METODIKA

pro tvorbu studií bezpečnosti v letecké dopravě s využitím kvantitativních metod

Výzkumný projekt TA ČR Zéta č. TJ01000252

Ústav letecké dopravy
Fakulta dopravní
ČVUT v Praze

Letiště Praha, a.s.

Lališ Andrej Ing., Ph.D.
Stojić Slobodan Ing., Ph.D.
Štumbauer Oldřich, Ing.

Kafková Markéta, Ing.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Letiště Praha

T A
Č R
Technologická agentura České republiky

Program Zéta

Metodika pro tvorbu studií bezpečnosti v letecké dopravě s využitím kvantitativních metod

Obsah

Úvod

Studie bezpečnosti patří bezesporu mezi klíčové aktivity, které je potřeba provádět ve všech rizikových průmyslech, letectví nevyjímaje. Základním smyslem těchto studií je posouzení, zda konkrétní systém (technologie, infrastruktura, postupy a procedury atp.) má dobré předpoklady být přijatelně bezpečným v provozu. Tento úkol se týká nejen posuzování zcela nových systémů, které nemají žádnou historii v provozu, ale také změn systémů již existujících, které je potřeba z různých důvodů upravit. Obzvláště v moderní době je toto poměrně náročný úkol, jelikož moderní technologie se stává více komplexní a také více závislá na složitých interakcích se svým uživatelem i okolím [1]. V letectví je tento aspekt formulován v nejnovější (čtvrté) verzi ICAO Doc. 9859 Safety Management Manuálu [2], od Mezinárodní organizace pro civilní letectví ICAO, jako problém vzájemné propojenosti a z toho pramenící závislosti jednotlivých složek letecké dopravy navzájem. Z tohoto důvodu je třeba klást větší důraz na systémové aspekty i v oblasti studií bezpečnosti a pokud možno omezovat dopad subjektivního hodnocení bezpečnostních analytiků na celkový výsledek studií. Právě na zmiňované výzvy dnešní doby reaguje tato metodika.

Metodika poskytuje základní návod pro analýzu a vyhodnocování rizika v procesech letecké dopravy, se zaměřením se na organizace typu letiště. Svým obsahem dokument zapadá do procesu řízení rizik a jeho novost vychází ze začlenění aktuálních znalostí bezpečnostního inženýrství, resp. teorie bezpečnosti. Metodika je plně v souladu s mezinárodními standardy a doporučeními v letecké dopravě, především se zmiňovaným dokumentem ICAO Doc. 9859 Safety Management Manual [2]. Dokument vychází ze současných postupů realizace bezpečnostních studií v letectví, které jsou implementovány v leteckém průmyslu nejčastěji jako variace metodiky SAM (Safety Assessment Methodology) [3] publikované Evropskou organizací pro bezpečnost leteckého provozu EUROCONTROL (European Organisation for the Safety of Air Navigation). Hlavní novostí je rozšíření a konsolidace základního procesu metodiky SAM, konkrétně kroků týkajících se identifikace nebezpečí a posouzení rizika, se systémovým modelem bezpečnosti STAMP (Systems-Theoretic Accident Model and Processes) [4]. Metodika tak řeší současné výzvy v oblasti propojení a systémové závislosti moderních rizikových odvětví, jako je letectví. Metodika na druhou stranu nenavrhuje žádnou změnu principů metodiky SAM, pouze některé její části využívá jako základ pro rozšíření. Samostatným rozšířením je pak doplnění kvantitativního hodnocení, které se týká přizpůsobení některých kroků studií bezpečnosti za účelem zvýšení celkové objektivity provádění studií bezpečnosti, zejména v kontextu hodnocení úrovně rizika. V tomto ohledu dokument cílí zejména na problémy, které souvisí s aplikací matice rizik. I dle standardů ICAO se jako jeden z hlavních nástrojů navrhuje využití matice rizik s dvoudimenzionálním hodnocením, kdy se posuzuje pravděpodobnost a závažnost daného následku nebezpečí. Dle výzkumu vybraných matematických vlastností matice rizik však tato má výrazná omezení, jakými jsou špatné rozlišení, chyby, suboptimální přidělování zdrojů a nejednoznačné vstupy a výstupy [5]. I dle samotné teorie modelu STAMP je matice rizik jako nástroj pro hodnocení rizika značně omezená a její aplikace pro hodnocení nových nebo pozměněných systémů je často sporná [4].

V následujících kapitolách je detailně přiblížena nová metoda pro realizaci studií bezpečnosti se zaměřením se na leteckou dopravu, konkrétně organizace typu letiště. V samostatné kapitole jsou vysvětleny teoretické základy systémového přístupu k provádění studií

bezpečnosti a detailněji je popsán vybraný systémový model STAMP jako i metodika STPA [6], která byla původně navržena autory modelu STAMP k analýze nebezpečí. Následuje vlastní popis metodiky s názornými ukázkami její aplikace.

1. Cíl metodiky

Metodika si klade za cíl diseminovat výsledky realizovaného výzkumu Českým vysokým učením technickým v Praze ve spolupráci se společností Letiště Praha, a.s. v projektu č. TJ01000252 s podporou Technologické agentury České republiky. Metodika je souhrnem znalostí z projektu a obsahuje postup pro tvorbu studií bezpečnosti v letecké dopravě, se zaměřením na organizace typu letiště, s využitím systémového přístupu a kvantitativních metod pro analýzu a vyhodnocení rizik. Cílem nově vzniklé metody je zvýšení objektivity vyhodnocování úrovně rizika v rámci studií bezpečnosti se zaměřením na oblast letišť a vytvoření metody, která bude sledovat systémový přístup k bezpečnosti.

2. Dedikace

Metodika je primárně určena pro organizace typu letiště, které mají zájem o zlepšení postupů provádění studií bezpečnosti a tím i zvýšení úrovně provozní bezpečnosti na vlastní infrastruktuře. Metodiku lze aplikovat i v jiných typech organizací v leteckém průmyslu nebo také v jiných rizikových průmyslech, jako je jaderná energetika, chemický průmysl apod. I když je samotný postup metodiky obecný, v případě aplikace na otázky bezpečnosti jiných typů organizací jako jsou letiště, resp. jiného než leteckého průmyslu, metodika nezaručuje úplnou shodu se specifikacemi těchto domén a je proto v těchto případech potřeba zvážit případné úpravy nebo doplnění.

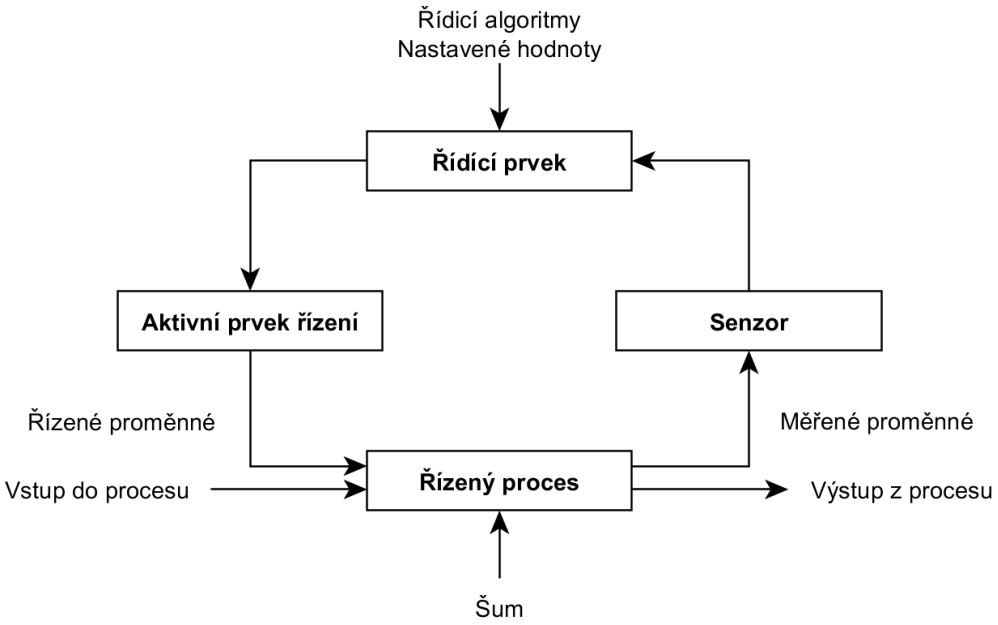
3. Popis metodiky

V této kapitole je uveden vlastní popis nového postupu pro tvorbu studií bezpečnosti v letecké dopravě, se zaměřením se na organizace typu letiště, s využitím systémového přístupu a kvantitativních metod pro analýzu a vyhodnocení rizik. Nové postupy vychází z teorie modelu STAMP, nejprve jsou proto představeny relevantní části této teorie. V metodice je uveden základní popis teorie se všemi relevantními odkazy, se kterými by měl uživatel obeznámit, aby plně porozuměl obsahu metodiky. V další kapitole pak následuje detailní popis nového postupu pro tvorbu studií bezpečnosti jako i několik praktických ukázek aplikace jejích částí.

3.1 Teorie bezpečnosti dle modelu STAMP [4]

STAMP je moderní systémový model bezpečnosti, který interpretuje problém bezpečnosti jako problém řízení. Model zde přebírá koncept zpětnovazebního řízení (tzv. “feedback control”) [7], jelikož tento koncept reprezentuje, jak jsou moderní systémy řízené, a to jak po sociální, tak po technické stránce. I když má zpětnovazební řízení původ v počítačové technologii, lze jím popsat i ryze sociální systém, kde řídícím prvkem je člověk a řízeným prvkem také člověk.

Základním konceptem zpětnovazebního řízení je řídící smyčka zobrazena na obrázku obr. 1. Dle teorie modelu STAMP je možné jakoukoliv nehodu nebo incident popsat v kontextu zpětnovazebního řízení a v tomto popisu nalézt příčiny, proč systém selhal jako celek. Teorie zde tvrdí, že nemůže nastat žádná nehoda nebo incident (a tedy i běžné události v provozu) bez toho, aby došlo k selhání tzv. řídící struktury, tedy sítě vzájemně propojených řídících smyček. Model STAMP odvádí bezpečnostního analytika od základní interpretace dat o bezpečnosti pomocí deskriptivní statistiky (průměr, trend nebo odchylka v počtu výskytů typů událostí za jednotku času) a nutí ho konstruovat popis (reprezentaci) systému, který data vytvořil. Toto ve výsledku umožňuje, aby bezpečnostní analytik uvažoval systém jako celek. Vytvořený popis systému zároveň přímo podporuje analýzu, jak podobným situacím předcházet.

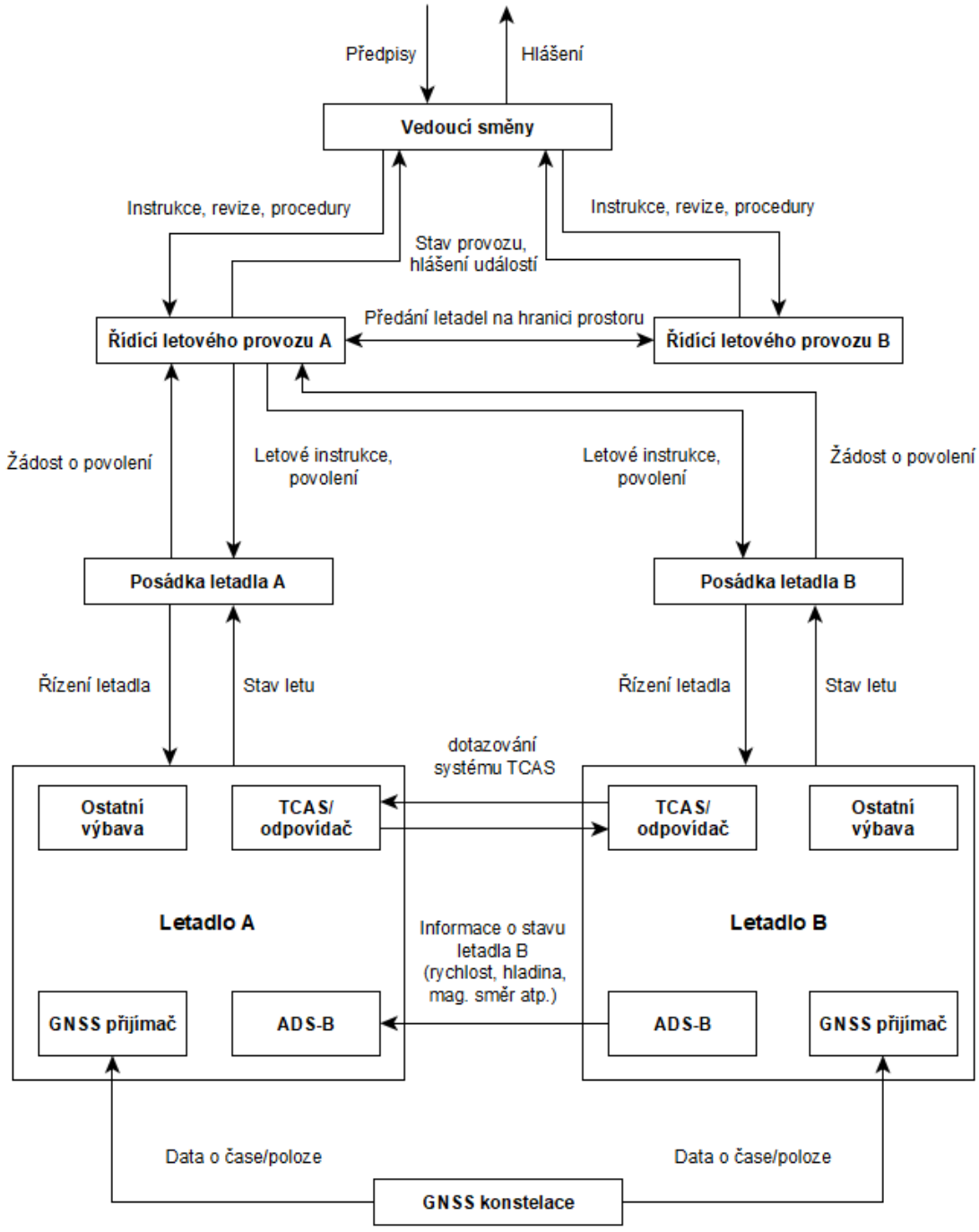


Obr. 1 Řídící smyčka dle teorie zpětnovazebního řízení (upraveno a přeloženo z [4])

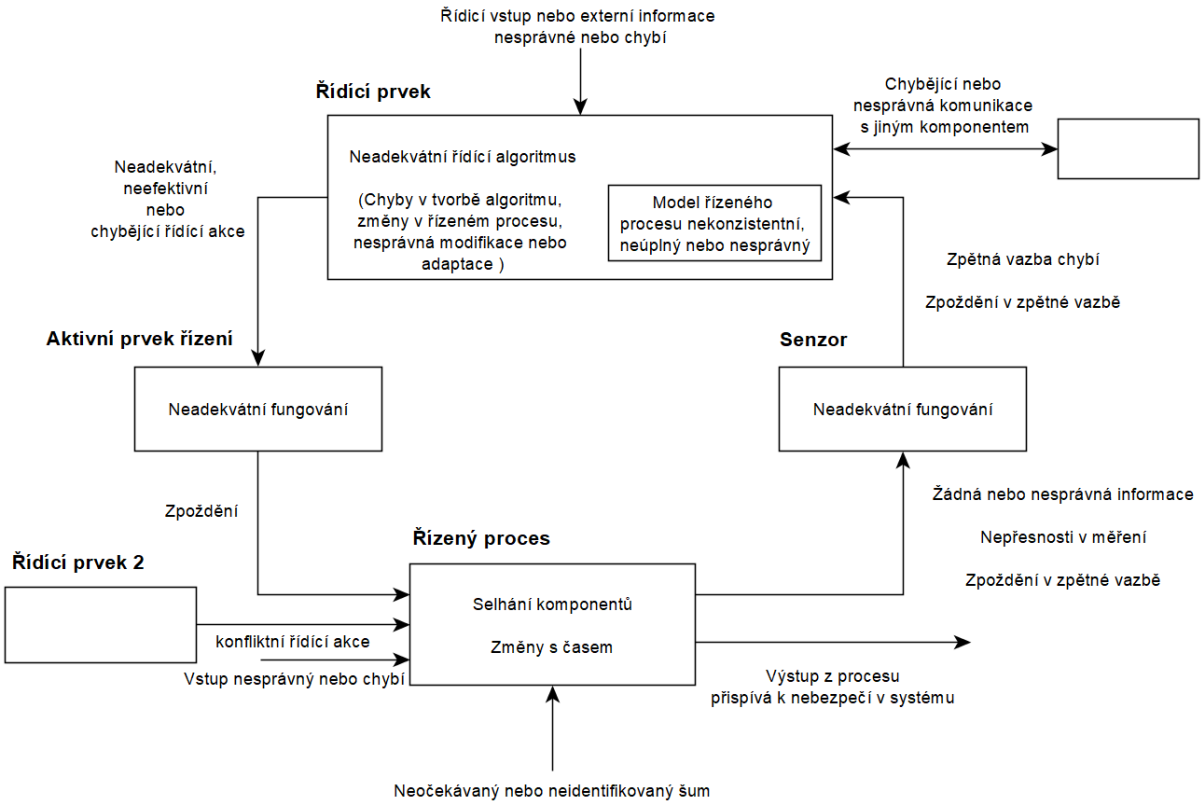
Z výše uvedeného je patrné, že všechny metody založené na teorii STAMP vyžadují, aby v každé analýze bezpečnosti byla zobrazena relevantní část systému, kterou je třeba hodnotit z pohledu bezpečnosti právě pomocí řídících smyček. Jak je vidět z obrázku výše, toto vede ke tvorbě objektového diagramu, který popisuje hodnocený systém z pohledu rolí a odpovědností (tedy řídících prvků) a nástrojů (aktivní prvky řízení, senzory), které se využívají k řízení bezpečnosti. Postupnou specifikací a propojováním sady řídicích smyček je možné vytvořit podrobný popis (reprezentaci) systému, tedy celkovou řídící strukturu, která může být zobecněná pro vytvoření funkčního popisu systému, a ne pouze objektového. Jednoduchý příklad řídící struktury z domény letecké dopravy je zobrazen na obr. 2.

K provedení analýzy bezpečnosti se pak využívá kombinace vytvořeného popisu systému s obecným schématem identifikace nebezpečí, resp. s taxonomií bezpečnostních problémů, které teorie modelu STAMP obsahuje (viz obr. 3 a 4). V tomto dokumentu jsou uvedeny obě varianty schématu pro identifikaci nebezpečí (základní i rozšířená) a také základní taxonomie bezpečnostních problémů, kterou teorie STAMP využívá. Teorie tímto zajišťuje úplnost

analýz, jelikož všechny bezpečnostní problémy, které nejsou vyloučené v reálném provozu, by měly být zváženy v kontextu daného popisu systému, resp. řídící struktury a potenciálních kauzálních scénářů které mohou vést k nehodám a incidentům. V některých případech je samotný popis systému postačující pro identifikaci bezpečnostních problémů.



Obr. 2 Příklad řídící struktury dle modelu STAMP v letecké dopravě - situace znázorňuje dvě letadla (A, B) řízené řídícím letového provozu A, kde letadlo B následuje letadlo A na trati. (upraveno a přeloženo z [5])



Obr. 3 Základní schéma identifikace nebezpečí a taxonomie problémů bezpečnosti dle STAMP (upraveno a přeloženo z [4])

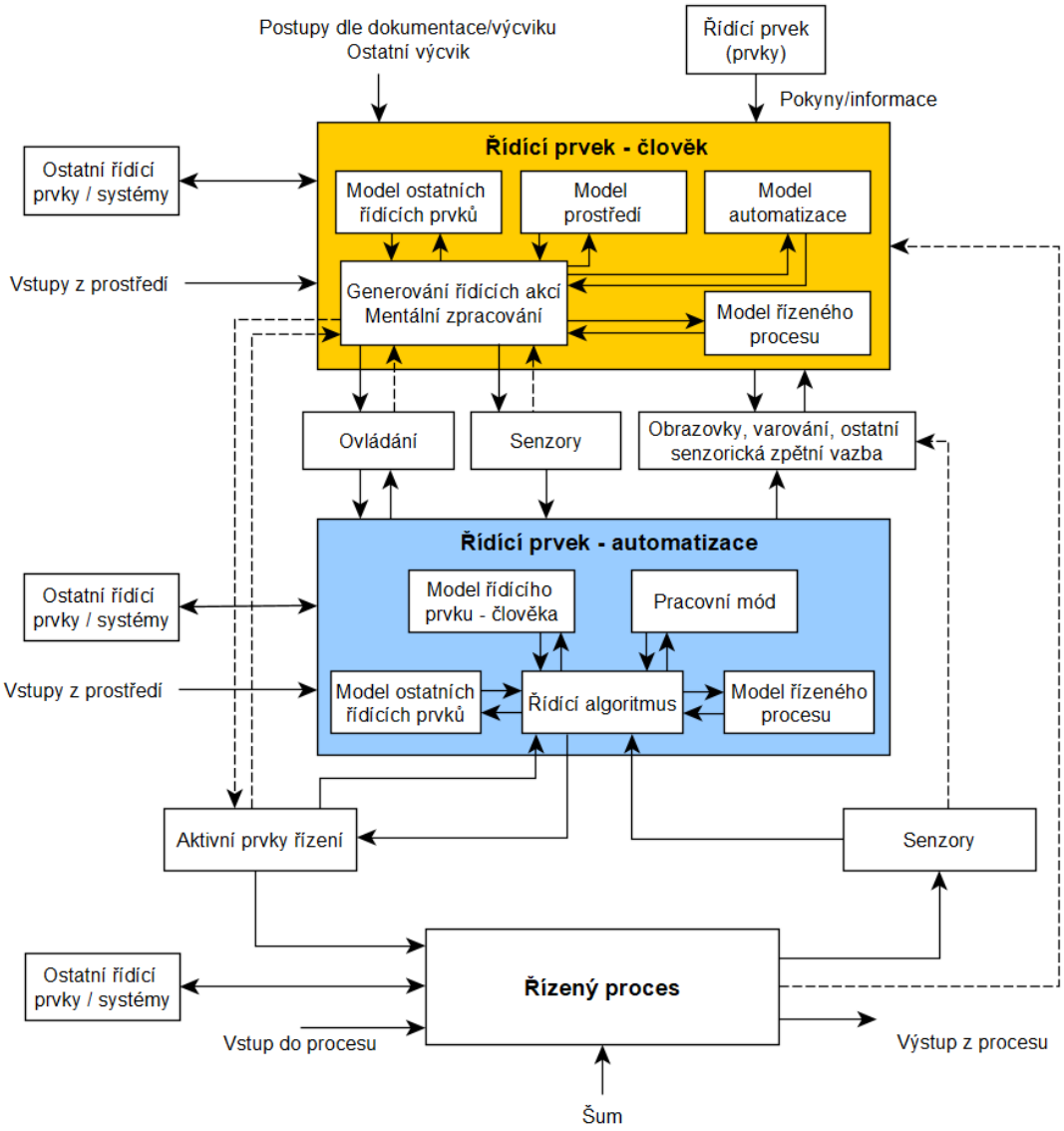
V kontextu bezpečnostních studií, autoři modelu STAMP vyvinuli metodiku analýzy nebezpečí STPA (System-Theoretic Process Analysis), která podporuje praktické využití teorie modelu STAMP průmyslovými uživateli. Jak již bylo zmíněno, tato metodika vyžaduje vytvoření popisu řízeného systému (řídící struktury) a následně jeho analýzu. Metodika STPA sestává konkrétně z následujících kroků [5]:

1. Identifikace cíle (zaměření) analýzy
2. Tvorba popisu systému (diagramu smyček řízení)
3. Identifikace nebezpečí
4. Identifikace scénářů, při kterých může nastat nehoda nebo incident

K zajištění správného výběru části systému nebo části několika systémů a jejich rozhraní slouží krok 1. Z praktických důvodů je vhodné, aby v kroku 2 vznikl diagram pouze vybrané části systému nebo systémů a jejich rozhraní, jelikož úplný popis reality může být značně náročný na realizaci a v kontextu samotné studie bezpečnosti nemusí být využitelný. Krok 3 je následně založen na analýze všech elementů a vazeb v diagramu smyček vytvořeného v kroku 2 pro identifikaci nebezpečného řízení. Krok 4 pak vede k tomu, aby byl analyzován celkový diagram, se zaměřením na možné cesty selhání systému jako celku v důsledku realizace konkrétních scénářů.

Kromě identifikace nebezpečí, které vychází v teorii STAMP ze základního vnímání problému bezpečnosti jakožto problému řízení, je zde ještě otázka hodnocení rizika. STAMP v tomto ohledu využívá matici rizik s tím rozdílem, že autoři teorie navrhují nepoužívat parametr pravděpodobnosti, pokud ho nelze určit s jistotou (ať už kvantitativně, nebo kvalitativně). Za obzvlášť problematický se v této teorii považuje odhad pravděpodobnosti v případech, kdy se

hodnotí neexistující systém a v kontextu kterého neexistují žádná historická data, která by mohla sloužit jako základ pro odhad budoucí pravděpodobnosti. V takovém případě se považuje jakýkoliv odhad pravděpodobnosti za nepodložený, a tedy zcela jistě neodpovídající realitě.



Obr. 4 Rozšířené schéma pro identifikaci nebezpečí dle teorie modelu STAMP. Kombinací základní taxonomie bezpečnostních problémů z obr. 3 a vyobrazeného rozšířeného schématu lze vytvořit rozšířenou taxonomii bezpečnostních problémů dle STAMP. Přerušované čáry znázorňují vazby, které nemusí v systému existovat, jejich implementace je však na zvážení v kontextu zvýšení úrovně bezpečnosti (upraveno a přeloženo z [5]).

Jako řešení problému pravděpodobnosti teorie modelu STAMP nabízí dvě rámcová řešení. Prvním rámcovým řešením je vytvoření sady otázek nebo posuzovacích kritérií, na které lze odpovědět lépe než na otázku, jaká bude pravděpodobnost výskytu konkrétního typu problému v budoucím provozu. Příkladem takových otázek může být: (1) Povede navrhovaná změna k potřebě zavedení nových opatření pro zmírnění rizika? (2) Povede navrhovaná změna k novým funkcím, které mají potenciál redukovat efektivitu současné strategie pro řízení rizik? (3) Jsou související módy selhání a příčiny nebezpečí v navrhované změně stejné, nebo se liší? (4) Jaký je rozsah změny v nárocích na zkušenost řídících prvků? atp. Otázky

by měly být vytvořeny pro každý případ bezpečnostní studie tak, aby zohledňovaly její kontext a relevantní řídící strukturu. Jak je patrné z tohoto rámcového řešení, bezpečnostní analytik by měl nabýt jistotu o přijatelné míře rizika v navrhovaném systému z celkové sady otázek a odpovědí. Odpovědi by tak měly vytvořit veškerý racionál pro předpoklad, že v systému nejsou známa žádná nepřijatelná rizika. Samozřejmě toto nevylučuje potřebu sledování dalšího vývoje a následně provozu, který by měl potvrdit správnost předpokladů z realizované bezpečnostní studie.

Druhým rámcovým řešením je použití nové proměnné - tzv. potenciálu pro zmírnění rizika - jako náhrady resp. odhadu neznámé pravděpodobnosti [8]. Tento potenciál hodnotí každé identifikované nebezpečí z pohledu možností pro jeho zmírnění. Nejvíce žádoucí je stav, kdy se v systému nachází pouze nebezpečí, kterých riziko je možné eliminovat nebo zmírňovat přímo v návrhu systému, resp. v provozu, a nevyžadují komplikovaná, nebo značně nákladná opatření pro zmírnění. V takovémto systému se řídí rizika jednoduše a ze samotného návrhu je zřejmé, že nehody a incidenty budou v systému vznikat jen obtížně.

Volba konkrétního rámcového řešení závisí na konkrétní studii bezpečnosti, resp. konkrétním systému pro posouzení. Teorie zde v systémech s neznámou pravděpodobností nevylučuje ani použití obou rámcových přístupů k hodnocení rizik najednou. Ve všech případech však platí, že studie bezpečnosti by měla být realizována opakovaně v průběhu celkového návrhu změny nebo nového systému, který má být zaveden do provozu. Důvodem pro opakované provedení studie bezpečnosti je riziko, že v pozdějších fázích návrhu změny nebo tvorby nového systému může být implementace opatření pro zmírnění rizika značně nákladná, ne-li nemožná a častokrát i málo efektivní. Naopak v dřívějších fázích hodnocení změny nebo návrhu nového systému je zpravidla možné vybírat mezi několika alternativami a včas tak volit návrh, který nebude z pohledu bezpečnosti problematický v pozdějších fázích. Nejvhodnější se jeví opakované provedení studie bezpečnosti vždy po dosažení klíčových milníků v projektu návrhu změny nebo tvorby nového systému, jako je stanovení cíle, principů návrhu, dosažení základní architektury systému nebo návrhu konkrétní fyzické reprezentace [4]. Opakované provedení studie bezpečnosti je však vždy závislé na druhu konkrétního projektu a teorie zde nestanovuje všeobecně platný postup pro jakýkoliv projekt.

3.2 Procesní model letiště

Teorie modelu STAMP, stejně jako i metodiky navrženy jejími autory, pracují s předpokladem, že je potřeba vytvořit ad-hoc popis systému při každé analýze. Důvodem pro tento předpoklad je skutečnost, že neexistuje praktický způsob správy aktuálního popisu systému v reálném čase, který by předem poskytl všechny potřebné detaily pro analýzy založené na teorii STAMP. Nicméně, s postupným vývojem a nabýváním praktických zkušeností s modelováním firemních a obchodních procesů (tzv. business process modeling) se objevují nové možnosti, které by umožnily tvorbu a správu takového popisu systému nebo alespoň jeho významné části. Toto je klíčovým předpokladem této metodiky, která tím vytváří nové možnosti pro budoucí metodiky založené na teorii STAMP.

Na základě nového předpokladu výše je vymezení systému možné právě na základě modelování procesů, zde konkrétně letiště. Procesy, které nejsou detailně zdokumentovány v provozní dokumentaci lze považovat za okolní prostředí systému. Na druhé straně takový systém může být příliš robustní, a proto by měla být zvážena možnost jeho dekompozice nebo

filtrování dle obsahu konkrétní bezpečnostní analýzy. Toto je možné provést s pomocí samotné definice procesů; každá analýza je obsahově zaměřená na vybrané procesy organizace, a tedy všechny ostatní procesy se v takové analýze stávají okolním prostředím zájmového systému. Toto vede k pružnosti bezpečnostních analýz realizovaných dle této metodiky.

Při detailním pohledu představuje proces logicky uspořádanou posloupnost či souslednost činností, které přinášejí užitek. Business process modelling je nástroj, pomocí kterého lze popsat logickou strukturu jednotlivých aktivit uvnitř organizace a jako takový nabízí možnost tvorby funkčního popisu systému (tedy popisu toho, co konkrétní systém dělá, než čím je). Komplexní pohled na činnosti uvnitř organizace umožňuje jejich důkladnou analýzu a usnadňuje pochopení funkčních souvislostí a zákonitostí v systému.

Výhodou procesního modelu je možnost dekompozice, která přináší vyhodnocení podprocesů, často až na úrovni jednotlivých činností, s potenciálem měření jejich efektivity. Detailní zaměření na aktivity v procesu může být při tvorbě studie bezpečnosti velmi přínosné. Další výhodou procesního přístupu je skutečnost, že přináší vhodné vstupy pro analýzu systému při zavádění změn.

Jak již bylo zmíněno v předešlé kapitole, STAMP nabízí metodiku STPA jako technický nástroj pro analýzu nebezpečí, který může být využit v studiích bezpečnosti. Navržená metodika v tomto dokumentu vychází z jiného přístupu, který však vede ke stejným výsledkům jako aplikace STPA. Počátečním krokem v této metodice je tvorba procesní dokumentace jako úplného funkčního popisu systému. V případech, kdy takový popis není možné vytvořit, je vhodné aplikovat konvenční postup STPA. Pokud taková dokumentace existuje nebo může být vytvořena, pak je dále nutné jí propojit se základními koncepty (objekty) z teorie modelu STAMP. Přesah standardní procesní dokumentace dle business process modeling a teorie modelu STAMP je přímočarý: každý (pod)proces má odpovědné osoby (role) pro každou definovanou aktivitu nebo úkol. Tato odpovědná osoba se stává řídícím prvkem a konkrétní aktivita resp. úkol se stává řízeným procesem. Procesní model je tedy třeba doplnit pouze o sadu aktivních prvků řízení, kterými může řídící prvek řídit daný proces a sadu senzorů, pomocí kterých je zajištěna zpětnovazební linka. Z toho vyplývá, že řídící prvky jsou vymezeny právě množinou aktivních prvků řízení a množinou senzorů, které jsou pro řízení daného procesu k dispozici. Konkrétní příklad aplikace principů zpětnovazebního řízení do modelovacího nástroje uvádí obr. 5. Z něj je patrné, že pro popis množiny aktivních prvků řízení byl využit atribut odpovědné role “Particular responsibilities” a pro popis množiny senzorů atribut odpovědné role “Particular recommendations”. Tento a následující příklady byly vytvořeny v nástroji pro modelování firemních procesů Adonis[1] a zmiňované atributy byly vybrány jako nejvhodnější pro zápis informace o aktivních prvcích řízení a senzorech. Zmiňované příklady však slouží pouze pro ilustrativní účely a v žádném případě nejsou cílené na propagaci nebo podporu využití tohoto konkrétního software pro aplikaci metodiky. V případě použití jiných nástrojů může být vhodné využití resp. zavedení jiných atributů pro vkládání této informace.

Dle koncepce modelu bezpečnosti STAMP dochází k nehodám v důsledku externích poruch, selhání součástí systému nebo disfunkčních interakcí mezi komponentami systému, a to

[1] https://www.adonis-community.com

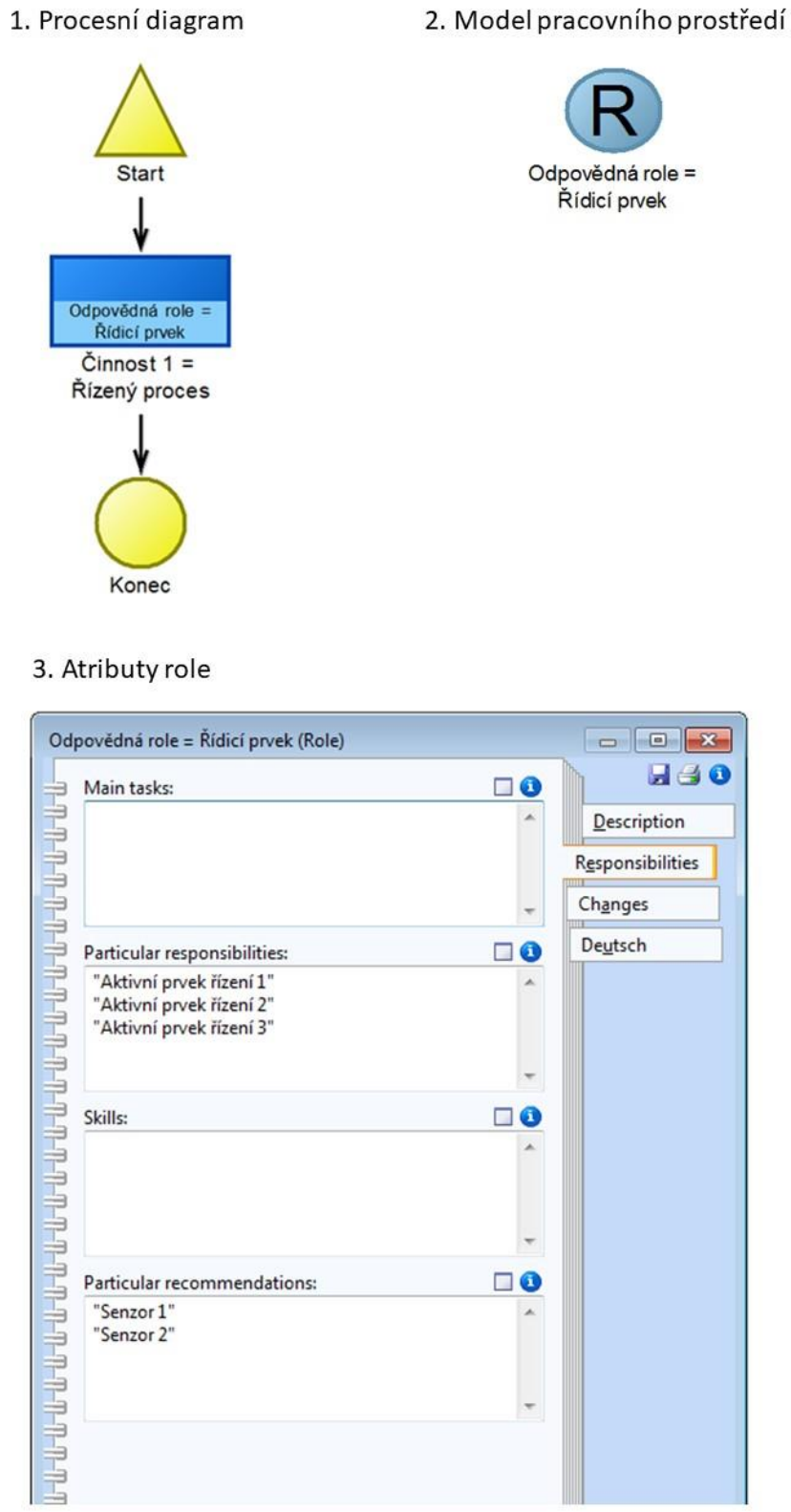
pokud nejsou řídící strukturou řádně ošetřeny. Lze tedy konstatovat, že nehody vyplývají z nedostatečného řízení a bezpečnost je považována za záležitost správně nastavené řídící struktury. Zabránění budoucím nehodám vyžaduje navržení takové řídicí struktury, která dostatečným řízením udrží činnosti v potřebných mezích. Odchylka od předpokládaného chování v řízeném systému (tedy rozdíl mezi tím, jak je práce popsána v provozní dokumentaci a jak se ve skutečnosti realizuje) je v této metodice nazývána deviací.

Deviace jsou v této metodice klíčovým konceptem a jsou definovány jako odchylky od vymezených činností, které mají potenciál přispět k nehodě. Deviace by měly být stanoveny pro každou aktivitu v procesním modelu, tedy pro každou řídicí smyčku. Stanoví je expert uvažujíc analyzovaný systém nebo jeho část (tedy analyzované procesy s jasně vymezenými procesy okolního prostředí) v konkrétní analýze a dále uváží možné nehody a incidenty, které mohou nastat na úrovni konkrétního systému. Při tvorbě bezpečnostní studie je třeba prověřit, že řídící smyčka je nastavena správně tak, aby mohla reagovat na každou z možných deviací, to znamená, že realizace deviace je identifikovatelná některým ze sady senzorů a že lze činnost některým ze sady řídících prvků vrátit zpět do přípustných mezí. Jelikož lze deviace chápat jako odchylky od aktivit v rámci jednoho procesního kroku, i jejich zápis v modelu se váže na jednotlivé činnosti. Deviace mohou být zaznamenány pomocí atributů dostupných k detailnímu popisu aktivit v procesech. Tyto atributy jsou obvykle dostupné v modelovacích nástrojích pracujících s BPMN (obr. 6. ilustruje využití atributů v prostředí nástroje Adonis).

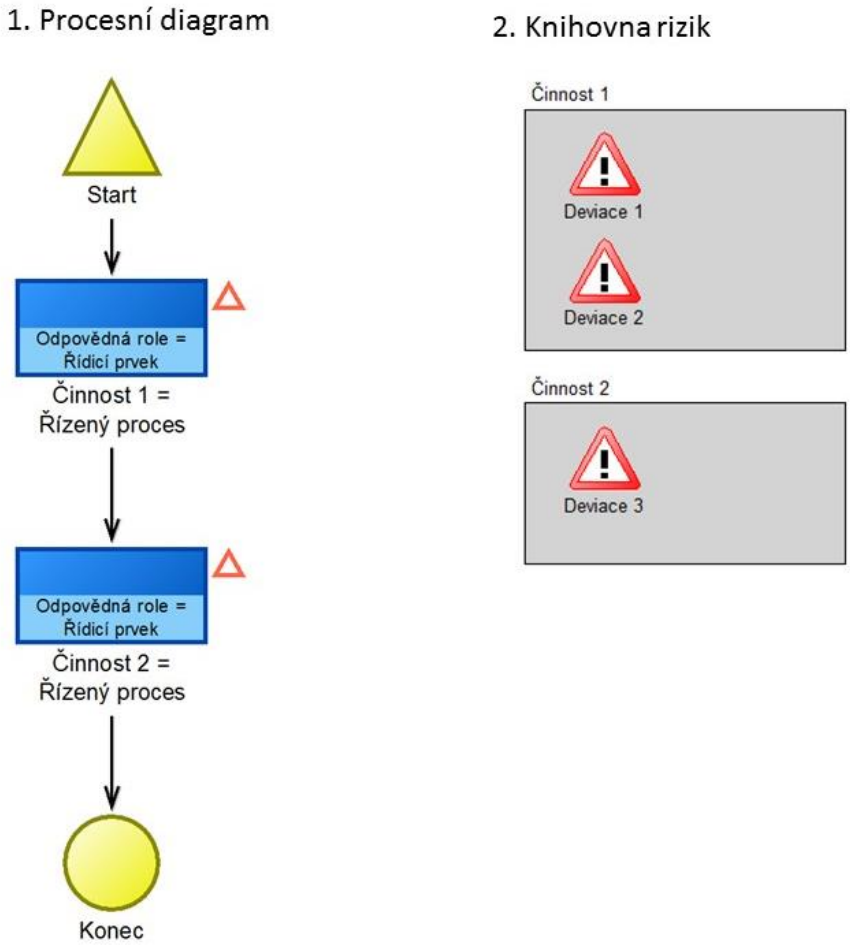
Seznam deviací je základem pro identifikaci nebezpečí. Potenciální nebezpečí jsou identifikována pomocí analýzy procesů bezpečnostním analytikem, který ohodnotí jednotlivé kroky procesu a definuje jejich nejhorší možný následek. Procesní model sestává z logicky uspořádaných kroků procesu, který reprezentuje tok činností jednotlivého procesu, tudíž identifikovaná nebezpečí nemusí být striktně vázána na konkrétní krok procesu, ale jsou často společná pro několik kroků. Konkrétní krok procesu resp. skupina kroků procesu, vůči kterým je nebezpečí relevantní, by měla být identifikována na základě předem zjištěných deviací. Praktický příklad navrhovaného postupu identifikace nebezpečí je uvedený v kapitole 3.6. Identifikace nebezpečí z pohledu systému jako celku znamená analýzu na vyšších úrovních systému, kde se uvažují pouze závažné následky. Proaktivní přístup k bezpečnosti a k jejímu řízení však znamená soustředění pozornosti především na deviace.

Seznam příslušných deviací lze vytvořit systematicky například pomocí řídící dokumentace, kde jsou pečlivě popsány jednotlivé kroky, které musí být dodrženy pro správný a bezpečný průběh konkrétního procesního kroku. Daná instrukce, pokud je provedena špatně nebo není provedena vůbec, je právě hledanou deviací. Vhodnou pomůckou pro tvorbu seznamu deviací je systematické obsazování jednotlivých kategorií deviací dle teorie STAMP, tedy pomocí základního schématu identifikace nebezpečí z obr. 3 a 4.

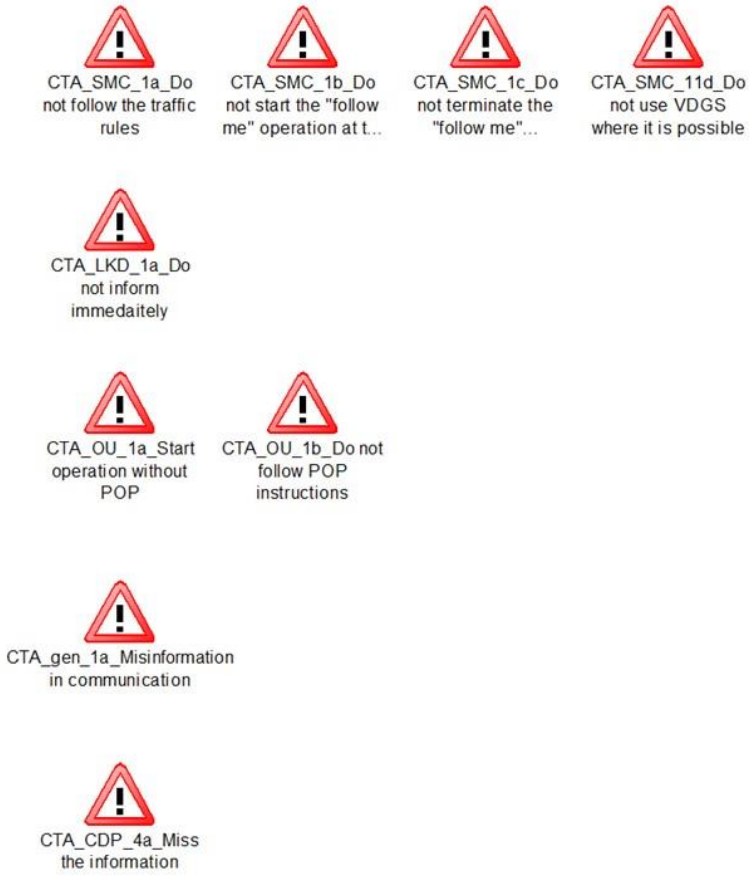
Vzniklé knihovny modelovacího nástroje následně poskytují bezpečnostnímu analytikovi další pohled na systém nebo jeho část. Například v knihovně rizik lze získat seznam všech deviací vyskytujících se v jednom procesu, jak uvádí příklad na obr. 7. Podobně lze využívat knihovnu rolí pro náhled na množinu řídících prvků, jak uvádí příklad na obr. 8.



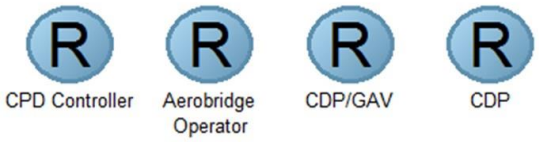
Obr. 5 Využití prostředí nástroje pro modelování provozních postupů pro vkládání informací potřebných pro analýzy založené na modelu bezpečnosti STAMP



Obr. 6 Využití prostředí nástroje pro modelování provozních postupů pro vkládání informací o deviacích od vymezených činností v procesech



Obr. 7 Ukázka seznamu deviací extrahovaných z procesního modelu



Obr. 8 Ukázka seznamu řídících prvků extrahovaných z procesního modelu

3.3 Rozhraní systému

Modelování procesů je také nástrojem, který pomůže organizaci začlenit vlastní procesy do okolního prostředí v kontextu rozhraní s jinými organizacemi. Tato rozhraní jsou pro řízení provozní bezpečnosti velmi podstatná. Je nezbytné si uvědomit, že provozovatel letiště se nachází ve specifické situaci, kdy odpovídá za udržení požadované úrovně provozní bezpečnosti, ale za většinu procesů odehrávajících se na provozní ploše neodpovídá, resp. tyto procesy sám neřídí. Zde se totiž na letištní infrastruktuře odehrávají procesy, které spadají do odpovědnosti jiných subjektů působících na letišti - např. provozovatele letadla, handlingové společnosti, plnicí společnosti, cateringové společnosti apod. Kromě procesů, které přímo spadají do odpovědnosti provozovatele letiště lze proto nalézt procesy, ve kterých dochází k interakci mezi provozovatelem letiště a dalším subjektem a také procesy, ve kterých nevystupuje žádný řídící prvek letiště.

Procesy okolního prostředí analyzovaného systému nebo jejich části sice nespadají do odpovědnosti provozovatele letiště, je však rovněž vhodné je analyzovat dle představované metodiky. Od popisu procesů a příslušné řídící struktury provozovatele letiště se pak neliší principiálně, ale pouze úrovní detailu, do které může být analýza zpracována. Řídící smyčky v procesních krocích, za které není odpovědný provozovatel letiště, lze zpracovat jenom na generické úrovni dle teorie STAMP a základní znalosti procesu.

3.4 Popis hodnocení deviace

Seznam deviací tak, jak je znázorněn na obr. 7, představuje základ pro identifikaci nebezpečí a tak jako nebezpečí samotná, i deviace musí být ohodnoceny z pohledu rizika. Identifikace nebezpečí zde ale probíhá na základě modelu STAMP pomocí identifikace deviací od navrhovaného chování systému na úrovni řízených procesů a jednotlivých aktivit, hodnocení deviací je tedy prioritnější a metodika se zabývá právě tímto hodnocením. V metodice je tedy hodnocení rizika vázáno na hodnocení zmíněných deviací a konkrétní kvantitativní postupy, jak toho dosáhnout, jsou uvedeny v této kapitole. Hodnocení rizika nebezpečí je založeno na stejném principu, nicméně důsledným hodnocením deviací je toto provedeno zároveň a nebezpečí pak nemusí být hodnocena samostatně.

Hodnocení každé deviace je v této metodice rozděleno do čtyř kritérií: závažnost, řiditelnost, detekovatelnost a časová rezerva. Tato čtyři kritéria jsou navzájem nezávislá. Výsledkem hodnocení není jedno souhrnné číslo vyjadřující riziko související s konkrétní deviací, ale vektor indexů vyjadřující kritičnost deviace v kontextu rizika, které deviace v řízeném systému jako celku vytváří. V posouzení vyžaduje od hodnotitele podrobné znalosti o systému a provozu, který je hodnocen.

Každá z deviací je hodnocena vektorem indexů. Jednotlivé složky vektoru jsou závislé na kritériích hodnocení a takovéto rozdělení poskytuje nejen podrobnější pohled na slabé stránky hodnoceného systému, ale také navádí bezpečnostního analytika, jakým způsobem lze hodnocený systém zlepšit z pohledu rizika.

3.4.1 Kritéria pro hodnocení deviací

Tato kapitola detailně popisuje kritéria, která hodnotí jednotlivé deviace. Následující kapitoly pak popisují celkový proces hodnocení procesu a systému a pro srozumitelnost je v další kapitole uvedena i ukázka hodnocení na konkrétních letištních procesech.

1. **Kritérium – Závažnost (Severity)**

Toto kritérium posuzuje nejhorší potenciální událost, ke které může dojít v případě, že deviace nastane.

Kvantitativní hodnocení zachovává obvyklý způsob hodnocení rizika z leteckého průmyslu. Závažnost je však na rozdíl od současných standardů hodnocena dle dopadu na čtyři skupiny, konkrétně lidé, technika, prostředí a provoz. Každá ze skupin má určenou vlastní škálu hodnocení.

Hodnocení dopadu nejhorší potenciální události na cestující nebo pracovníky je navrhováno podle škálování, které uvádí tab. 1 [9,10]. Hodnocení dopadu nejhorší potenciální události na životní prostředí a infrastrukturu je řízeno škálou, kterou uvádí tab. 2 [9]. Hodnocení dopadu nejhorší potenciální události na leteckou a pozemní techniku uvádí tab. 3 [11]. Hodnocení dopadu nejhorší potenciální události na provoz je určeno škálou dle tab. 4.

Tab. 1 Škála pro hodnocení dopadu nejhorší potenciální události na cestující nebo pracovníky - skupina lidé

Bez efektu	1
Snížení komfortu cestujících nebo pracovníků	2
Výrazné snížení komfortu cestujících nebo pracovníků	3
Potenciální lehká zranění cestujících nebo pracovníků	4
Hazardní scénář ohrožení života nebo vážného zranění	5

Tab. 2 Hodnocení dopadu nejhorší potenciální události na životní prostředí a na infrastrukturu - skupina prostředí

Žádný nebo minimální dopad na prostředí lokálního charakteru, případný minimální dopad je jednoduše odstranitelný bez nutnosti investovat velké množství zdrojů	1
Výrazný dopad na prostředí rozsáhlého charakteru, který je odstranitelný s nutností investovat velké množství zdrojů	3
Výrazný dopad na prostředí rozsáhlého charakteru, který není odstranitelný nebo vyžaduje zásah mimo organizaci	5

Tab. 3 Hodnocení dopadu nejhorší potenciální události na leteckou a pozemní techniku - skupina technika

Bez efektu	1
Pozemní technika je provozuschopná se sníženou výkonností	2
Pozemní technika je provozu neschopná, ale opravitelná	3
Pozemní technika je provozu neschopná a neopravitelná nebo dochází k poškození letadlové techniky - NO AOG	4
Poškození letadlové techniky AOG	5

Tab. 4 Hodnocení dopadu nejhorší potenciální události na provoz - skupina provoz

Bez efektu	1
Minimální dopad na pozemní provoz	2
Dopad na pozemní provoz způsobující menší zpoždění více letů	3
Výrazné zpoždění více letů	4
Zrušení letu nebo výrazné zpoždění velkého množství dalších letů	5

2. Kritérium – Detekovatelnost

Detekovatelnost stanovuje pravděpodobnost správné detekce deviace v systému ještě předtím, než má deviace dopad na proces nebo na systém. Hodnota detekovatelnosti vyjadřuje schopnost systému správně a včas detekovat své selhání a odchýlení od bezpečného režimu. Hodnotící škálu uvádí tab. 5.

Tab. 5 Hodnocení detekovatelnosti deviace

Vysoká pravděpodobnost detekce možné deviace ještě předtím, než nastane	1
Pravděpodobná detekce deviace bezprostředně předtím, než nastane	2
Deviace je detekována ve chvíli, kdy nastane	3
Deviace je detekována až v jejím průběhu	4
Deviace není detekována, nebo je detekována velice pozdě	5

3. Kritérium – Řiditelnost

Řiditelnost vyjadřuje vlastnost systému včasně reagovat na deviaci a vrátit proces do běžného a tedy bezpečného režimu s využitím přípustných vstupů, tedy pomocí aktivního řízení vzniklé situace. Zahrnuje existenci účinných a vhodných opatření pro kontrolu nebo zastavení deviace nebo snížení následků na nejnižší možnou mez, resp. přijatelnou úroveň. [12] Hodnotící škálu uvádí tab. 6.

Tab. 6 Hodnocení řiditelnosti

Deviace je plně automaticky řiditelná - s využitím automatizace	1
Deviace je jednoduše řiditelná	2
Deviace je obtížně řiditelná	3
Při deviaci je řiditelné pouze snížení následků	4
Deviace není řiditelná	5

4. Kritérium – Časová rezerva

Hodnocení tohoto kritéria cílí na hodnocení rozdílu času alokovaného na proces a času potřebného na správné provedení procesu. Tento rozdíl nazýváme časovou rezervou. Dostatečná časová rezerva, tedy situace, kdy pracovník není pod časovým tlakem, nemá vliv na deviaci, která v procesu může nastat.

Malá, žádná nebo dokonce záporná časová rezerva způsobuje stresovou situaci, která zvyšuje pravděpodobnost vzniku deviace. Vzhledem ke konfliktu cílů, kdy aktivitu je potřeba navzdory nedostatku času vykonat, je tím pracovník podvědomě tlačen k nedodržení procesu nebo nedostatečné kontrole svých kroků a tedy k nižší kvalitě práce. Toto vede ke vzniku deviace během řízeného procesu. Škála, která se v této metodice využívá k hodnocení časové rezervy, je zobrazena v tab. 7.

Tab. 7 - Hodnocení časové rezervy

Proces není časově omezen	1
Proces má komfortní časovou rezervu	2
Proces má minimální časovou rezervu	3
Proces nemá žádnou časovou rezervu	4
Proces má zápornou časovou rezervu (čas potřebný na provedení procesu je delší, než je čas k dispozici)	5

3.4.2 Vlastní hodnocení deviací

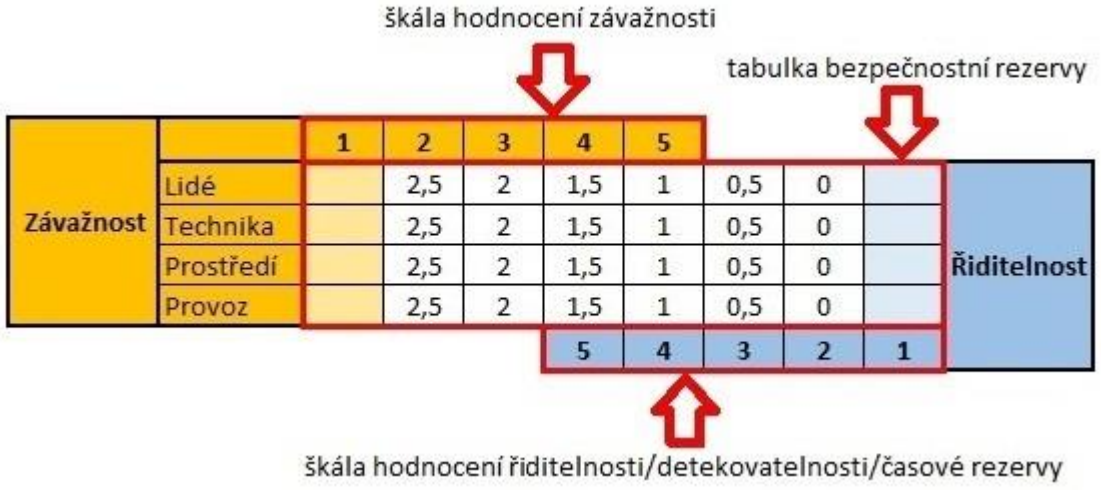
Vlastní hodnocení deviací vyžaduje stanovení tří indexů, které tvoří výsledný vektor hodnocení deviace. Stanovení uvedených indexů vychází z funkční korelace kritéria závažnosti vůči ostatním kritériím. Závažnost je jako kritérium podobné standardní matici rizik. Naproti tomu ostatní tři kritéria posuzují schopnosti řídicího systému vytvořeného za účelem předcházení nebo řízení odchylky. Závažnost je proto porovnávána s těmito kritérii tak, aby se obě posuzovali v jediném kontextu, tj. v kontextu potenciálního dopadu deviací a možností jejich prevence. Toto je postaveno na základní myšlence metodiky a teorie STAMP, že bezpečnost je otázkou řízení systému. Během posuzování rizik by proto měla být vyhodnocena schopnost řídícího systému adekvátně identifikovat a řídit problémy bezpečnosti. To je také hlavní důvod, proč jsou kritéria nadále hodnocena v matici.

Následující indexy je potřebné vyhodnotit z pohledu schopnosti detekovat a řídit deviace:

- Index řiditelnosti
- Index detekovatelnosti
- Index časové rezervy

K znázornění funkční korelace lze využít následující tabulku (tab. 8), zde konkrétně s indexem řiditelnosti.

Tab. 8 Tab. funkční korelace kritéria závažnosti vůči kritériu řiditelnosti



V levé horní straně tabulky je znázorněno kritérium závažnost s jednotlivými skupinami (lidé, technika, prostředí a provoz) a samotné hodnocení (škála) je orientována zleva doprava. Na pravé dolní straně je uvedeno kritérium řiditelnosti, u kterého se hodnocení provádí zprava doleva. Kromě tohoto kritéria se stejným způsobem provádí hodnocení pro další dvě kritéria detekovatelnosti a časové rezervy. Centrální část tabulky tvoří tzv. bezpečnostní rezerva. Bezpečnostní rezerva je určena součtem hodnot z nevybarvených polí centrální části tabulky a reprezentuje tedy pomyslnou bezpečnostní rezervu v řízení konkrétní deviace. Hodnota takto vypočtené rezervy se stává hodnotou konkrétního indexu, zde indexu řiditelnosti. Tabulka bezpečnostní rezervy nabývá hodnot od 0 do 2,5. Stanovení těchto konkrétních hodnot je pouze doporučením a uživatel je může upravovat dle vlastní potřeby. Tab. 8 nicméně již byla kalibrována v prostředí letišť a vede k přesným výsledkům v celkovém hodnocení.

V případě úpravy hodnot centrální části tabulky je třeba zachovat základní pravidla:

- Hodnoty zleva doprava mají vždy klesající trend, v této metodice se jedná o aritmetickou posloupnost. Tímto je zajištěno, že v případě nízké závažnosti a nízké řiditelnosti je zde ještě dostatečná bezpečnostní rezerva (přijatelné riziko). Toto nastavení hodnot bezpečnostní rezervy preferuje kritérium závažnosti pomocí vyšší váhy.
- Nejnižší hodnotou v tabulce bezpečnostní rezervy je 0
- Maximální hodnota bezpečnostní rezervy je součet všech rezerv, když obě korelovaná kritéria jsou hodnocena stupněm 1 dle škál
- Minimální hodnota bezpečnostní rezervy je negativní hodnota překrývající se části dvou korelovaných hodnocení
- Pokud dojde k překryvu v jakékoliv části tabulky, jako výsledný index se počítá pouze negativní hodnota uvedená v tomto překryvu
- Pokud je hodnota jedné nebo více skupin závažnosti vyšší o dva nebo více stupňů, hodnoty v ostatních nižších stupních se vynásobí tzv. faktorem (stanoveným koeficientem)

Pro názornost a lepší pochopení jsou v následujících tabulkách znázorněny různé scénáře výpočtu a je vysvětleno zachování uvedených pravidel.

Tab. 9 Maximální hodnota indexu při nejvyšší závažnosti a nejlepším stavu řiditelnosti

Závažnost		1	2	3	4	5				Řiditelnost
	Lidé						0,5	0		
	Technika						0,5	0		
	Prostředí						0,5	0		
	Provoz						0,5	0		
					5	4	3	2	1	

V tab. 9 je uveden příklad situace, kde pro danou deviaci, která má nejvyšší hodnotu závažnosti pro všechny skupiny a zároveň nejlepší (zde nejnižší) hodnotu řiditelnosti, dostáváme výslednou hodnotu bezpečnostní rezervy, tj. indexu řiditelnosti, jako hodnotu 2. Žlutě vybarvená pole centrální části tabulky reprezentují “pohlcení” bezpečnostní rezervy vysokou závažností konkrétní deviace (zde ve všech ohledech hodnocena stupněm 5). Naopak vysoká řiditelnost (hodnocena stupněm 1) centrální pole tabulky zachovává, tedy v tabulce zůstává 8 polí s kumulativním součtem všech hodnot rovnajícím se 2, který tvoří výsledné hodnocení. Tato hodnota je z pohledu řízení rizik hraniční, protože ukazuje na velmi problematickou deviaci z pohledu závažnosti, ale zároveň zahrnuje informaci o dobře nastaveném systému řízení dané deviace.

Následující tab. 10 znázorňuje nejnižší hodnotu bezpečnostní rezervy (indexu). Nejnižší hodnotou je součet negativní bezpečnostní rezervy v oblasti překryvu dvou hodnocení. V tabulce již dochází oproti tab. 9 také k čerpání centrální části modře zabarvenými poli díky nízkému hodnocení řiditelnosti (zde 5 dle škály). Červeně zabarvená pole reprezentují pole, která by byla vybarvena žlutě i modře zároveň a jedná se tedy o nedostatek bezpečnostní rezervy, který se vyjádří kumulativním součtem negovaných hodnot původní centrální části tabulky (zde tedy konkrétně -10).

Tab. 10 Nejnižší hodnota indexu

Závažnost		1	2	3	4	5				Řiditelnost
	Lidé				1,5	1				
	Technika				1,5	1				
	Prostředí				1,5	1				
	Provoz				1,5	1				
					5	4	3	2	1	

V následujících tabulkách je zobrazen princip snižování hodnoty indexu a násobení marginalizovaných hodnot faktorem, tj. koeficientem, který zvyšuje relevantnost nejproblematičtější hodnoty závažnosti.

Tab. 11 Rozdíl v hodnocení závažnosti o jeden stupeň

		1	2	3	4	5			
Závažnost	Lidé			2	1,5	1	0,5		Řiditelnost
	Technika		2,5	2	1,5	1	0,5		
	Prostředí		2,5	2	1,5	1	0,5		
	Provoz		2,5	2	1,5	1	0,5		
					5	4	3	2	1

Z tab. 11 je patrné, že v případě hodnocení závažnosti, kde se hodnoty u jednotlivých skupin liší pouze o jeden stupeň, dochází pouze k odečtení hodnoty indexu.

Tab. 12. Rozdíl v hodnocení závažnosti o dva stupně

		1	2	3	4	5				
Závažnost	Lidé				1,5	1	0,5	0		Řiditelnost
	Technika		0,75	2	1,5	1	0,5	0		
	Prostředí		0,75	2	1,5	1	0,5	0		
	Provoz		0,75	2	1,5	1	0,5	0		
					5	4	3	2	1	

V případě, kdy je rozdíl jednoho nebo více hodnocení závažnosti dva a více stupňů, dochází k násobení hodnot ve všech neobsazených polích předchozího sloupce faktorem, který je stanoven pro uspořádání hodnot rezervy v této metodice jako číslo 0,3. Hodnoty rezervy v příslušném sloupci se násobí faktorem jednou, pokud je rozdíl mezi kteroukoliv dvojicí složek hodnocení závažnosti dva, dvakrát, pokud je tři, a třikrát pokud je rozdíl roven čtyři. V tab. 12 je vidět, že hodnoty v prvním sloupci jsou vynásobeny hodnotou 0,3, zatímco hodnoty v následujícím sloupci zůstaly zachované (rozdíl menší než dva stupně).

Tab. 13. Rozdíl v hodnocení závažnosti o dva a více stupňů

		1	2	3	4	5				
Závažnost	Lidé					1	0,5	0		Řiditelnost
	Technika				1,5	1	0,5	0		
	Prostředí		0,07	0,6	1,5	1	0,5	0		
	Provoz		0,07	0,6	1,5	1	0,5	0		
					5	4	3	2	1	

V tab. 13 je znázorněno násobení faktorem v případě, kdy je hodnocení závažnosti vyšší o dva a více stupňů u více než jedné hodnocené skupiny. V modelové situaci je hodnocení závažnosti pro skupinu lidé vyšší o tři stupně a pro skupinu technika o dva stupně než hodnocení zbývajících dvou skupin. Hodnoty v neobsazených polích sloupce 2 jsou násobeny koeficientem třikrát. Dvakrát jsou násobeny z důvodu, že hodnocení první skupiny je o tři

stupně vyšší, a navíc jedenkrát, protože hodnocení druhé skupiny je o dva stupně vyšší než u zbývajících dvou skupin.

Výsledkem celkového hodnocení deviace je stanovení velikosti bezpečnostní rezervy pro jednotlivá kritéria. Tyto hodnoty následně tvoří složky vektoru výsledného hodnocení. Výsledné hodnocení uvažované deviace *v* je tedy složeno z velikosti stanovených indexů pro kritéria detekovatelnost - *v_1* , řiditelnost - v_2 a časovou rezervu - v_3. tj.:

$$v = (v_1, v_2, v_3)$$

V případě potřeby promítnout do hodnocení deviace parametry jako počasí, nevhodná frekvence procesu, kde se deviace vyskytuje, nebo zvýšená důležitost deviace z pohledu bezpečnosti, je možné velikost bezpečnostní rezervy snížit nebo zvýšit zavedením dalšího koeficientu, kterým se pronásobí centrální pole hodnotící matice. Koeficient parametrů i parametry jsou v takovém případě voleny dle požadavků organizace využívající hodnocení.

3.4.3 Hraniční hodnoty hodnocení deviací

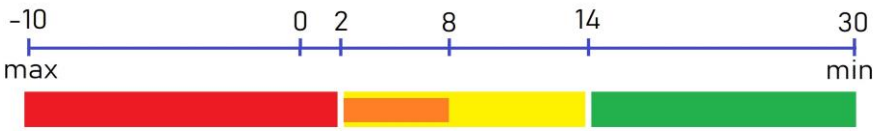
Po dokončení procesu hodnocení deviace jsou určené výsledky porovnány s novou škálou (Obr. 10), která stanovuje významné hraniční hodnoty. Škála sleduje podobnou logiku jako matice rizik, která se používá v současných systémech řízení provozní bezpečnosti. Jsou stanoveny čtyři barvy pro jednotlivé úseky, které reprezentují úroveň přijatelnosti rizika. Slovní hodnocení jednotlivých barev je za účelem kompatibility s maticí rizik[2] podobné (červená - nepřijatelné riziko, oranžová - nežádoucí riziko, žlutá - tolerovatelné riziko, zelená - přijatelné riziko). Vzhledem k tomu, že finální hodnocení deviace se skládá ze tří indexů, každý z nich je hodnocen individuálně a může mít jinou úroveň rizika.

Je důležité upozornit, že standardní matice rizik se skládá ze tří barev. Oranžová barva je v tomto případě přidána pro zjemnění škály jako ukázka podrobnějšího popisu rizika a může být použita dle potřeb jednotlivých organizaci.

Hraniční hodnoty jednotlivých úseků jsou definovány na základě výpočtů problematických scénářů (viz obr. 9):

- Hodnota 2 - všechny skupiny kritéria závažnosti jsou hodnoceny stupněm 5, druhé kritérium stupněm 1 nebo 2 (stav ukazuje na uspokojivou úroveň řízení bezpečnostních mechanismů, ale upozorňuje na vysokou závažnost možného dopadu deviace)
- Hodnota 8 - všechny skupiny kritéria závažnosti jsou hodnoceny stupněm 2, druhé kritérium stupněm 5 (stav ukazuje na špatný stav řízení bezpečnostních mechanismů, a zároveň na relativně nízkou závažnost, která ale není minimální)
- Hodnota 14 - všechny skupiny kritéria závažnosti jsou hodnoceny stupněm 2, druhé kritérium stupněm 4 (stav ukazuje na hraniční bod, kde hodnoty všech kritérii jsou na hranicích přijatelnosti a jakékoliv zhoršení výsledku nebude hodnoceno jako přijatelné)

[2] Metodika z praktických důvodů zachovává základní kompatibilitu s reprezentací rizika pomocí matice rizik (využití barevných zón) pro usnadnění její implementace v leteckém průmyslu.



Obr. 9 - Nová škála přijatelnosti rizika

3.4.4 Hodnocení procesů

V případě hodnocení procesů se souborem deviací je proces jako celek ohodnocen výběrem nejkritičtější hodnoty každého z indexů (a to i v případě, že každý index vychází z jiné deviace), a zároveň aritmetickým průměrem všech bezpečnostních rezerv v procesu (tj. rezerv všech deviací), vyjadřujících možnosti pro zlepšení procesu.

Nejkritičtější deviace je taková, která má nejmenší součet bezpečnostních rezerv kritérií.

3.5 Hodnocení na úrovni systému

Výsledkem realizace předešlých kroků je seznam nebezpečí (deviací) a jejich hodnocení pomocí vektoru indexů bezpečnostní rezervy. Hodnocení nevyžaduje stanovení parametru pravděpodobnosti, jak je obvyklé u matice rizik, pouze hodnocení v uvedených kritériích dle kapitoly 3.4.1. Výsledkem je také hodnocení procesů, tedy sad deviací, které se mohou vyskytnout v rámci jednoho procesu, např. procesu plnění letadla. Posledním krokem je analýza všech deviací v kontextu systému jako celku.

Tato metodika navrhuje v tomto ohledu simultánní využití obou rámcových řešení dle teorie STAMP, tedy vyhodnocení potenciálu pro zmírnění rizika jako i vyhodnocení sady otázek v kontextu realizované studie jako celku.

3.5.1 Potenciál pro zmírnění rizika

Jak již bylo zmíněno v kapitole 3.1, tento potenciál hodnotí identifikovaná nebezpečí z pohledu možností pro zmírnění rizika, které s nimi souvisí. Zde je tedy potřeba rozlišit nebezpečí (deviace), která vyžadují nápravná opatření od těch, které jsou již hodnoceny jako přijatelné z pohledu bezpečnosti. Dále je pak nutné rozlišit, o jaký typ nápravného opatření se jedná. Hodnocení deviací v tomto smyslu sleduje škálu uvedenou v tab. 14.

Vyhodnocení celkového potenciálu pro zmírnění rizika je dáno jako statistika zastoupení jednotlivých kategorií (typů) nápravných opatření dle tab. 14. Pomocí vyhodnocení této statistiky analytik získává kompletní přehled o bezpečnostní studii, zejména tak nepřímý přehled o možné pravděpodobnosti vzniku nežádoucích následků nebezpečí.

Nejvíce žádoucí je stav, kdy všechny deviace lze hodnotit z pohledu nápravných opatření jako 1. nebo 2. typu dle tab. 14. Zvyšování poměrného zastoupení nápravných opatření 3. a zejména pak 4. a 5. typu indikuje mezery v návrhu bezpečnosti. Obecně platí, že opatření 5.

typu by se v bezpečnostní studii neměla vůbec objevovat, ovšem přijatelná míra zastoupení opatření jednotlivých typů je na zvážení v kontextu konkrétní bezpečnostní studie.

Tab. 14 - Hodnocení typů nápravných opatření z pohledu potenciálu pro zmírnění rizika

1. Deviace nevyžaduje nápravu
2. Náprava cílí na odstranění deviace
3. Náprava cíli na zlepšení řiditelnosti, detekovatelnosti anebo časové rezervy
4. Náprava cíli na snížení závažnosti, tedy expozice okolí působení deviace
5. Náprava cíli na snížení následků realizace deviace

3.5.2 Vyhodnocení sady systémových otázek

V tomto kroku je nutné zvážit hodnocený návrh změny systému v konkrétní studii bezpečnosti v kontextu jeho dopadu na širší okolí systému, tedy včetně částí systému, které nejsou přímo hodnoceny v dané studii bezpečnosti. Tato metodika navrhuje jako základní sadu systémových otázek otázky uvedené v tab.15.

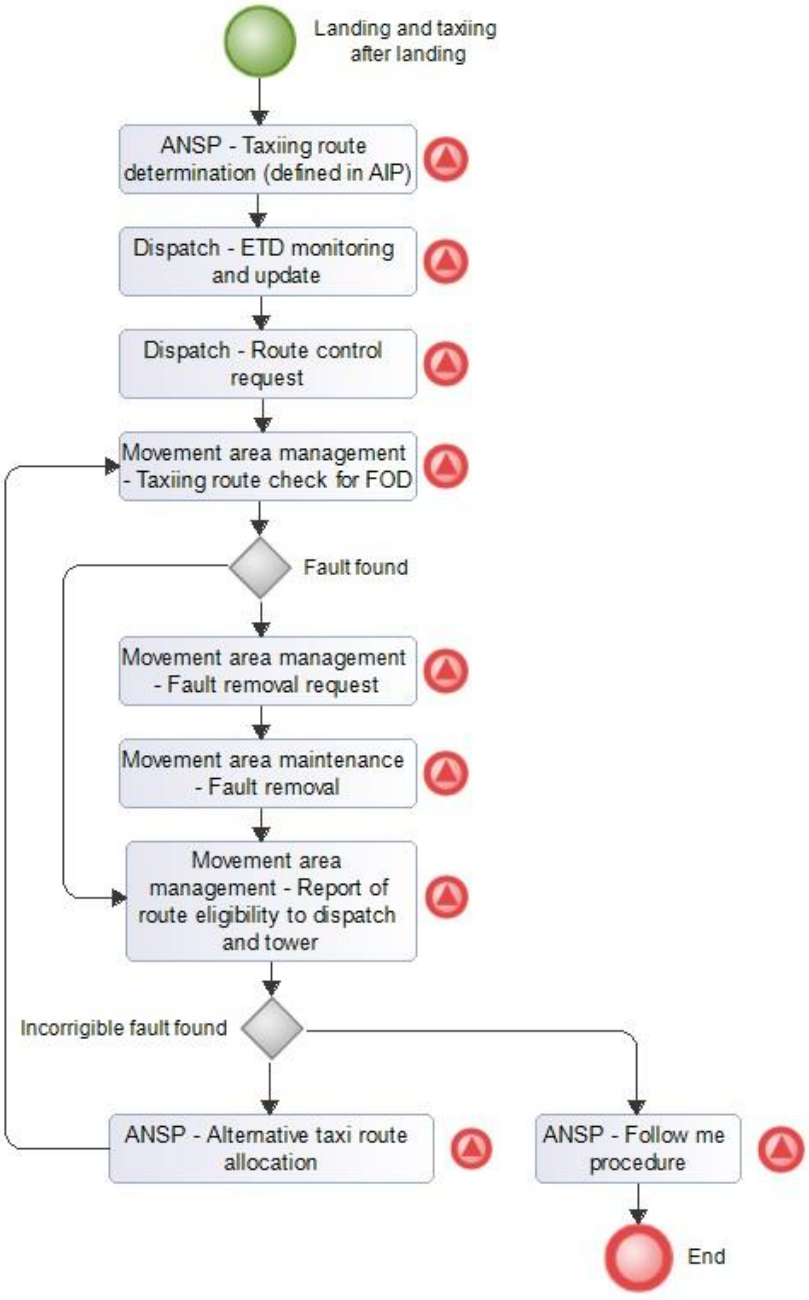
Tab. 15 - Systémové otázky

1. Vyžaduje navrhovaná změna zavedení nových typů opatření pro zmírnění rizika?
2. Může navrhovaná změna redukovat efektivitu některých současně zavedených opatření pro zmírnění rizika?
3. Může navrhovaná změna negativně ovlivnit řiditelnost některé z deviací v systému?
4. Může navrhovaná změna negativně ovlivnit detekovatelnost některé z deviací v systému?
5. Může navrhovaná změna negativně ovlivnit časovou rezervu některého z procesů v systému?
6. Může navrhovaná změna negativně ovlivnit závažnost některého z procesů v systému?

Tyto systémové otázky tvoří pouze kontrolní seznam na závěr bezpečnostní studie a odpověďmi na ně by bezpečnostní analytik měl uzavřít seznam předpokladů a argumentů pro finální rozhodování o implementaci posuzovaného návrhu z pohledu bezpečnosti. V kombinaci se všemi předešlými kroky této metodiky tak vzniká ucelené hodnocení návrhu. Ideální je v tomto ohledu hodnocení několika možných alternativ pro realizaci plánované změny, pokud alternativy existují, nebo také několikanásobné provedení studie bezpečnosti v průběhu tvorby návrhu změny tak, aby bylo možné optimalizovat celkový návrh z pohledu bezpečnosti.

3.6 Příklad hodnocení rizika v letištních procesech

Pro názornost a lepší srozumitelnost hodnocení rizika dle metodiky je toto provedeno na příkladě deviací z prostředí letišť. Jako ukázkový příklad lze použít proces pojíždění kritického typu letadla po přistání. Proces je znázorněn na obr. 10.



Obr. 10. Procesní mapa pojíždění kritického typu letadla po přistání

Takto připravená mapa umožňuje provedení základní bezpečnostní analýzy a definici jednotlivých deviací, které jsou využity k identifikaci nebezpečí. Po identifikaci deviací z tohoto procesu lze stanovit následující seznam:

Determine the inappropriate route_ANSP
Miss the information_Dispatch
Misinformation in communication_General
Do not check the entire area (from the TWY axis to the taxiway strip boundary to both sides)_Movement area Management
Do not record the fault_Movement area Management
Do not pass the information_Movement area Maintenance
Misinformation in communication_General
Do not remove the fault_Movement area Maintenance
Do not control removal_dispatch
Determine the inappropriate route_ANSP
Do not follow the traffic rules
Do not start the "follow me" operation at the start of taxiing_Surface movement
Do not terminate the "follow me" operation at the nearest cross before the RWY exit_Surface movement

Následující krok je zaměřen na identifikaci nebezpečí. Jak již bylo vysvětleno v kapitole 3.2, nebezpečí jsou identifikována pro jednotlivé kroky procesu jako nejhorší možný scénář dle předem definovaných deviací. Tab. 16 obsahuje seznam identifikovaných nebezpečí souvisejících s konkrétními kroky procesu z obr. 10.

Další krok je hodnocení rizik. Příklad bude proveden pro dvě vybrané deviace, a to:

1. Do not check the entire area (from the TWY axis to the taxiway strip boundary to both sides)_Movement area Management (Neprovedena kontrola celé plochy pojížděcí dráhy)
2. Do not pass the information_Movement area Maintenance (nepředání informace dále)

Hodnocení rizika pro první z deviací provádí kvalifikovaný bezpečnostní analytik pro všechny skupiny kritéria závažnost. Pro příklad této deviace je hodnocení následující:

- Lidé - 2 (Snížení komfortu cestujících nebo pracovníků - bez přímého vlivu na cestující nebo ostatní personál v procesu. Lze očekávat zpoždění nebo změnu v organizaci provozu pokud dojde ke kolizi letadla s FOD na pojížděcí dráze.)
- Technika - 3 (Pozemní technika je provozu neschopná, ale opravitelná - přímý dopad na letadlo nebo vozidlo po kolizi s FOD. Možné poškození podvozku letadla a uzavření pojížděcí dráhy, provedení odtahu letadla)

- Prostředí - 1 (Žádný nebo minimální dopad na prostředí lokálního charakteru, případný minimální dopad je jednoduše odstranitelný bez nutnosti investovat velké množství zdrojů - prostředí není ohroženo ve většině možných scénářů)
- Provoz - 3 (Dopad na pozemní provoz způsobující menší zpoždění více letů - uzavření pojížděcí dráhy a potřeba pozemních prostředků pro odtah)

Tab. 16 Systémová nebezpečí

Identifikovaná nebezpečí	Související krok procesu
Inappropriate route determination (route not adequate for safe operation, possible collision or excursion)	Taxiing route determination
	Alternative taxi route allocation
Collision with an object during taxiing (collision with the FOD, damage of the aircraft or its parts)	ETD monitoring and update
	Route control request
	Taxiing route check for FOD
	Fault removal request
	Fault removal
	Report of route eligibility to dispatch and tower
	Follow me procedure

Hodnocení tohoto kritéria bude stejné pro stanovení jednotlivých indexů. Ostatní kritéria byla hodnocena následovně:

- Řiditelnost - 3 (Deviace je obtížně řiditelná - procedura byla provedena, bez definice revizního procesu nebo využití kontrolního zařízení)
- Detekovatelnost - 2 (Pravděpodobná detekce deviace bezprostředně předtím, než nastane - možnost reakce posádky v případech pozemní překážky)
- Časová rezerva - 2 (Proces má komfortní časovou rezervu - alokovaných 30 minut na celkovou proceduru)

Ukázka uvedeného hodnocení s využitím tabulky funkční korelace je znázorněna níže:

Index řiditelnosti

Závažnost		1	2	3	4	5				Řiditelnost
	Lidé			2	1.5	1				
	Technika				1.5	1				
	Prostředí		0.2	2	1.5	1				
	Provoz				1.5	1				
					5	4	3	2	1	

Index detekovatelnosti

Závažnost		1	2	3	4	5				Detekovatelnost
	Lidé			2	1.5	1	0.5			
	Technika				1.5	1	0.5			
	Prostředí		0.2	2	1.5	1	0.5			
	Provoz				1.5	1	0.5			
					5	4	3	2	1	

Index časové rezervy

Závažnost		1	2	3	4	5				Časová rezerva
	Lidé			2	1.5	1	0.5			
	Technika				1.5	1	0.5			
	Prostředí		0.2	2	1.5	1	0.5			
	Provoz				1.5	1	0.5			
					5	4	3	2	1	

Celkové hodnocení rizika deviace je reprezentováno vektorem:

V=(**14,2**; **16,2**; **16,2**)

Dle stanovené škály přijatelnosti rizika spadá hodnocení této deviace do kategorie přijatelné riziko, všechny indexy mají hodnotu vyšší 14, a spadají tedy do zelené zóny.

Hodnocení druhé z deviací (nepředání informace) je zobrazeno v tabulkách níže.

Index řiditelnosti

Závažnost		1	2	3	4	5			
	Lidé			2	1.5	1	0.5		
	Technika		0.75	2	1.5	1	0.5		
	Prostředí		0.75	2	1.5	1	0.5		
	Provoz				1.5	1	0.5		
					5	4	3	2	1

Řiditelnost

Index detekovatelnosti

Závažnost		1	2	3	4	5			
	Lidé			2	1.5	1	0.5		
	Technika		0.75	2	1.5	1	0.5		
	Prostředí		0.75	2	1.5	1	0.5		
	Provoz				1.5	1	0.5		
					5	4	3	2	1

Detekovatelnost

Index časové rezervy

Závažnost		1	2	3	4	5			
	Lidé			2	1.5	1	0.5		
	Technika		0.75	2	1.5	1	0.5		
	Prostředí		0.75	2	1.5	1	0.5		
	Provoz				1.5	1	0.5		
					5	4	3	2	1

Časová rezerva

Celkové hodnocení rizika deviace je reprezentováno vektorem:

V=(**19,5**; **19,5**; **19,5**)
I zde se dle stanovené škály přijatelnosti jedná o přijatelné riziko, všechny indexy spadají do zelené zóny hodnocení.

4. Srovnání novosti postupů se současnými standardy

V kontextu současných standardů provádění studií bezpečnosti v organizacích typu letiště metodika přináší dvě klíčové novosti. První novost se týká aplikace teorie modelu bezpečnosti STAMP společně s nástroji business process modeling, které zjednodušují uplatnění teorie modelu STAMP v leteckém průmyslu. Druhá novost se týká zavedení uceleného rámce kvantitativních postupů, který doplňuje teorii modelu STAMP a metodik na nich založených, tedy i STPA a některé nové postupy, které s ní v tomto dokumentu souvisí.

4.1 Srovnání novosti v kontextu modelu STAMP a metodiky STPA

Metodika přímo vychází z teorie modelu STAMP a nabízí alternativní způsob jak dosáhnout výsledky metodiky STPA. Hlavní rozdíl spočívá v tom, že tato metodika může být přímo aplikována s jinými manažerskými procesy provozovatele letiště (pokud existují) pomocí nástrojů business process modeling. V tomto ohledu podporuje aplikaci teorie STAMP a je s ní plně kompatibilní. V organizacích, kde procesní dokumentace neexistuje nebo kde je značně nepraktické takovou dokumentaci zavést na dostatečné úrovni detailu, je pro analýzu nebezpečí vhodnější STPA. I v takovém případě však může být STPA kombinována s kvantitativním rámcem pro hodnocení rizika z této metodiky k provedení analýzy nebezpečí a rizik. Kromě základních konceptů teorie zpětnovazebního řízení a systémové teorie, tato metodika také pracuje s několika dalšími myšlenkami teorie modelu STAMP, zejména s myšlenkou problematické povahy odhadu pravděpodobnosti v kontextu vyhodnocování rizika ve studiích bezpečnosti, které propojuje s konkrétní doménou v letecké dopravě a tím také přibližuje teorii modelu STAMP do dopravního odvětví.

4.2 Srovnání novosti v kontextu standardu letecké dopravy

Současné standardy pro řízení změn jsou stanoveny především leteckým předpisem L19 [13], resp. dokumentem ICAO Annex 19 [14], a pak dokumentem ICAO Doc. 9859 Safety Management Manual [2] od Mezinárodní organizace civilního letectví ICAO. Ustanovení těchto dokumentů jsou však poměrně obecná a nestanovují žádnou konkrétní metodu, která by měla být aplikována na proces řízení změn. V letecké dopravě se nicméně pro tento účel nejčastěji využívá variací metodiky SAM (Safety Assessment Methodology) [3] publikované Evropskou organizací pro bezpečnost leteckého provozu EUROCONTROL (European Organisation for the Safety of Air Navigation). I když je metodika SAM poměrně detailní, pro proces identifikace nebezpečí není stanovena konkrétní metoda a uživatel si zpravidla volí vlastní postup, jak identifikovat nebezpečí. Obvykle je tento založen na modelech bezpečnosti jako je např. Reasonův model švýcarského sýra nebo na starších metodách jako HAZOP, popřípadě metodě poruchového stromu FTA (Fault Tree Analysis) s její variacemi. Pro vyhodnocení rizika se pak využívá standardní matice rizik.

Tato metodika přináší novost v porovnání se zmiňovanými standardy zejména ve využití systémového modelu STAMP, pro identifikaci nebezpečí ale také jako vstup do procesu hodnocení rizik. Metodika zde stanovuje, jak prakticky využít teorii modelu STAMP v organizacích typu letiště a tedy jak včasně identifikovat bezpečnostní problémy, které nelze identifikovat staršími modely a metodami bezpečnosti. Implementací nové teorie jsou procesy metodiky SAM související s analýzou rizik přizpůsobeny a již nespoléhají na kombinaci starších predikčních modelů bezpečnosti, které SAM doporučuje. Proces hodnocení rizika je zde pak upraven způsobem, který limituje subjektivní hodnocení zejména v problematických aspektech hodnocení pravděpodobnosti.

5. Popis uplatnění certifikované metodiky

Tato metodika popisuje nový postup pro tvorbu studií bezpečnosti v letecké dopravě, se zaměřením se na organizace typu letiště a odpovídá procesům řízení změn v rámci systémů řízení provozní bezpečnosti (Safety Management System - SMS) leteckých organizací.

Metodiku je možné uplatnit v několika směrech uvedených v následujících odstavcích. I když se jedná o inovativní řešení, které není přímo vyžadováno legislativou nebo leteckým předpisem, uplatnění metodiky je se současnou legislativou a předpisem kompatibilní, navíc pozitivně ovlivňuje procesy řízení změn a zlepšuje povědomí o aktuálních a prioritních problémech letišť, čímž umožňuje další zvyšování úrovně provozní bezpečnosti v provozu.

Metodiku lze uplatnit v kontextu implementace ustanovení leteckého předpisu L19 resp. ICAO Annex 19 a také specifických ustanovení dle ICAO Doc. 9859 Safety Management Manuálu týkajících se řízení změn v rámci systémů řízení bezpečnosti SMS.

Metodiku lze uplatnit v kontextu platné evropské legislativy týkající se administrativních procedur pro organizace typu letiště podléhající nařízení Evropské komise č. 216/2008 [15], tedy zejména v kontextu nařízení Evropské komise č. 139/2014 [16].

Metodiku lze uplatnit v kontextu aplikace metodiky SAM od Evropské organizace pro bezpečnost leteckého provozu EUROCONTROL, v případech provádění postupů studií bezpečnosti dle této metodiky.

6. Ekonomické aspekty

Aplikace metodiky přináší několik nákladů souvisejících s její implementací. Tyto souvisejí se zavedením nových postupů provádění studií bezpečnosti, které jsou náročnější na realizaci, než je současný standard v letecké dopravě, zejména v prostředí organizací typu letiště. Bezpečnostní analytik musí být obeznámen s provozní dokumentací konkrétní organizace, identifikovat relevantní postupy a projektovat budoucí změnu, tedy i poskytovat potřebné vstupy pro aktualizaci provozní dokumentace. V některých případech může být výhodné zvýšit počet zaměstnanců s odpovědností pro provádění studií bezpečnosti v konkrétní organizaci, tato metodika však takové opatření nezbytně nevyžaduje pro její implementaci.

Implementace metodiky nevyžaduje vývoj speciálního softwarového nástroje. Z technického hlediska tato metodika také nevyžaduje žádné systémové změny, což vylučuje související technické a výrobní náklady. Procesy metodiky využívají stávající řešení z domény aplikace BPMN, které jsou často již součástí procesů řízení organizací, zatímco analýzu rizik lze provádět pomocí standardního softwaru, jako např. pomocí balíčku Microsoft Office. Procesy metodiky, včetně vytvoření seznamu nebezpečí a deviací, jsou cíleny na pracovníky řízení bezpečnosti v dané organizaci. Předpokládaná doba pro provedení jednotlivých kroků metodiky závisí na velikosti příslušné organizace. Pro školení a implementaci metodiky do procesů posuzování bezpečnosti je zapotřebí přibližně třídenní workshop.

Potenciální ekonomické přínosy naopak souvisí se zvýšením úrovně bezpečnosti, kterou je možné zajistit v procesech řízení změn u organizací typu letiště. Metodika přináší způsob, jak efektivně identifikovat a dále pracovat s větším množstvím nebezpečí, než je obvyklé v současných studiích bezpečnosti. Má tedy potenciál odhalit víc problémů bezpečnosti a tím umožnit včasné a zpravidla tedy i méně nákladné zmírnění rizika souvisejícího s těmito problémy. Metodika cílí i na vlastní hodnocení rizika, tedy předkládá kvantitativní postupy, kterými dekomponuje některé ryze subjektivní aspekty současných postupů provádění studií

bezpečnosti. Tímto pozitivně přispívá k prioritizaci bezpečnostních problémů a ve výsledku i k lepší alokaci zdrojů na zajištění přijatelné úrovně bezpečnosti.

Dalším aspektem je, že metodika má potenciál zlepšit i jiné oblasti než bezpečnost, přestože se zabývá pouze bezpečností. Tyto oblasti se týkají například řízení kvality a procesů nebo řízení ochrany vůči protiprávním činům na letištích. Univerzálnost postupu je založena na využití BPMN, čímž se integruje metodika se standardními obchodními procesy a jejich řízením, a také na teorii STAMP, která má potenciál poskytovat podporu v rozhodování dalším doménám.

Seznam použité literatury

[1] Dekker, S. *Drift into failure: from hunting broken components to understanding complex systems*. Burlington, VT: Ashgate Pub., 2011. ISBN 978-1409422211.

[2] International Civil Aviation Organization (ICAO). Safety Management Manual (SMM): Doc 9859 AN/474. Fourth Edition. Montréal, 2018. ISBN 978-92-9249-214-4.

[3] EUROCONTROL, "Safety Assessment Methodology", A framework of methods and techniques to develop safety assessments of changes to functional systems. Dostupné z: https://www.eurocontrol.int/tool/safety-assessment-methodology

[4] Leveson, N. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. ISBN 978-0-262-01662-9.

[5] Cox, L. A. What's Wrong with Risk Matrices? *Risk Analysis*. 2008, 28(2), 497-512. DOI: 10.1111/j.1539-6924.2008.01030.x. ISSN 02724332.

[6] Leveson, N. a Thomas P. STPA Handbook. 2018. Dostupné z: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[7] Doyle, J. C., Francis, B.A. a Tannenbaum, A. *Feedback control theory*. Mineola, N.Y.: Dover, 2009. ISBN 978-0486469331.

[8] Leveson, N. a Dulac, N. Incorporating Safety in Early System Architecture Trade Studies, Journal of Spacecraft and Rockets, Vol. 46, No. 2 (2009), pp. 430-437.

[9] EP3 Environmental Incident Reporting & Management, Defence National Environmental Standard Environmental Incident Reporting & Management, Department of Defence, Australian Government, 2014.

[10] Federal Aviation Administration (FAA), System Safety Handbook, Chapter 3: Principles of System Safety, 2013.

[11] European Organisation for Civil Aviation Equipment (EUROCAE). ED78A/DO264 -"Guidelines for approval of the provision and use of Air Traffic Services supported by data communications" EUROCAE. 2000.

[12] Karanikas, N. An introduction of accidents' classification based on their outcome control. Safety Science. 2015, 72, 182-189. DOI: 10.1016/j.ssci.2014.09.006. ISSN 09257535.

[13] Ministerstvo dopravy ČR. Letecký předpis L19 - řízení bezpečnosti. Číslo jednací 166/2013-220-LPR/1, 2013.

[14] International Civil Aviation Organization (ICAO). Annex 19 - Safety Management. Second Edition. Montréal, 2016. ISBN 978-92-9249-965-5.

[15] Nařízení Evropského parlamentu a Rady (ES) č. 216/2008 o společných pravidlech v oblasti civilního letectví a o zřízení Evropské agentury pro bezpečnost letectví. OJ L 79. Dostupné z: http://data.europa.eu/eli/reg/2008/216/oj

[16] Nařízení Komise (EU) č. 139/2014 kterým se stanoví požadavky a správní postupy týkající se letišť podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008. OJ L 44. Dostupné z: http://data.europa.eu/eli/reg/2014/139/oj

Seznam publikací, které předcházely metodice

Lališ, A., Socha, V., Křemen,P., Vittek, P., Socha, L. and Kraus J. Generating synthetic aviation safety data to resample or establish new datasets. *Safety Science*. 2018, 106, 154-161. DOI: 10.1016/j.ssci.2018.03.013. ISSN 09257535.

Lališ, A., Socha, V., Vittek, P. and Stojić, S. Predicting safety performance to control risk in military systems. In: *2017 International Conference on Military Technologies (ICMT)*. IEEE, 2017, 2017, s. 392-396. DOI: 10.1109/MILTECHS.2017.7988791. ISBN 978-1-5090-5666-8.

Leveson, N. and Dulac, N. Incorporating Safety in Early System Architecture Trade Studies. *Journal of Spacecraft and Rockets*. 2009, 46(2), 430-437. DOI: 10.2514/1.37361. ISSN 0022-4650.

Leveson, N., Wilkinson, Ch., Fleming, C., Thomas, J. and Tracy I. A Comparison of STPA and the ARP 4761 Safety Assessment Process. MIT Technical Report, 2014. Dostupné z:http://sunnyday.mit.edu/papers/ARP4761-Comparison-Report-final-1.pdf

Sales, T. P., Baião, F., Guizzardi, G., Almeida, J. P., Mylopoulos, J. The Common Ontology of Value and Risk. Trujillo, J. C., Davis, K. C., Du, X., Li, Z., Ling, T. W., Li, G. Lee, M. L. ed. *Conceptual Modeling*. Cham: Springer International Publishing, 2018, 2018-09-26, s. 121-135. Lecture Notes in Computer Science. DOI: 10.1007/978-3-030-00847-5_11. ISBN 978-3-030-00846-8.