevence ztrát a procesní bezpečnost. Jejich definice uvedeme také proto, že jsou to nástroje, které slouží ve spojitostech s technologiemi k ochraně osob I majetku. Prevence ztrát (Loss Prevention) je systematický přístup k prevenci (předcházení) havárií nebo k minimalizaci jejich dopadů. Zahrnuje prostředky pro eliminaci zdrojů rizik nebo omezení pravděpodobnosti jejich realizace a pro zmírnění dopadů spojených s touto realizací (preventivní a následná opatření). Dále zahrnuje identifikaci vhodných kontrolních opatření, identifikaci a aplikaci vhodných nápravných opatření, kterými se zajišťuje bezpečná entita mající příslušnou úroveň bezpečí a udržitelného rozvoje a nepředstavující nepřijatelné nebezpečí pro své okolí [9].

Procesní bezpečnost nebo lépe bezpečnost procesů je odvětví bezpečnosti zaměřené na bezpečnost v průmyslu, ve kterém je řada výrobních a přídavných procesů, které jsou nutné k vytvoření konečného produktu daného průmyslu. Jde přitom o zabránění vzniku havárií, které mají zvláštní a charakteristické rysy pro daný specifický průmysl. Zabývá se např. prevencí bezprostředních úniků chemických látek nebo energií ve škodlivém množství, a v případě, že se tyto úniky vyskytnou, tak omezením jejich velikosti, dopadů a následků. Nezahrnuje otázky klasické bezpečnosti a ochrany zdraví při práci, tj. zabývá se čistě technickými problémy, čímž se liší od systémové bezpečnosti, která je zacílená na všechna základní veřejná aktiva.

9 Bezpečnost leteckého motoru

Letadlo je létající dopravní prostředek těžší vzduchu s pevným křídlem. Jedná se o bezpečný systém, který tvoří základní části a to jsou-drak (křídlo, trup, ocasní plochy, řízení, podvozek), výstroj (záchranné systémy, odmrazovací, klimatizace a přetlakování, vybavení kabiny, přístroje) a pohonná jednotka [10]; schématický technický popis letadla je na obr. 2.



Obr. 2. Schématický popis letadla [10].

Aby letadlo mohlo letět, potřebuje určitou rychlost letu a úhel náběhu, jinak by mohlo dojít ke ztrátě potřebného vztlaku pro let. Potřebnou rychlost letu zabezpečuje tažná jednotka, tj. motor letadla. Motor letadla se skládá z generátoru (srdce motoru), který je složen z kompresoru, spalovací komory a generátorové turbíny. Kompresor z okolní atmosféry nasává vzduch, který stlačí a přesune dále do spalovací komory. Ve spalovací komoře dochází ke vstřikování paliva, které hoří, a vzniklé horké plyny pohánějí turbínu generátoru. Přes společnou hřídel tato turbína pohání kompresor a tím získává stlačený vzduch, který je potřebný k hoření paliva [1]. Pro pohon volné turbíny, která je připojena k vrtuli přes reduktor (převodovka o stálém poměru, jejímž účelem je snižování vysokých otáček volné turbíny na úroveň použitelnou pro vrtuli), se využívá zbylá energie v horkých plynech za generátorovou turbínou [1].

Důležitou funkci při ochraně motoru plní ochranný kryt [6]. Jde o statický, tj. nerotační díl, jehož funkcí je zachytit případné úlomky lopatek nebo disku, případně jiných dílů. Nachází se uvnitř leteckého motoru, uchycený k jeho vnějšímu plášti a obklopující výkonovou turbínou. Protože navazuje na spalovací komoru, z které jsou horké plyny usměrňovány na lopatky výkonové turbíny, je navrhován tak, aby kromě pohlcování nárazové práce, odolával vysoké teplotě a tlaku [1].

Proto ochranný kryt musí být dimenzován pro zachycení velké kinetické energie. I když lopatka turbíny má relativně malou hmotnost, tak výpočet [11] ukazuje, že odstředivá síla při otáčkách, kterými lopatka v leteckém motoru rotuje, dosahuje hodnoty téměř 16 000 N, což je v přepočtu přibližně 1.6 t.

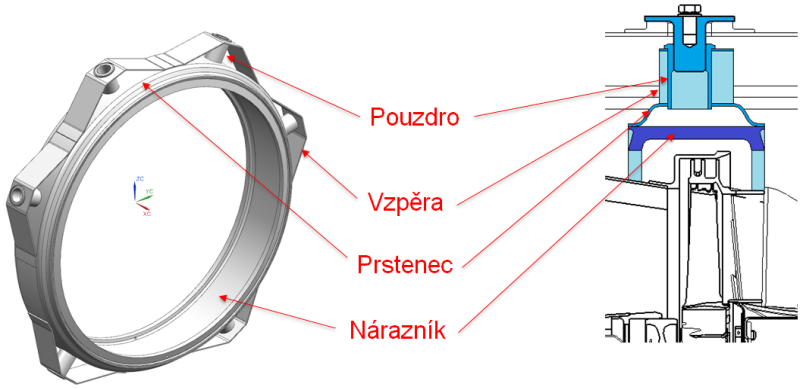
Z hlediska návrhu konstrukce ochranného kruhu se vždy jedná o kompromis. Na jedné straně je požadavek na konstrukci dostatečně robustnou, aby byla bezpečnost dostatečně zajištěna. Na druhé straně je požadavek na co nejmenší hmotnost.

Analýza závad rotoru [11] ukázala, že za selhání motoru jsou odpovědné v 60 % úlomky dílů motoru (56 % úlomky lopatek, 4 % úlomky disků, skříně, těsnění apod.), a že ochranný kryt nezachytil jen 15 % úlomků lopatek.

10 Data pro ochranný kryt

Z technické dokumentace [1] vyplývá, že všechny díly horké sekce leteckého proudového motoru, tj. i ochranný kryt, musí odolávat působení vysokých teplot a vysokých tlaků. Proto jediným druhem materiálů, které můžeme použít, jsou niklové a kobaltové superslitiny. Do této skupiny patří i vytvrditelná niklová superslitina Nimonic 80A, která se použitá po výrobu ochranného krytu.

Vyhotovení celého ochranného krytu je zdlouhavý a náročný proces. Sestava ochranného kruhu se skládá ze čtyř dílů (obr. 3), které jsou vzájemně spojeny svařováním.



Obr. 3. Zobrazení sestavy ochranného krytu a jeho komponent (vlevo) a zobrazení umístění ochranného krytu v turbovrtulovém motoru (vpravo) [4]

Ochranný kryt se skládá ze 4 částí:

1. Nárazník - je nejdůležitější část ochranného krytu, která přijde jako první do kontaktu s lopatkami. Slouží k samotnému zachycení případných uvolněných dílů vysokotlaké turbíny (lopatek).
2. Pouzdro - slouží k umístění čepu (čep již není součástí sestavy ochranného krytu). Čep slouží k ustavení celé sestavy ochranného krytu s pláštěm motoru.
3. Prstenec - slouží k ustavení pouzdra pro uchycení k plášti motoru.
4. Vzpěra - slouží k upevnění pouzdra na správné pozici vzhledem k nárazníku.

Výrobní proces uvedených dílů zahrnuje velké spektrum výrobních technologií, jak ukazuje procesní mapa uvedená v práci [11]. Lze mezi nimi najít zpracování na klasických soustruzích nebo pomocí zámečnických prací, CNC obrábění jako je použití CNC soustruhů a CNC frézek a ohýbání. Mezi dalšími použitými metodami jsou metody speciálních procesů, jako je žíhání na odstranění vnitřního pnutí a precipitační vytvrzení nebo svařování metodou bodového svařování a TIG (Tungsten Inerts Gas) svařování. Důležitou operací mezi zpracováním materiálu jsou mezioperační kontroly pro překontrolování rozměrů a správného opracování. Jednou z takových specifických kontrol je defektoskopie barevně luminiscenční pro indikaci trhlin a povrchových vad materiálu.

Na základě analýz výrobních postupů v práci [11] provedených na základě provozního deníku [2] se ukázalo také kritickým úkonem svařování TIG. Proto uvádíme výsledky šetření.

Svařování TIG patří mezi obloukové metody svařování. Elektrický oblouk hoří mezi netavící se wolframovou elektrodu a roztaveným svarovým kovem (svarovou lázní) v inertní atmosféře

ochranného plynu. Pro účely svařování se jako ochranný plyn používá argon, helium, nebo jejich směsi [12].

Svařování metodou TIG (Tungsten Inerts Gas) bylo vyvinuto na konci 30. let 20 století, pro potřeby svařování hořčíkových slitin. Tato metoda svařování z části nahradila nýtování, jako v té době nejpoužívanější metody spájení komponent z hliníku a hořčíku v leteckém průmyslu.

Předmětná metoda svařování má nezastupitelnou pozici při svařování komponent z nerezové oceli, hliníku, hořčíku, mědi a reaktivních materiálů (např. titanu a tantalu). Tloušťka svařovaných materiálů se pohybuje od několika desítek milimetrů až po tloušťku několika milimetrů [13].

Výhody metody TIG oproti jiným způsobům svařování jsou dle [13]:

1. Produkce svarů vysoké kvality, tj. nízká deformace svařovaných dílů, svary s minimálním množstvím nečistot, plynů, respektive pórů a trhlin, jejichž výskytem se snižuje únosnost materiálu (odolnost vůči vysoké teplotě a tlaku).
2. Při svařování nevznikají výprsky, nevzniká tedy ani potřeba jejich dodatečného odstraňování.
3. Svařování je možné provádět s, nebo bez přídavného materiálu.
4. Svařování téměř všech druhů materiálů a také svařování různorodých materiálů.
5. Přesná kontrola svářecích parametrů.

Metoda svařování TIG se používá v případech, kdy jsou požadavky na vysokou kvalitu svarů. Pomocí metody je možné svařit téměř všechny druhy kovových materiálů. Svářeč během svařování je schopný velmi přesné kontroly tepla vneseného do svaru, protože okolí svaru není během svařování obklopeno výpary a plyny z procesu [13].

Kromě výhod má ale svařování metodou TIG v porovnání s ostatními metodami svařování také nevýhody [13], a to:

1. Nižší výkon svařování v porovnání s jinými obloukovými metodami svařování.
2. Vyšší nároky na zručnost svářečů.
3. Vyšší ekonomická náročnost výroby v porovnání s metodou svařování obalenou elektrodou.

Dle předpisu AWS D17.1 [14] se svary dle vzájemné polohy svařovaných dílů rozdělují na:

1. Tupé svary – spoj dvou materiálů (plechů, nebo trubek), vzájemně spojenými čelnými plochami.
2. Koutové svary – spojení dvou materiálů, které jsou vzájemně pod úhlem, a svarový spoj je umístněný v okrajích těchto svařovaných dílů.

Dále uvedeme výsledky jen pro svařování pomocí tupého svaru metodou TIG.

11 Použité metody rizikového inženýrství

Pro odhalení a posouzení rizik byly použity metody: procesní mapa, tj. schématické znázornění procesu výroby, které ukazuje místa, kde může vznikat konflikt ve výrobě z důvodu nedostatečných kapacit pracoviště nebo špatného plánování výroby [15]; kontrolní seznam [3]; a bezpečnostní audit [1].

Specifický kontrolní seznam byl sestaven podle výrobního postupu svařování metodou TIG [4], při kterém byla určena kritická místa na základě deníku provozních událostí firmy [2]. Je uveden v tab. 1.

Tab. 1. Kontrolní seznam použitý pro vyhodnocení rizik procesu svařování

Pořadové číslo	Otázka	ANO	NE	Poznámka
Příprava před svařováním				
1	Jsou spojované plochy svařovaných dílů kovově čisté, tj. jsou zbaveny okují a hrubých vrstev oxidu?			
2	Jsou spojované plochy svařovaných dílů zbaveny mastnoty?			
3	Jsou spojované plochy svařovaných dílů zbaveny jiných nečistot ovlivňujících kvalitu prováděných svarů?			
4	Je slícování svařovaných dílů, tj. velikost svařovací mezery v souladu s požadavky předpisu?			
5	Je slícování svařovaných dílů, tj. velikost přesazení svařovaných ploch v souladu s požadavky předpisu?			
6	Jsou hrany spojovaných materiálů v místě budoucího svaru zbaveny otřepů?			
7	Jsou hrany spojovaných materiálů v místě budoucího svaru bez výraznějšího sražení?			
8	Jsou svařované díly pokládané na čistý odmaštěný povrch pracovního stolu?			
9	Je s díly manipulováno v čistých bavlněných rukavicích nepouštějících vlákna?			
Stroje a zařízení				
10	Používají se pro účely svařování pouze certifikované stroje a zařízení?			
11	Používají se pro účely svařování pouze kalibrované stroje a zařízení?			
12	Používají se pro účely svařování stroje a zařízení stanovené v technologickém postupu [16]?			
13	Je zdroj svařování schopný plynulé regulace v celém rozsahu hodnot parametru svařování, uvedených v technologickém postupu [17]?			
14	Je zdroj ochranného plynu schopný plynulé regulace v celém rozsahu hodnot parametru svařování, uvedených v technologickém postupu?			
15	Je zdroj svařovacího proudu bez známek poškození?			
16	Je příslušenství bez známek poškození?			
17	Jsou kabely bez známek poškození?			
18	Je podložka, na které je umístěný svařovaný dílec, rovná, bez výrazných nerovností a důlků.			
19	Je podložka pro svařování z elektricky vodivého materiálu?			
20	Jsou svorky svařovacího zařízení umístěny v těsné blízkosti svařovaného dílu?			
21	Je mezi svorkou a podložkou zabezpečena dostatečná elektrická vodivost?			
22	Splňuje kvalita ochranného plynu minimální požadavky na čistotu dle platných norem a předpisu [16]?			
23	Je používaný ochranný plyn dle technologického postupu [16] s platnou atestací?			
24	Je svařovací hořák dimenzovaný pro dané proudové zatížení?			
25	Jsou kabely dimenzovány pro dané proudové zatížení?			
26	Je hubice hořáku bez viditelného poškození?			
27	Je průměr hubice v rozsahu stanoveném v technologickém postupu [16], umožňující přívod dostatečného množství ochranného plynu pro efektivní ochranu svařovaného kovu před účinky okolní atmosféry?			
28	Shoduje se typ wolframové elektrody s požadavky uvedenými v technologickém postupu [16]?			
29	Shoduje se průměr wolframové elektrody s požadavky uvedenými v technologickém postupu [16]?			
30	Je wolframová elektroda dimenzovaná i pro maximální proudové zatížení?			
Svářečský personál				
31	Provádí svařování kvalifikovaný svářečský personál?			
32	Je svářečský personál řádně vyškolen?			
33	Má svářečský personál platný svářečský průkaz?			

34	Má svářečský personál platnou lékařskou prohlídku?			
Proces svařování				
35	Jsou v případě požadavků na stehování stehy rozmístěny rovnoměrně?			
36	Jsou stehy bez trhlin a kráterů?			
37	Je použit jako přídavný materiál pouze certifikovaný svařovací drát?			
38	Je přídavný materiál odmaštěn?			
39	Je přídavný materiál zbavený prachu a nečistot?			
40	Je přídavný materiál řádné označen?			
41	Je přídavný materiál skladovaný v originálním obalu?			
42	Používá se pouze řádně označený přídavný materiál?			
43	Je zakázáno používat neoznačený přídavný materiál?			
44	Je použit pro účely svařování svařovací drát požadovaného chemického složení?			
45	Je použit pro účely svařování svařovací drát uvedený v technologickém postupu [16]?			
46	Je použit pro účely svařování svařovací drát požadovaného rozsahu průměrů?			
47	Je svařovací proud nastaven dle technologického postupu nebo certifikátu svaru [16]?			
48	Je rychlost svařování nastavena dle technologického postupu nebo certifikátu svaru [16]?			
49	Je povrch svarové housenky po svařování očištěn nerezovým kartáčem?			
50	Je teplem ovlivněná oblast po svařování očištěna nerezovým kartáčem?			
Kontrola po svařování				
51	Je vizuální kontrola svaru prováděna na pracovišti pro tuto kontrolu určenou?			
52	Jsou k dispozici záznamy o kontrole minimální požadované hodnoty intenzity osvětlení (300 lx)?			
53	Je vizuální kontrola prováděna volným okem dle předpisu pro vizuální kontrolu svaru?			
54	Je vizuální kontrola prováděna lupou požadovaného zvětšení dle předpisu pro vizuální kontrolu svaru [16]?			
55	Je personál provádějící vizuální kontrolu svaru kvalifikovaný?			
56	Je personál provádějící vizuální kontrolu svaru proškolený?			
57	Jsou záznamy pro účely kontroly k dispozici?			
58	Jsou v případě odhalení chyb svaru, tyto chyby svaru odstraněny?			
59	Jsou chyby svaru odstraněny pouze v rozsahu povolující daný předpis?			

Hodnocení výsledků bezpečnostního auditu provedeného dle kontrolního seznamu je posuzováno dle stupnice ČSN OHSAS 18001, tab. 2 [18].

Tab. 2. Míra rizika dle stupnice [18]

Míra rizika	**Hodnoty "NE" v %**
Extrémně vysoká	Více než 95 %
Velmi vysoká	70 - 95 %
Vysoká	45 - 70 %
Střední	25 -45 %
Nízká	5 - 25 %
Zanedbatelná	Méně než 5 %

12 Výsledky bezpečnostního auditu a návrhy na zlepšení bezpečnosti

Kontrola procesu svařování byla provedena na pracovišti Svařovna pod dohledem technologa a auditora. V případě odpovědí „NE“ bylo uvedeno, proč je odpověď záporná. Vyhodnocování bylo prováděno auditorem. Kromě vyhodnocení kontrolního seznamu byla zhotovena i fotodokumentace a byl sepsán zápis, který podepsali všichni zúčastnění, tj. i svářeč [19].

Ze zápisu o auditu [19] vyplývá, že z celkového počtu 59 otázek bylo zodpovězeno 6 otázek jako "NE", tj. 10 % záporných odpovědí. Z hlediska posuzování rizika se jedná o nízkou míru. Pro odstranění 4 problémů, které ovlivňují kvalitu svaru, byla navržena opatření:

1. Problém 1 - spojované plochy svařovaných dílů nejsou před samotným svařováním zbaveny okují, hrubých vrstev oxidu, mastnoty a jiných nečistot negativně ovlivňujících kvalitu prováděných svarů [4,12,13]. Před svařováním jsou svařované díly pouze umyty v čistící lázni. Na povrchu těchto dílů jsou patrné zbytky čistící emulze.

Návrh na zlepšení: Pro dosažení vysoké kvality svarových spojů je nutné z povrchu dílů v místě budoucího svaru odstranit všechny nečistoty. Povrchové oxidy, případné okuje je vhodné odstranit mechanicky za pomoci nerezového kartáče nebo SiC brusiva (smirkové plátno). Odmaštění dílů je vhodné provádět chemicky, tj. acetonem nebo technickým lihem. Je to důležité proto, že mastnota, zejména síra se ve svarové lázni slučuje s niklem a způsobuje trhliny v daném svaru.

2. Svařované díly je nutné před svařováním dopasovávat z důvodu často nevyhovující velikosti svarové mezery [2,4].

Návrh na zlepšení: Pro dosažení vysoké kvality svarových spojů je potřebné, aby svarová mezera u lemových svarů byla minimální, ideálně nulová. Důvodem je skutečnost, že při tuhnutí svarového kovu dochází k jeho smršťování a tím vzniku tahových napětí. Čím větší svarová mezera, tím větší tahová napětí vznikají. Když velikost vzniklých tahových napětí překročí mez pevnosti materiálu, dochází ke vzniku trhlin. Proto má na kvalitu provedených svarů vliv nejen samotné svařování, ale také příprava, tj. sestavení dílů. Dosáhnout požadovaného sestavení je možno dosáhnout dodržením technologického postupu [16], tj. dodržení předepsaných tolerancí, které mají za následek zvýšení přesností rozměrů vyráběných dílů.

3. Přídavný materiál pro svařování se používá ve formě tyček o průměru Ø 2,0 mm. Ačkoli je daný svar certifikován s přídavným drátem Ø 2,0 mm jako vyhovující, pro svařování tlouštěk materiálů, z jakých je vyroben ochranný kryt, by bylo vhodnější volbou použití přídavného drátu menšího průměru, ideálně Ø 1,6 mm. Důvodem je nižší teplo potřebné pro odtavení svařovacího drátu, a tedy i nižší množství tepla vneseného do svaru. Tím se dosáhne užší teplem ovlivněné oblasti svaru (TOO) [4,16]. V našem případě se jedná o svařování vytvrzeného materiálu, v kterém vznikají trhliny právě v TOO [2], tj. čím užší TOO, tím menší je pravděpodobnost vzniku vad.

Návrh na zlepšení: Momentálně není na území České republiky dodavatel dodávající přídavný materiál požadované tloušťky 1,6 mm. Zahraniční dodavatelé potřebný materiál nabízejí, ale v balení v množství, které svařovna není schopna dlouhodobě spotřebovat a nákupem od těchto dodavatelů by došlo k velkému plýtvání. Proto tento návrh nebyl zatím realizován.

4. Pro účely svařování není k dispozici polohovací zařízení. Navržením vhodného polohovadla s nastavitelnou rychlostí otáčení by se dosáhlo usnadnění práce, zvýšení pohodlí a neposlední řadě zvýšení kvality práce, a tedy i svaru [11]. Polohovadlo by se dalo využít i pro jiné svařované díly do motoru.

Návrh na zlepšení: Nákup nového polohovacího zařízení a posouzení jeho vlivu na zvýšení kvality svaru a ergonomii práce.

13 Závěr

Na základě projektu o spolupráci s firmou GE Aviation Czech jsou postupně vytvářeny nástroje na snížení provozních rizik s cílem zajistit vysokou bezpečnost motorů letadel. Jeden z nástrojů zacílený na bezpečnost ochranného krytu motoru letadla pro proces svařování je předmětem sdělení. Bezpečnostní audit provedený podle specifického kontrolního seznamu byl proveden na pracovišti svařovny, při svařování dílů ochranného krytu, za přítomnosti technologa svařování a auditora.

Při bezpečnostním auditu byly zjištěny nedostatky týkající se přípravy dílů před svařováním. K odstranění nedostatků byla navržena opatření, které firma začala realizovat. K dnešnímu dni nedošlo k realizaci změny tloušťky průměru tloušťky svařovacího drátu, tj. provádění svařování přídavným materiálem, tj. drátem menšího průměru, protože na trhu přídavný materiál požadovaného průměru a v požadovaném množství není.

Poděkování: Článek zpracován v rámci dotace projektu RIRIZIBE, CZ.02.2.69/0.0/0.0/16_018/0002649.

Použité zdroje

[6] GE AVIATION. Výroba turbovrtulového motoru v 6 krocích. https://www.geaviation.cz/clanky/detail/35_95-vyroba-turbovrtuloveho-motoru-v-6-krocich

[7] GE AVIATION CZECH. Technické provozní deníky. Praha: GE Aviation Archives.

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

[9] GE AVIATION CZECH. Technologický postup výroby ochranného krytu. Praha: GE Aviation Archives 2016.

[10] GE AVIATION CZECH. Technická dokumentace. Praha: GE Aviation Archives 2017.

[11] PROCHÁZKOVÁ, D. Ochrana osob a majetku. ISBN: 978-80-01-04843-6. Praha: ČVUT 2011, 301p.

[12] ČESKÁ TECHNOLOGICKÁ PLATFORMA BEZPEČNOSTI PRŮMYSLU. - Co je to kultura bezpečnosti. http://www.cztpis.cz/safety-culture-award/kultura-bezpecnosti/

[13] DEPOSITPHOTOS. Kultura bezpečnosti – Stock obrázek. http://cz.depositphotos.com/65417987/stock-photo-culture-of-safety.html

[14] PROCHÁZKOVÁ, D. Analýza a řízení rizik. ISBN: 978-80-01-04841-2. Praha. ČVUT 2011, 405p.

[15] ULT. Letadla. http://www.aerospace.fsik.cvut.cz

[16] MAREŠOVÁ, Š. Nástroj ke snížení rizik při výrobě specifických dílů pro motor letadla. Praha: ČVUT, fakulta dopravní 2017, 66p.

[17] HRIVŇÁK, I. Zváranie a zvariteľnosť materiálov. ISBN 978-802-2731-676. Bratislava: STU 2009, 126p.

[18] OLSON, D. L. ASM Handbook, Volume 6: Welding, Brazing, and Soldering. ISBN 978-0-87170-382-8. Washington: ASM 1993, 168p.

[19] AWS D17.1/D17.1M:2010-AMD1. Specification for Psion welding of aerospace and applications. Miami: FL: American Welding Society 2013.

[20] ASME. The Impact Load on Containtment Rings During a Multiple Blade Shed In Aircraft Gas Turbine Engines. http://asme.org

[21] SMC. Publication Number SMC-099. Nimonic alloy 80A. http://www.haraldpihl.se/globa lassets/pdf/057nimonic-alloy-80a.pdf

[22] FLICKR Report 4310481794. https://www.flickr.com/photos/browndogwelding/4310481794

[23] PROCHÁZKOVÁ, D. Základy řízení bezpečnosti kritické infrastruktury. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223p.

[24] GE AVIATION CZECH. Zápis z auditu, 24. 4. 2017. Praha: GE Aviation Archives.

220 – Česká společnost pro jakost
Přidělení ISBN pro Vaši níže uvedenou publikaci:
ISBN 978-80-02-02841-3
Aktivity ČR v rámci European Safety and Reliabitily Assocation,
Sborník přednášek, kolektiv autorů, 1. vydání, rok vydání 2018, vazba brožovaná