METODIKA

pro využití teorie modelu STAMP v prostředí dozorových orgánů odvětví letecké dopravy

Projekt TA ČR Programu DOPRAVA 2020+ č. CK01000073

Ústav letecké dopravy
Fakulta dopravní
ČVUT v Praze

Lališ Andrej
Grötschelová Kateřina
Stojić Slobodan

Program **Doprava 2020+**

Metodika pro využití teorie modelu STAMP v prostředí dozorových orgánů odvětví letecké dopravy

Obsah

Úvod

Dozor nad bezpečností letecké dopravy je jedním z pilířů řízení bezpečnosti v moderní letecké dopravě. Role dozorových institucí je klíčová zejména proto, že jejich úkolem je plnit objednávku veřejnosti na bezpečnou leteckou dopravy, díky čemuž tato role připadá na nestranné instituce – Úřady pro civilní letectví. Úřady si za dobu plnění své funkce vyvinuly systém, pomocí kterého dohlížejí na bezpečnost v leteckých organizacích. Kombinují sledování shody na bázi požadavků danými nařízeními, zákony či předpisy a zkušenosti či znalosti úředníků z dozorované oblasti, kteří s organizacemi komunikují. V několika ohledech zde hraje roli také sledování ukazatelů výkonnosti v bezpečnosti, ke kterému se letecká doprava dlouhodobě přesouvá.

Ohodnotit skutečný stav bezpečnosti konkrétní organizace není triviální úkol. Shoda s požadavky není garancí vysoké míry bezpečnosti a identifikace problémových aspektů provozu letecké dopravy mnohdy závisí na týmu úředníků a jejich zkušenostech. V bezpečnostním inženýrství však v poslední době vzniklo několik přístupů a metod, které mají tento problém řešit. Jedná se o metody určené jak pro identifikaci nebezpečí a rizik, tak ke sledování výkonnosti v bezpečnosti či práci s audity a inspekcemi. Tyto metody patří do tzv. systémového přístupu k bezpečnosti, který na rozdíl od dosavadního řízení bezpečnosti usiluje o holistický (tzv. „celosystémový") přístup.

Tato metodika pracuje s jedním ze současných řešení – modelem bezpečnosti Systems Theoretic Accident Model and Processes (STAMP). Tento model interpretuje problém bezpečnosti jakožto problém řízení. V jeho chápání je tedy klíčové to, jak jsou organizace nastaveny z pohledu rolí, odpovědností a interakcí mezi nimi. Bezpečnost se pak dle STAMP chápe jako systémová vlastnost, která existuje pouze pokud organizace fungují bezpečně jako celek. V letecké dopravě se navíc pod pojmem „celek" neboli „systém" chápou všechny organizace, včetně Úřadů pro civilní letectví, a jejich interakcí. Pokud tedy má být zajištěna bezpečnost letecké dopravy, v moderním světe to znamená dynamický proces neustálého nastavování a ladění leteckých organizací uvnitř a zároveň mezi sebou navzájem, kde Úřady plní nejen roli pozorovatele či nestranné entity, ale zároveň aktivní roli účastníka takového procesu.

Tato metodika je produkt výzkumného projektu, který si kladl za cíl najít praktický způsob, jak použít nová teoretická východiska systémového přístupu k bezpečnosti v praxi dozorových institucí v letecké dopravě. Úkolem projektu bylo odpovědět na nelehké otázky z praxe ohledně systémového přístupu k bezpečnosti, a vytvořit doporučený postup, který je prezentován v tomto dokumentu. Tento obsahuje i praktické ukázky a názorné příklady, které byly ověřovány s Úřadem pro civilní letectví České republiky.

Dokument ve výsledku popisuje nové metody a postupy, které vedou primárně ke zvýšení schopnosti úředníků identifikovat a aktivně pracovat s problémy bezpečnosti letecké dopravy, a to na bázi skutečně dosahované úrovně bezpečnosti leteckých organizací v provozu. Vede také k další digitalizaci, modernizaci, integraci a zefektivnění procesů dozorového orgánu v civilním letectví.

1 Cíl metodiky

Metodika si klade za cíl diseminovat a podpořit výsledky realizovaného výzkumu Českým vysokým učením technickým v Praze ve spolupráci s Úřadem pro civilní letectví v rámci projektu č. CK01000073 s podporou Technologické agentury České republiky. Metodika je souhrnem klíčové znalosti dosažené v řešeném projektu a obsahuje základní postupy pro zpracování a analýzu dat o bezpečnosti na úrovni dozorových institucí a postup pro tvorbu auditních otázek pro audity založené na systémovém přístupu k bezpečnosti. Metodika cílí na digitalizaci, modernizaci, integraci a zefektivnění procesů dozorového orgánu v civilním letectví za současného snížení administrativní zátěže, kterou snáší subjekty státního dozoru.

2 Dedikace

Metodika je primárně určena pro organizace zabývající se dozorem nad bezpečností letecké dopravy, které se zajímají o možnosti zlepšení v oblasti identifikace problémů bezpečnosti a zacílení auditů a inspekcí v dozorovaných organizacích. Dokument obsahuje praktické příklady z oblasti letecké dopravy, včetně užitečných odkazů a citací, které s touto doménou souvisí. Metodiku lze aplikovat i na další odvětví dopravy, ve kterých se provádí dozor nad bezpečností organizací. V takovém případě je však nezbytné zvážit potřebu modifikace nebo přizpůsobení konkrétních postupů na zvolené podmínky.

3 Popis metodiky

V této kapitole je uveden popis využití teorie modelu STAMP v prostředí dozorových orgánů odvětví letecké dopravy, a to formou několika samostatných postupů, které řeší dílčí problémy aplikace STAMP v tomto prostředí, s praktickými ukázkami. V této kapitole jsou také popsány základy modelu bezpečnosti STAMP, jejich vazba na prezentované postupy této metodiky a užitečné odkazy na související metody.

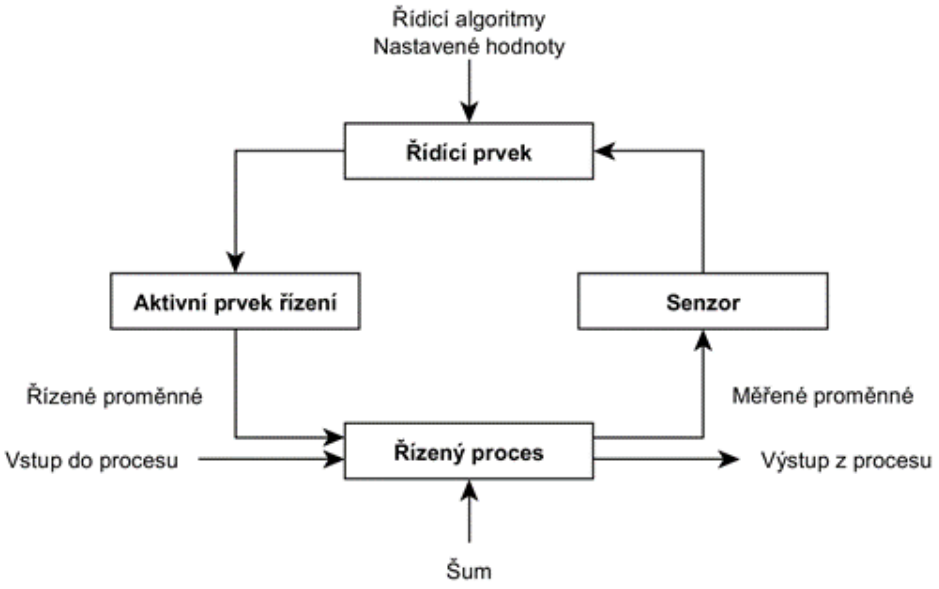
3.1 Model bezpečnosti STAMP

Systems Theoretic Accident Model and Processes (STAMP) je kauzální model bezpečnosti, který říká, že jakýkoliv problém bezpečnosti je svou podstatou problémem řízení. Tím se myslí, že obecně v našem světě i konkrétně ve světě leteckých organizacích je rozhodující, jak efektivní kontrolu nad probíhajícími procesy máme a zda se procesy kontrole s postupem času nevymykají. Procesy v socio-technických systémech je nutné aktivně nebo pasivně řídit pro zajištění předem stanovených cílů. Řízením se přitom myslí jakákoliv změna stavu v řízených procesech, kterou lze ve smyslu STAMP provést managementem organizace, pracovníky v provozu nebo automatizací či fyzickými, pasivními zábranami.

Zajištění bezpečnosti jakožto systémové vlastnosti je proto otázkou tvorby celkového systému řízení nad všemi řízenými procesy, jakož i otázkou udržení kontroly nad procesy

v průběhu času. STAMP v tomto ohledu využívá systémové teorie a myšlenky zpětnovazebního řízení, které se v případě aktivního řízení schematicky reprezentuje pomocí tzv. řídící smyčky (obr. 1). Tvorba systému řízení tedy znamená organizaci lidí a techniky do hierarchie tzv. řídících prvků, distribuci odpovědností mezi ně, a nakonec nastavení interakcí, které každému řídícímu prvku zajistí, že v jakémkoliv okamžiku bude mít k dispozici potřebné informace o aktuálním stavu řízených procesů (pomocí tzv. senzorů) a způsoby, kterými může stav procesů měnit, tedy řídit (pomocí tzv. aktivních prvků řízení). Toto je klíčová myšlenka, kterou se STAMP odlišuje od jiných modelů bezpečnosti (jako např. SHELL nebo Reasonův model bezpečnosti), a která umožňuje zmíněný holistický přístup k bezpečnosti.

Správně nastavený systém řízení musí být schopen rozpoznat, že nějaký z řízených procesů se vymyká kontrole a aktivně zasáhnout proti úplné ztrátě kontroly nad ním, která obvykle vede k nehodě, resp. nese s sebou ztrátu něčeho pro organizaci cenného. V krajním případě to může znamenat i úpravu systému samotného v některých jeho částech, pokud tyto části již nejsou schopny efektivně řídit konkrétní procesy. Tento případ je blízký zejména dozorovým institucím, jejichž úkolem je monitorovat hlavní rysy a výkonnost aktuálně provozovaných systémů a včasně detekovat nežádoucí degradaci, resp. vyžadovat nápravná opatření.



Obr. 1 - Řídící smyčka zpětnovazebního řízení (upraveno a přeloženo z [1])

Reálné systémy jsou tvořeny sadou (obvykle desítkami nebo stovkami) navzájem provázaných řídících smyček, ve kterých není triviální identifikovat bezpečnostní problémy. Autoři STAMP proto navrhli metody určené pro řešení konkrétních otázek bezpečnosti z pohledu STAMP v reálných systémech. Základními metodami jsou analýza nebezpečí System-Theoretic Process Analysis (STPA) a analýza nehod Causal Analysis based on System Theory (CAST). Obě jsou přehledně zpracovány v samostatných

manuálech [2, 3]. Z pohledu využití modelu bezpečnosti STAMP v procesech dozoru nad leteckými organizacemi je klíčová zejména metoda STPA a její rozšíření známé jako Active STPA [4].

STPA je svou podstatou proaktivní metoda, umožňuje totiž predikci všech možných bezpečnostních problémů jakožto ztráty kontroly nad řízením, a to pouze na bázi popisu toho, jak je konkrétní systém navržen. Vstupem pro tuto metodu může být běžně dostupná certifikační dokumentace konkrétní letecké organizace a její představa o tom, jak bude v provozu fungovat. Pro predikci možných bezpečnostních problémů přitom nejsou potřebná žádná historická data o bezpečnosti, která častokrát ani neexistují. Není ani potřeba hlubší expertní znalost dozorované organizace, jelikož z pohledu dozoru nad ní je podstatný pouze princip toho, jak organizace zajišťuje kontrolu nad svými procesy, ne podstata procesů jako takových. Pokud by však v některých případech byla podstata procesů klíčová, lze jí v potřebné míře diskutovat přímo s danou organizací v rámci běžné auditní činnosti. Dozorovým úřadům metoda STPA dává unikátní možnost problémy identifikovat mnohem dříve, než se jakkoliv projeví v nabytých datech o bezpečnosti z provozu.

Výstupy STPA lze využít nejen pro identifikaci možných bezpečnostních problémů, ale i jako klasifikátory pro nově příchozí bezpečnostní data, nebo jako podklad pro tvorbu auditních otázek. Active STPA je rozšíření metody STPA, které je zaměřeno právě na tyto kroky, a to pro účely řízení bezpečnosti v probíhajícím provozu. Zde autoři STAMP poukazují na to, jak lze využít výstupy STPA v typických procesech sběru a vyhodnocování dat o bezpečnosti, které se děje v rámci systému řízení provozní bezpečnosti (safety management system (SMS)). Protože stát řídí bezpečnost a dozoruje organizace na stejných principech jako SMS [5], lze Active STPA uplatnit i v rámci dozorových činností leteckých úřadů.

V postupech této metodiky se využívá STPA jako základní metoda pro identifikaci a další práci s nebezpečími a Active STPA pro zpracování a analýzu dat o bezpečnosti. Pro vykonání postupů, které jsou založeny na STPA, je tedy nezbytná alespoň základní znalost této metody, kterou lze nabýt z manuálu k ní [2]. Vhodná je také alespoň základní znalost Active STPA pro postupy, ve kterých se toto rozšíření STPA využívá.

3.2 Formalizace procesů dozorového orgánu

Tento postup je doporučený v případě, kdy se analýze nebezpečí podrobuje samotná dozorová instituce. Jak již bylo zmíněno, Úřady plní nejen roli pozorovatele a nestranné entity, ale zároveň také aktivní roli účastníka procesů letecké dopravy. Jako takové mohou přispět k leteckým nehodám tím, že sami ztratí kontrolu nad organizacemi a buď umožní, nebo přímo podpoří svou činností vznik nebezpečí v leteckém provozu.

Hlavním cílem dozorových institucí je certifikovat a dozorovat letecké organizace (jako například letiště, údržbové organizace, letecké dopravce atd.) a zajistit tak přijatelnou úroveň bezpečnosti na státní úrovni. Samotný dozorový orgán ale není výjimkou a musí

také aktivně pracovat se svými procesy a provádět například interní audity, aby zajistil, že jeho postupy budou efektivní a v dostatečné míře zajišťující bezpečnost.

Správa procesů začíná vždy u procesní dokumentace, kde jsou detailně popsány jednotlivé procesy včetně odpovědností a referencí na další související dokumentaci. Procesní dokumentace ale může trpět určitými nedostatky jako například tím, že proces může být popsán fragmentovaně a čtenář, resp. odpovědná osoba či organizační jednotka se tak může odchýlit v jeho chápání od původního záměru. Dalším problémem, který se v dokumentaci může vyskytovat je chybějící odpovědnost nebo zjednodušovaná či slučovaná odpovědnost. Pod zjednodušenou odpovědností si lze představit situaci, kdy za určitou aktivitu je odpovědný například provozovatel či organizace. Pokud se v textu často vyskytuje tato odpovědnost, pro čtenáře pak není zřetelné, kdo je za co reálně odpovědný a na koho se má čtenář (fyzická osoba) v případě problému obrátit.

Dozorový orgán, stejně jako i každá jiná organizace, může pro správu svých procesů využít i grafickou formu, která se tak stává doplňkem k textové podobě procesní dokumentace. Grafické mapování procesů je výhodné především pro správné pochopení vztahů mezi jednotlivými aktivitami, pokud jsou procesy komplexnější, a zároveň dobře slouží k nalezení nedostatků v textové formě popisu procesů. Pomocí grafického mapování procesů lze poměrně snadno odhalit například skutečnost, že u některé aktivity není jasně přidělena odpovědnost či to, že není z textové formy jasně daný tok aktivit.

Pro grafické mapování procesů existují metodiky, podle kterých je možné při modelování vlastních procesů postupovat. Jednou z metodik, která tuto problematiku řeší komplexně a kterou lze přímo využít v kontextu aplikace STAMP v dozorových institucích je například Methodology for Modelling and Analysis of Business Process (MMABP) [6]. MMABP je základ pro modelování a analyzování podnikových systémů a procesů, její principy lze ale bez problémů aplikovat i na procesy subjektu typu dozorového orgánu. MMABP využívá pro modelování podnikových procesů standardizované modelovací jazyky a rámce jako je Business Process Model and Notation (BPMN) a The Open Group Architecture Framework (TOGAF) Event Diagram (neboli diagram událostí).

BPMN, jak už název napovídá, je notace vytvořená v souladu s aktuálními trendy v oblasti podnikových systémů. Primárním cílem BPMN je standardizovat popis procesů v celém jejich životním cyklu neboli workflow. Grafická notace je dobře srozumitelná pro projektové manažery či business analytiky, kteří s procesy aktivně pracují (tedy monitorují, řídí, spravují) a zároveň také splňuje formu technického zápisu procesů, se kterou dále mohou pracovat například vývojáři, kteří implementují řešení pro podporu procesů v organizaci. Business Process Diagram je diagram, kterým je notace definována, a tento diagram je tvořen zpravidla sítí grafických objektů, zejména aktivitami a toky, které definují pořadí vykonávaných aktivit.

Vzhledem k tomu, že BPMN popisuje procesy ve velkém detailu, využívá se někdy jako doplněk tzv. procesní mapa. K reprezentaci procesní mapy se využívá například

Eriksson-Penker process diagram nebo již zmíněný TOGAF Event Diagram. Procesní mapa zajišťuje globální pohled na procesy, který v BPMN není na této úrovni zastoupen. BPMN společně s procesní mapou tak tvoří jak globální, tak detailní pohled na podnikové procesy organizace (dozorového orgánu) a umožňují pro uživatele snadné pochopení procesů. Není ale nutnou podmínkou mapovat vždy podnikové procesy na obou úrovních. Každá organizace (dozorový orgán) rozumí vlastním interním procesům a nejlépe ví, co je v danou chvíli a pro daný účel přínosnější.

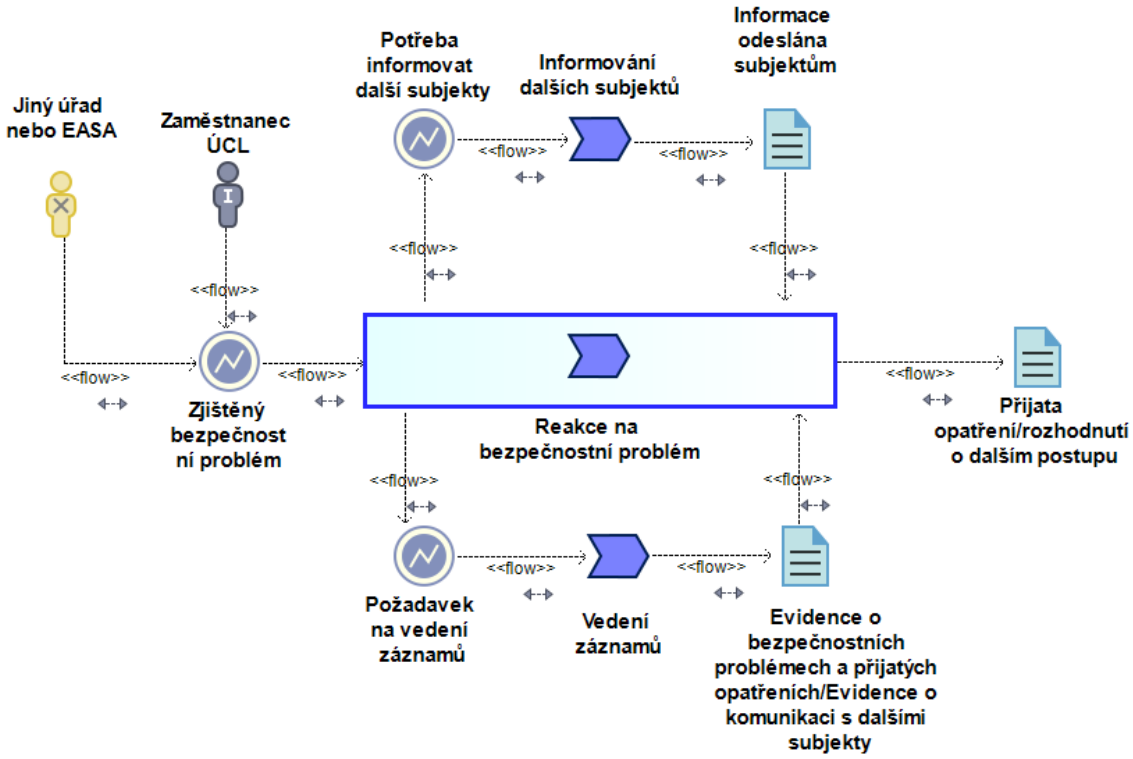
3.2.1 Tvorba procesních map a BPMN diagramů

Prvním krokem při tvorbě procesních map a modelování procesních diagramů je analýza textu dokumentace, ze které má modelovaný proces vycházet. Textová analýza se provádí ručně, kdy analytik čte (prochází) text a vyznačuje jeho důležité části, které jsou podstatné pro tvorbu diagramů. Pro tuto analýzu je zapotřebí se nejprve dobře seznámit s komponenty, které procesní mapa či diagram využívají, aby analytik věděl, co je pro něho v textu důležité a co ne. Textová analýza by v určitých případech mohla být prováděna i automaticky či poloautomaticky, jelikož již nyní existují nástroje (např. [7] nebo [8]), které umožňují provádět textovou analýzu podle požadavků kladených uživatelem a vyhledat v textu podstatné informace, se kterými pak může analytik (uživatel) dále pracovat. Příklad textové analýzy provedené ručně je na obr. 2, kde je uveden výňatek z textu interní směrnice dozorového orgánu. V textu byly analytikem označeny důležité části, které se následně využily při modelování procesu do jeho grafické podoby.

1. Zjistí-li zaměstnanec úřadu během výkonu dozoru bezpečnostní problém, nebo, má-li zaměstnanec úřadu podezření na bezpečnostní problém, oznámí tuto skutečnost neprodleně řediteli příslušného samostatného útvaru. Ten tuto informaci posoudí, a pokud také shledá podezření na bezpečnostní problém, přijme patřičná opatření k jeho vyřešení.
2. Součástí zvažovaných opatření musí být i informování dalších subjektů, které by daným problémem mohly být dotčeny - včetně EASA a příslušných úřadů jiných členských států EU v souladu s postupem dle Článku 8.
3. Pokud to povaha bezpečnostního problému vyžaduje (ředitel samostatného útvaru nemá potřebné kompetence k přijetí patřičného opatření, není schopen posoudit, zda se jedná o bezpečnostní problém nebo je problém natolik vážný, že je nezbytné ho řešit v rámci vedení), předá takovou informaci svému představenému, případně v případě ředitele sekce poradě vedení, která rozhodne o dalším postupu.

Obr. 2 - Výňatek textu ze směrnice dozorového orgánu

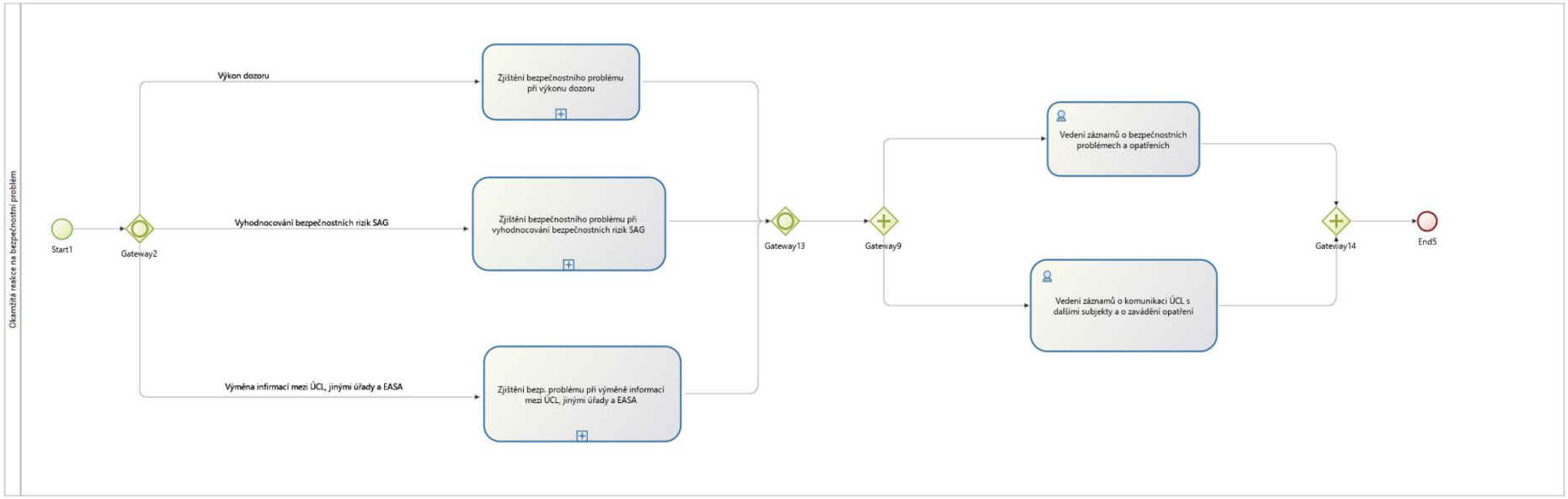
Na obr. 3 je vyobrazen TOGAF Event Diagram procesu „Reakce na bezpečnostní problém“ v prostředí dozorového orgánu. Hlavní proces v modrém obdélníku „Reakce na bezpečnostní problém“ je zde tzv. nosným procesem a další dva procesy „Informování dalších subjektů“ a „Vedení záznamů“ jsou procesy podpůrné. Každý proces má vlastní vstup a výstup. Vstupem pro nosný proces je „Zjištěný bezpečnostní problém“ a výstupem je „Přijata opatření/rozhodnutí o dalším postupu“. Vstup může v tomto případě zajistit externí („Jiný úřad nebo EASA“) či interní osoba („Zaměstnanec ÚCL“).



Obr. 3 - TOGAF Event Diagram procesu „Reakce na bezpečnostní problém“

Poté, co analytik vytvoří procesní mapu neboli např. TOGAF Event Diagram, může pokračovat modelováním BPMN diagramů. Není ale nutné postupovat vždy v tomto pořadí. Někdy může být pro analytika vhodnější modelovat nejdříve BPMN diagram, který je detailnější, a až následně vytvořit procesní mapu ve formě TOGAF Event Diagramů, která je abstrakcí detailnějšího diagramu. V některých případech může být totiž pro analytika složité vytáhnout z textu hlavní procesy včetně jejich vstupů a výstupů bez hlubší znalosti detailů procesu. Pokud se ale vytváří procesy nové, vhodnějším přístupem je nejprve tvorba obecného diagramu, který nejdříve oddělí nosné od podpůrných procesů a vytvoří přehled jejich návaznosti.

BPMN diagram na obr. 4 se skládá z konkrétních aktivit, které byly zvýrazněné v textu (viz obr. 2). Z kontextu procesní dokumentace je pro tvorbu BPMN diagramu potřeba vyčíst také určitá rozhodování či odlišné varianty pro různé typy problémů a ty jsou v digramu znázorněny žlutými kosočtverci, které se nazývají „Gateways“ a umožňují větvení či slučování toku procesu. Celý BPMN diagram se dělí na tzv. „Pools“. První část diagramu (neboli první Pool) je do většího detailu rozepsaný již zmíněný nosný proces. Samotné aktivity v prvním „Poolu“ mají dále své podaktivity či podprocesy, které se dále rozepisují pomocí dalších Poolů. Toto lze poznat podle malého znaku „+“ v dolní části obdélníku (aktivity) (viz obr. 4). Každá konečná aktivita by měla mít pak přiřazenou vlastní roli a tato role je odpovědná za vykonání konkrétní aktivity. Jestliže role přiřazena není, je patrné, že v textu chybí informace o tom, kdo je za aktivitu zodpovědný.



Obr. 4 - První „Pool“ z BPMN diagramu procesu „Reakce na bezpečnostní problém“

Pro tvorbu BPMN diagramů a procesních map existuje mnoho nástrojů, které lze využít. V této metodice byl pro BPMN diagramy využit nástroj Bonita Studio[1] a pro TOGAF Event Diagram nástroj Modelio[2]. Podobných nástrojů ale existuje několik a uživatelé si mohou zvolit podle na základě svých možností a potřeb.

3.2.2 Tvorba řídící struktury dle STAMP

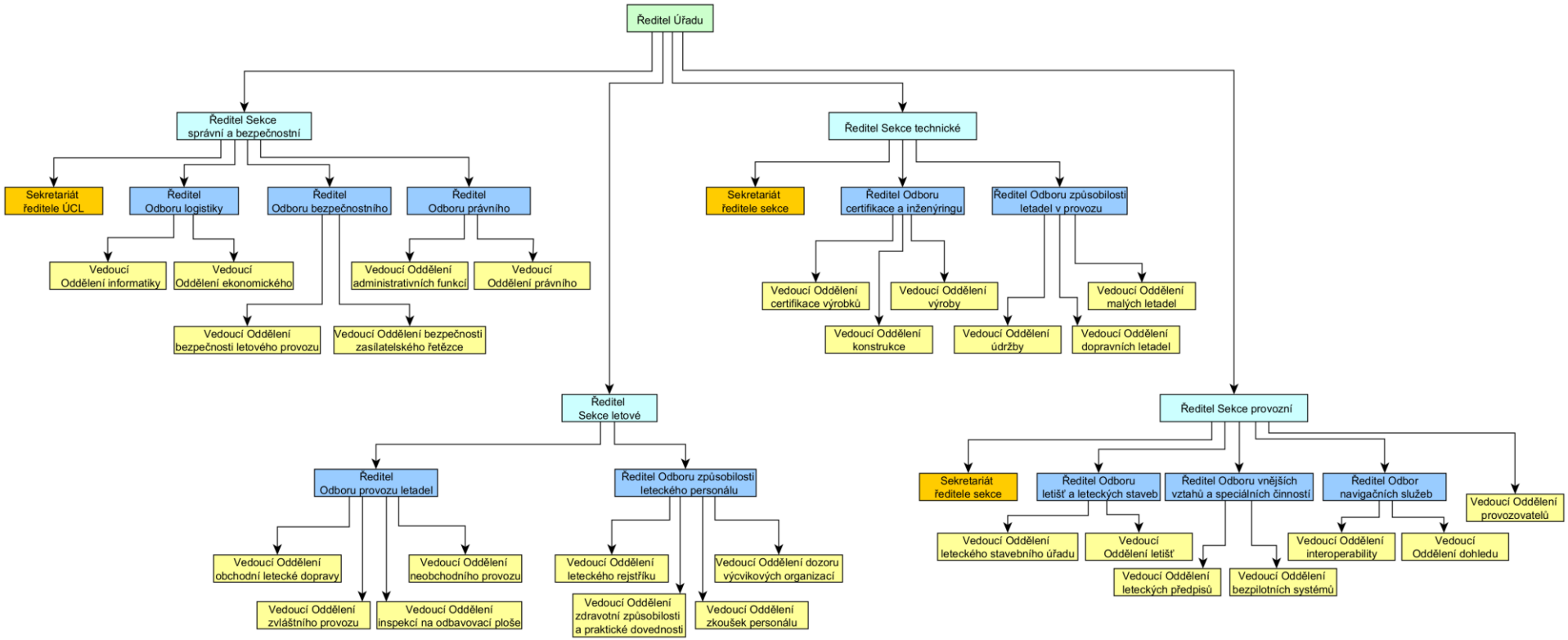
Jak bylo vysvětleno v kapitole 3.1., na modelu bezpečnosti STAMP je založena metodika STPA, pomocí které je možné provádět analýzu nebezpečí. Jelikož systémový pohled na bezpečnost zahrnuje širší pojetí systému, dozorové instituce samotné by měly provádět analýzu nebezpečí nad svými procesy. Součástí STPA analýzy je mimo jiné i tvorba řídící struktury (druhý krok STPA), která tvoří základ pro další kroky STPA. Samotná řídící struktura nemusí sloužit pouze k analýze nebezpečí. Pomocí ní může dozorový orgán získat lepší přehled nad svou organizační strukturou, procesy a interními či externími vztahy.

Pro vytvoření řídící struktury platí téměř shodný postup jako při vytváření procesních map či BPMN diagramů. Pro dozorový orgán je tedy důležité si vzít interní dokumentaci a vyznačit si v ní důležité části, které jsou potřebné pro tvorbu řídící struktury. Po tomto kroku následuje samotné modelování řídící struktury. Pokud však dozorový orgán už má vytvořené procesní mapy a BMPN diagramy, je vhodné je při modelování řídící struktury využít společně s procesní dokumentací. Informace o řídících prvcích, řízených procesech, ale i o řídících akcích či zpětné vazbě jsou zde často snadno dohledatelné a přehledné. Z toho důvodu jde pak tvorba řídící struktury snadněji a dokumentace slouží pouze jako doplněk pro upřesnění některých informací či vazeb mezi nimi.

V rámci modelování řídící struktury dozorového orgánu by se mělo uvažovat podobně jako při tvorbě procesních map a BPMN diagramů. To znamená, že by měl dozorový orgán začít tvorbou obecnější řídící struktury a postupně pokračovat do většího detailu. Pokud tedy dozorový orgán začíná modelovat řídící strukturu, je ideální začít s organizační strukturou a základními procesy, které má dozorový orgán vykonávat. Ukázka abstrahované řídící struktury dozorového orgánu (založena na skutečné organizační struktuře Úřadu pro civilní letectví) je na obr. 5, kde jednotlivé barvy označují různé úrovně řídících rolí.

Poté, co dozorový orgán vytvoří základní strukturu může začít zdetailňovat jednotlivé procesy či organizační jednotky vztahující se k určitým sadám procesů. K tomu může Úřadu pomoci procesní mapa (např. TOGAF Event Diagram), protože jsou zde uvedené nosné procesy, na které navazují procesy podpůrné. Lze tak získat základní přehled o vztazích mezi procesy, na jejichž základě lze modelovat další úrovně řídící struktury. Následujícím a případně i posledním krokem je největší detail řídící struktury, kde už se

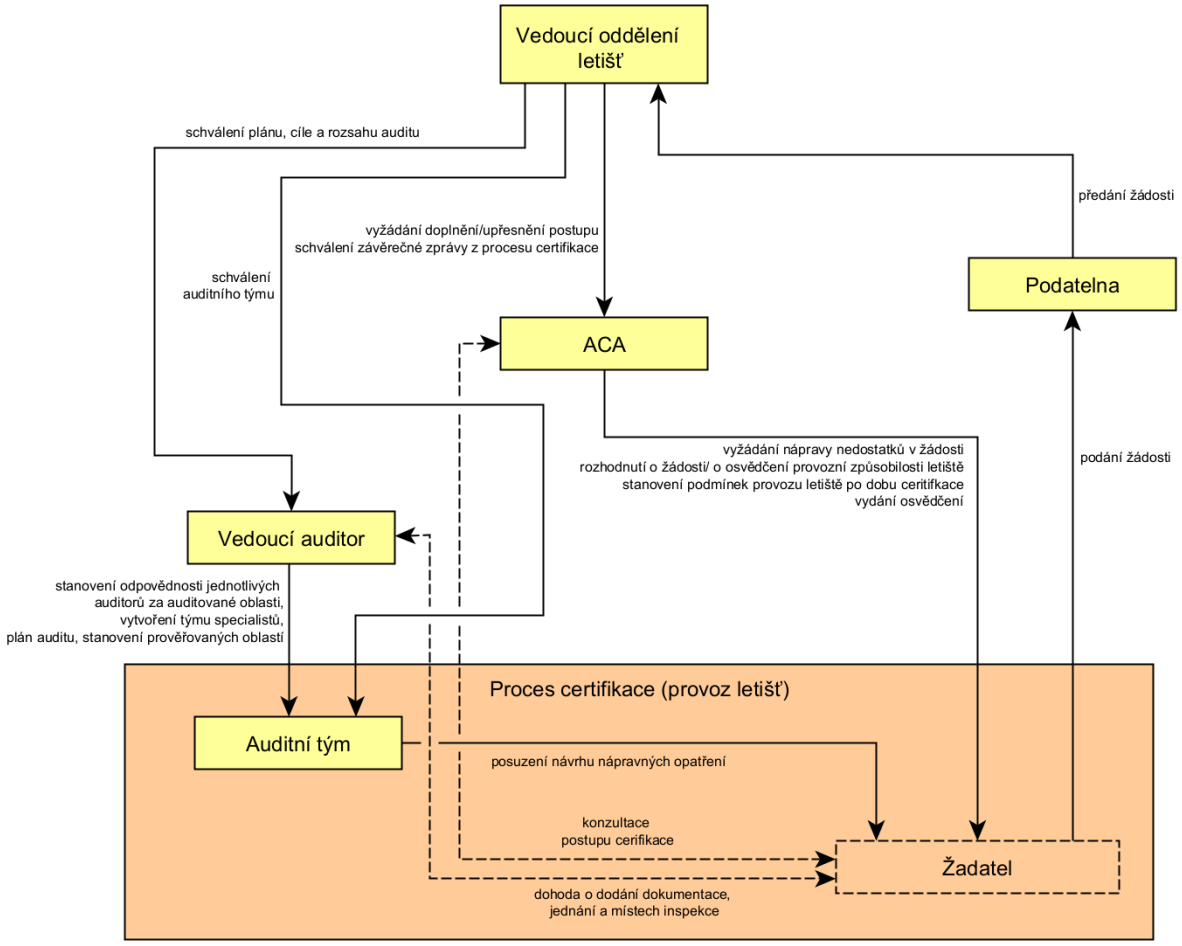
[1] https://www.bonitasoft.com/
[2] https://www.modelio.org/



Obr. 5 - Zobecněná řídící struktura dozorového orgánu

projeví konkrétní aktivity jednotlivých osob (rolí). K tvorbě největšího detailu v řídící struktuře se mohou využít BPMN diagramy, jelikož v nich jsou právě již zmapované jednotlivé role a jejich aktivity, za které jsou zodpovědné. Tím, že jsou aktivity propojené a kontinuálně na sebe navazují, tak je dobře čitelné i to, zda se mezi rolemi (neboli řídícími prvky v STPA) jedná o vazby typu „řídící akce“, „zpětná vazba“ nebo „koordinace“.

Abstrakce řídící struktury slouží následně uživateli (dozorovému orgánu) při dalším využití řídící struktury. Uživatel si může vybrat tu úroveň detailu, kterou v danou chvíli potřebuje. Jako příklad je uveden detail zobecněné řídící struktury (z obr. 5). Obr. 6 ukazuje detailní řídící strukturu pro proces certifikace, který probíhá v rámci oddělení letišť dozorového orgánu. Vazby se šipkami směrem dolů představují vazbu typu řídící akce, vazby směrem nahoru reprezentují vazbu typu zpětná vazba. Přerušovaná vazba pak reprezentuje vazbu typu koordinace.



Obr. 6 - Detail řídící struktury dozorového orgánu zaměřující se na proces certifikace na oddělení letišť

Pro kompletní analýzu nebezpečí pak musí dozorový orgán provést i další kroky STPA analýzy. Je tedy potřeba identifikovat ztráty, systémová nebezpečí a bezpečnostní požadavky (první krok STPA), dále určit nebezpečné řídící akce a požadavky na řídící prvky (třetí krok STPA) a na závěr identifikovat ztrátové scénáře (čtvrtý krok STPA).

Poslední částí je pak identifikace případných předpokladů na základě bezpečnostních požadavků, dle metody Active STPA.

Kompletní analýzou dozorový orgán zjistí své slabiny a může zapracovat na jejich posílení. Zároveň z pohledu systému je takto analýza využitelná i pro interní audity apod.

3.3 Formalizace znalosti o dozorované organizaci

Dozor nad organizacemi v letectví, který vykonává dozorová instituce, lze rozdělit na oblast certifikace a řízení změn a na oblast průběžného dozoru. Do průběžného dozoru patří provádění auditů a inspekcí. Průběžný dozor má za cíl zajistit, aby organizace a fyzické osoby neustále plnily své závazky. Pokud by v rámci průběžného dozoru bylo zjištěno, že organizace nebo fyzická osoba plní funkci v rozporu s předpisovými požadavky, pak je potřeba tento stav urychleně změnit.

Průběžný dozor v organizacích je dozorovým orgánem prováděn pomocí systému plánovaných a neplánovaných auditů a inspekcí. Tyto pomáhají zajistit přijatelnou úroveň bezpečnosti tím, že ověřují, zda jsou veškeré činnosti organizace provozovány bezpečně. Audity prováděné dozorovým orgánem se také často zaměřují na postupy systému řízení provozní bezpečnosti neboli SMS (Safety Management System) a ověření jeho výkonnosti a efektivity.

Pro to, aby mohl dozorový orgán provádět dozorovou činnost nad organizacemi potřebuje znát legislativu týkající se daného typu organizace a zároveň musí mít k dispozici certifikační dokumentaci konkrétní auditované organizace. V případě potřeby si dozorový orgán může vyžádat i podrobnější interní dokumentaci organizace.

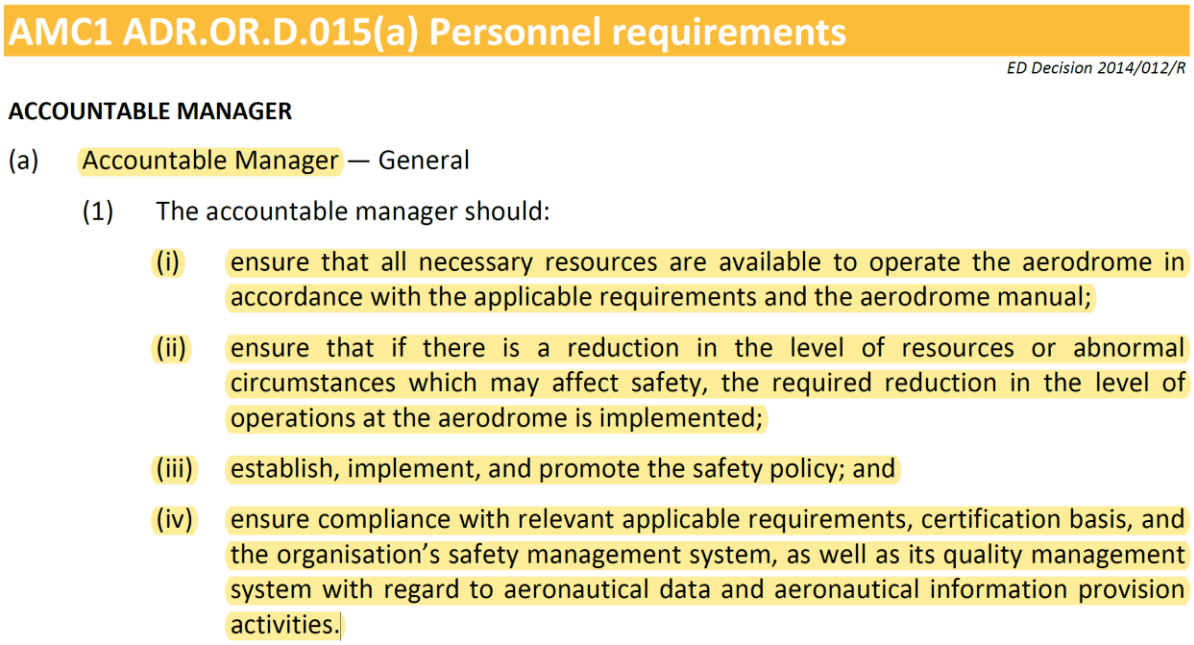
V případě aplikace této metodiky (a tedy systémového myšlení na bázi modelu STAMP) je potřebné si postupně vytvořit formalizovanou základnu pro všechny typy dozorovaných organizací či případně i pro konkrétní jednotlivé organizace. Následující kroky mohou dozorovým orgánům pomoci při tvorbě takové základny.

Dozorový orgán tedy v prvním kroku potřebuje příslušné předpisy či normy, které se vztahují k danému typu organizace. V případě, že chce tvořit formalizovanou základnu pro konkrétní organizaci, může využít přímo certifikační dokumentaci dané organizace. Postup je v obou těchto případech totožný. V certifikační dokumentaci konkrétní organizace jsou informace detailnější a konkrétnější, s jejím využitím tak může být formalizace pro dozorový orgán jasnější a snazší.

Dokumentace je obvykle soubor (ve většině případů formátu PDF), který obsahuje textový popis mimo jiné i potřebných vstupů pro STPA. Dozorový orgán tedy musí nejprve analyzovat dokument a vyhledat řídící prvky, řízené procesy a interakce. V praxi to lze provést tak, že osoba podrobně přečte dokumentaci a vyznačí v ní všechny zmíněné důležité informace (viz obr. 7). Následuje krok tvorby řídící struktury. V tomto kroku osoba vytvoří schéma řídící struktury podle druhého kroku STPA. Ve schématu tak budou zobrazeny anotované informace, tedy řídící prvky, řízené procesy a interakce. Na obr. 8 je znázorněna ukázka řídící struktury pro údržbové organizace, která byla

vytvořena podle předpisu a jedná se tedy o typ organizace, nikoliv o konkrétní organizaci.

Osoba tvořící řídící strukturu typicky začne s tvorbou nejobecnější řídící struktury, která vychází z organizační struktury konkrétní organizace nebo daného typu organizace. Ve většině případů (především u řídící struktury konkrétních organizací) si nevystačíme s obecnější řídící strukturou a je potřeba jít více do detailu. Z toho důvodu je potřeba tvořit také detailnější řídící struktury, které jsou podrobné. V praxi si to lze představit tak, že se v rozbalí např. jedna organizační jednotka/oddělení, a ta ukáže konkrétní řídící prvky a aktivity, které v ní probíhají.



AMC1 ADR.OR.D.015(a) Personnel requirements

ED Decision 2014/012/R

ACCOUNTABLE MANAGER

(a) Accountable Manager — General

(1) The accountable manager should:

(i) ensure that all necessary resources are available to operate the aerodrome in accordance with the applicable requirements and the aerodrome manual;

(ii) ensure that if there is a reduction in the level of resources or abnormal circumstances which may affect safety, the required reduction in the level of operations at the aerodrome is implemented;

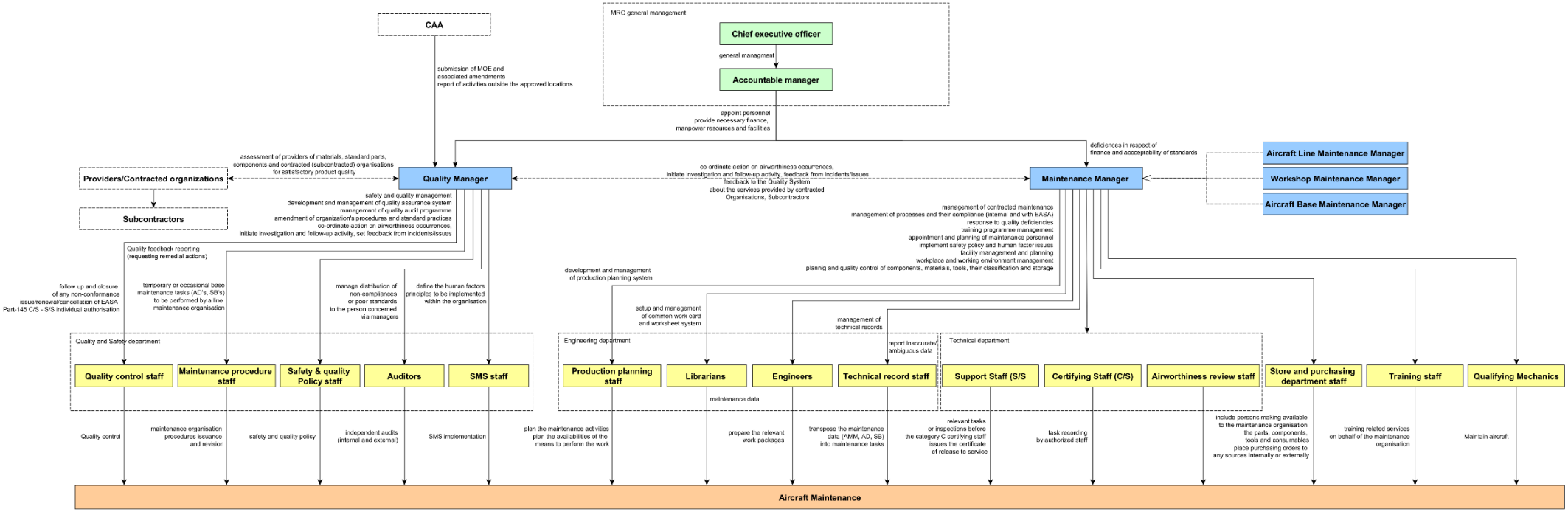
(iii) establish, implement, and promote the safety policy; and

(iv) ensure compliance with relevant applicable requirements, certification basis, and the organisation's safety management system, as well as its quality management system with regard to aeronautical data and aeronautical information provision activities.

Obr. 7 - Ukázka textu legislativního charakteru s vyznačením důležitých částí pro tvorbu řídící struktury dozorované organizace

V rámci prvního kroku STPA musí být definovány ztráty (ztrátové události) a nebezpečí na úrovni systému. Kromě řídící struktury by v rámci druhého kroku STPA měla vzniknout i tabulka, kde jsou vypsané řídící prvky a ke každému řídícímu prvku je definována jeho odpovědnost (činnost kterou udělá daný prvek sám), řídící akce (interakce směrem k podřízenému prvku), zpětná vazba (interakce směrem k nadřazenému prvku) a koordinace (interakce směrem k prvku na stejné úrovni v hierarchii). Tato tabulka (viz tab. 1) ve výsledku zobrazuje stejnou informaci, jako schéma řídící struktury (viz obr. 5, 6 a 8) a dozorovému orgánu poskytne základ či vstup při vytváření nebezpečných řídících akcí (třetí krok STPA).

Dále by měl dozorový orgán specifikovat ztrátové scénáře (čtvrtý krok STPA). K tomu jako vstup slouží tabulka nebezpečných řídících akcí vytvořených v rámci třetího kroku STPA. V neposlední řadě by měla osoba tvořící formalizovanou základnu určit bezpečnostní požadavky, a to na základě existujících systémových nebezpečí, nebezpečných řídících akcí a ztrátových scénářů. Na základě všech předešlých znalostí



Obr. 8 - Ukázka řídící struktury pro údržbové organizace vytvořené na základě legislativy

a primárně z bezpečnostních omezení pak dozorový orgán může specifikovat ještě předpoklady pro daný typ organizace či pro konkrétní organizaci, které by neměly být porušovány.

Tab. 1 - Tabulka řídících prvků

Řídící prvek	Odpovědnost („Responsibility“)	Řídící akce („Authority“)	Zpětná vazba („Accountability“)	Koordinace („Coordination“)
Řídící prvek 1				
Řídící prvek 2				
Řídící prvek 3				

Pokud dozorový orgán vytvoří tuto základnu, může z ní jednoduše vycházet při přípravě auditů (konkrétně při přípravě auditních otázek) nebo také při zpracovávání a vyhodnocování příchozích hlášení o událostech.

3.4 Zpracování a vyhodnocení hlášení od organizací

Jedním z hlavních a důležitých zdrojů pro udržování bezpečnosti na úrovni státu v civilním letectví je systém hlášení leteckých událostí. Systém hlášení leteckých událostí je v základu rozdělen na systém povinného hlášení událostí a na systém dobrovolného hlášení událostí. Systém hlášení leteckých událostí specifikuje nařízení Evropského parlamentu a Rady (EU) č. 376/2014 s prováděcím nařízením Komise (EU) 2015/1018.

Pro dozorový orgán jsou důležité veškeré informace z dozorovaných organizací (včetně povinného i dobrovolného hlášení událostí), které by přispěly k objasnění reálné situace v organizaci, a tak k plánování auditů, resp. ke zlepšování bezpečnosti v organizacích a na úrovni státu.

Vždy když dozorový orgán obdrží hlášení o události, ať už hlášení povinné nebo dobrovolné, tak informace z něho zaznamená v předem definované formě tak, aby byla výstupem sada strukturovaných dat, ve kterých může snadno vyhledávat a filtrovat podle potřeby. Hlášení mohou přicházet v různých datových formátech včetně e-mailu, PDF, E5X atd. Je na každém dozorovém orgánu, jakou formou data sbírá. To znamená, že je možné využít softwarové nástroje ale i klasické tabulkové nástroje, jakým je například MS Excel.

Po obdržení hlášení o události je primárním krokem vytvořit nový záznam v databázi a identifikovat základní informace o události, které je možné získat z obdrženého textu.

Mezi základní informace lze zařadit kategorie, které je možné vidět v modré části tab. 2. Mezi tyto kategorie lze zařadit: ID události, název, datum a čas, kategorii, třídu a typ události (na základě ECCAIRS taxonomie), lokaci a textový popis. V tab. 2 je ilustrativně uveden příklad hlášené události s anonymizací pole ID události, název a datum/čas. V dalších datových polích je vidět zařazení události podle taxonomie ECCAIRS a následuje uvedení lokace a příchozí textový popis události.

Následuje kategorizace hlášené události s pomocí Active STPA (viz žlutá část tab. 2). Prvním důležitým krokem je identifikovat zúčastněné strany. Jedná se o expertní posouzení, kdy uživatel identifikuje konkrétní letecké organizace, které se hlášené události účastnily. Je také možné, že jednu událost nahlásí více osob či organizací a v takovém případě dozorový orgán uloží a zároveň sloučí hlášení vztahující se k jedné události. V tab. 2 je jako účastník ilustrativně zaznamenána organizace „1-LKPR". V této události byla účastníkem pouze jedna organizace, v případě dalších organizací, které by v jedné události figurovaly, by se pokračovalo záznamem 2-XXX, 3-YYY atd.

Poté, co dozorový orgán určí zúčastněné strany (účastníky), je potřeba identifikovat další znalosti z obdrženého hlášení. Ke klasifikaci těchto znalostí dozorový orgán využije existující artefakty STPA vytvořené pro jednotlivé organizace či typy organizací.

Dalším krokem je identifikace ztrát (ztrátových událostí) a systémových nebezpečí, která se objevila v hlášené události. Klasifikace předpokládá použití již existujících artefaktů STPA vytvořených pro všechny zúčastněné letecké organizace. Osoba zaznamenávající událost (uživatel) tak jednoduše vybere jednu nebo více ztrát, která v události nastala a stejně tak i nebezpečí. V tab. 2 je jako ztráta zmíněno „Poškození infrastruktury". V některých hlášeních se ale ztráta objevit nemusí, pokud šlo například jen o incident a nedošlo tak k žádnému zranění či poškození.

Poté, co jsou klasifikovány ztráty a systémová nebezpečí, uživatel klasifikuje, které řídící prvky se podílely na události. Mezi řídící prvky nejčastěji řadíme odpovědné řídící nebo organizační jednotky. Pro uživatele to znamená, že je třeba vybrat z existujících řídících prvků zúčastněných organizací ty prvky, které figuroval v události a byly součástí vzniklého nebezpečí potažmo i ztráty. Uživatel tedy jednoduše vybere jeden nebo více řídících prvků dostupných v příslušných artefaktech STPA.

Po klasifikaci řídících prvků lze klasifikovat řízené procesy/aktivity, které souvisí s řídícími prvky. Měly by být vybrány pouze řízené procesy, které se týkají zúčastněných leteckých organizací a za které odpovídají vybraní řídící (řídící prvky). Uživatel by opět vybírá jeden nebo více řízených procesů dostupných v příslušných artefaktech STPA nebo případně vyhledá příslušný řízený proces v dokumentaci organizace (v případě, že takový proces v artefaktech STPA chybí) a doplní ho do seznamu řízených procesů.

Následuje výběr z bezpečnostních požadavků/předpokladů („constraints/assumptions"), konkrétně jde tedy o to, které bezpečnostní požadavky a předpoklady byly při události porušeny. Tento výběr je již omezen vybranými řídícími prvky, systémovým nebezpečím a řízenými procesy, které byly klasifikovány

Tab. 2 - Ukázka záznamu a zpracování hlášené události

ID události	Název	Datum/čas	Kategorie události	Třída události	Typ události	Lokace	Textový popis
314.....587	Požár XXX/027/20XX	Fri Mar XX 19:28:00 CET 20XX	24 - ADRM: Aerodrome	300 - Incident	5020800 - Main power	LKPR	Požár T2 na hlavní trafostanici. Vypnutí napájení během požárního zásahu mělo za následek zhasnutí plošného osvětlení odbavovací plochy u T1. Plné obnovení napájení v 19:51 LT.

Kategorizace pomocí Active STPA							
Účastník	**Ztrátová událost**	**Systémové nebezpečí**	**Odpov. řídící/ Org. jednotka**	**Aktivita/ Proces**	**Porušené předpoklady**	**Trend**	**Kauzální faktory**
1-LKPR	L-3: Poškození infrastruktury	H1.1: Infrastruktura letiště obsahuje překážky/ provozní omezení	OJ HZS: Hasičský záchranný sbor	Dohled nad elektronickým systémem požární signalizace Požární zásah	A1 – Letištní infrastruktura je zajištěna proti externím vlivům (např. počasí) A3 – Letištní infrastruktura a systémy poskytují službu dle požadavků (např. čas, technické parametry atd.)	-	-

v předchozích krocích. Uživatel jednoduše vybere jedno nebo více bezpečnostních omezení/předpokladů dostupných v příslušných artefaktech STPA.

Poslední částí tab. 2 jsou datová pole „Trend" a „Kauzální faktor". Tato datová pole lze vyplnit, pokud je možné tyto informace zjistit. Pole „Trend" je možné doplnit v případě, že se podobná událost v jedné organizaci či ve stejném typu organizace vyskytuje častěji a uživatel chce na tuto skutečnost upozornit v datech. K vyplnění této informace je potřeba mít dostatečné množství dat za delší časové období, ze kterého lze takovou informaci vyčíst. Pro vyplnění pole „Kauzální faktor" musí být tato informace čitelná z hlášení události. Pokud tomu tak není, datové pole zůstává prázdné. Kauzální faktor je možné doplnit i zpětně, pokud je událost šetřena.

Tab. 2 ukazuje příklad pouze jedné události. Pokud bude dozorový orgán postupovat stejným způsobem s každým příchozím hlášením o události a bude tak klasifikovat každou událost, vznikne databáze, ze které může být tvořen tzv. bezpečnostní panel („safety dashboard"), v němž lze sledovat statistické přehledy nad celou databází.

Příkladem může být tab. 3, kde je uveden přehled kolik ztrátových událostí nastalo v jedné organizaci za dané časové období. Podobný přehled uvádí i tab. 4, která říká, kolikrát byl porušen určitý předpoklad za dané období v jedné organizaci. Podobné přehledy je možné tvořit pro jakoukoliv kategorii z tab. 2 a dozorové orgány mohou použít například i reprezentaci pomocí grafů. Důležité je přehledy pravidelně aktualizovat a vycházet z nich při přípravě bezpečnostních auditů a inspekcí a v rámci dalších činností dozorového orgánu.

Tab. 3 - Přehled počtu ztrátových událostí v jedné organizaci za dané období

ID	Ztrátové události (Ztráty)	Počet
L-1	Ztráty na životech nebo zranění osob	0
L-2	Poškození nebo zničení letadla	11
L-3	Poškození infrastruktury	5
L-4	Ztráta reputace	0
L-5	Poškození životního prostředí	1

Tab. 4 - Přehled počtu porušených předpokladů v jedné organizaci za dané období

ID	Předpoklady	Počet porušení
A1	Letištní infrastruktura je zajištěna proti externím vlivům (např. počasí)	19
A2	Plánovaná zátěž pracovníků nepřesáhne jejich dimenzovanou kapacitu	3
A3	Letištní infrastruktura a systémy poskytují službu dle požadavků (např. čas, technické parametry atd.)	12
A4	Zvýšení provozu letištní infrastruktury nepřesáhne dimenzovanou kapacitu	0

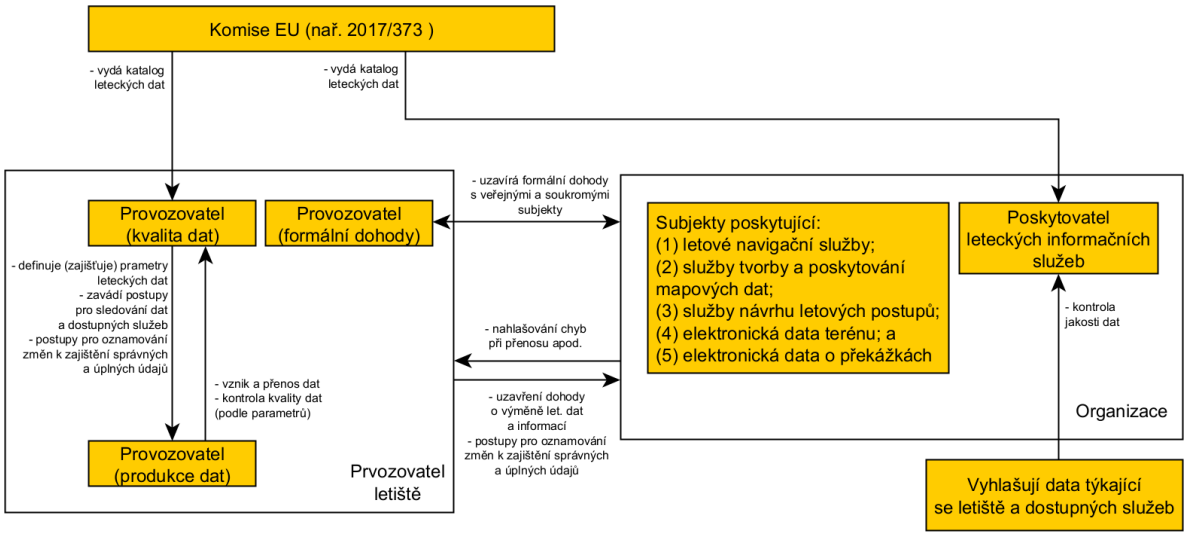
3.5 Auditní činnost

V rámci systému sledování shody koná dozorový orgán pravidelné audity v organizacích, které jsou jím dozorovány. Audity založené na systému sledování shody neboli „compliance-based" audity jsou prováděné tak, že se ověřuje, zda sledovaná organizace splňuje legislativní požadavky, a to přímým porovnáním stavu organizace s konkrétními požadavky. Kromě auditů založených na shodě existuje i možnost audit doplnit o tzv. „performance-based" auditní otázky neboli otázky založené na skutečné výkonnosti vyplývající z dat hlášení událostí a případně předešlých auditů a inspekcí.

3.5.1 Příprava a provedení auditu

Ve chvíli, kdy auditor ví, jakou organizaci půjde auditovat, může začít s přípravou auditních otázek. Pokud už jsou pro organizaci či pro typ organizace vytvořené STPA artefakty, tak auditor použije již hotovou STPA a vybere si pouze ty části řídící struktury, které jsou pro něho v rámci auditu stěžejní. Pokud mu ale potřebný detail či část řídící struktury chybí, je třeba ho vytvořit.

Auditor při běžném auditu využívá legislativní dokumentaci, a právě ta mu dobře poslouží i při tvorbě řídící struktury (druhý krok STPA). Auditor prochází dokumentaci, kterou zároveň využívá i pro přípravu klasického compliance-based auditu. V dokumentaci si označí důležité části a následně je převede do grafické podoby neboli do řídící struktury STPA (viz obr. 9). Poté, co je řídící struktura vytvořena je potřeba postupovat stejně jako při běžné STPA analýze, tedy vytvořit nebezpečné řídící akce („unsafe control actions"), bezpečnostní požadavky vztahující se k řídícím prvkům („controller constraints") a následně ztrátové scénáře („loss scenarios"). Pokud je STPA analýza již hotová např. z předchozího auditu, auditor pouze zkontroluje aktuálnost a případně upraví rozdílné části analýzy.



Obr. 9 - Ukázka řídící struktury vytvořené podle dokumentace týkající se požadavků na jakost dat

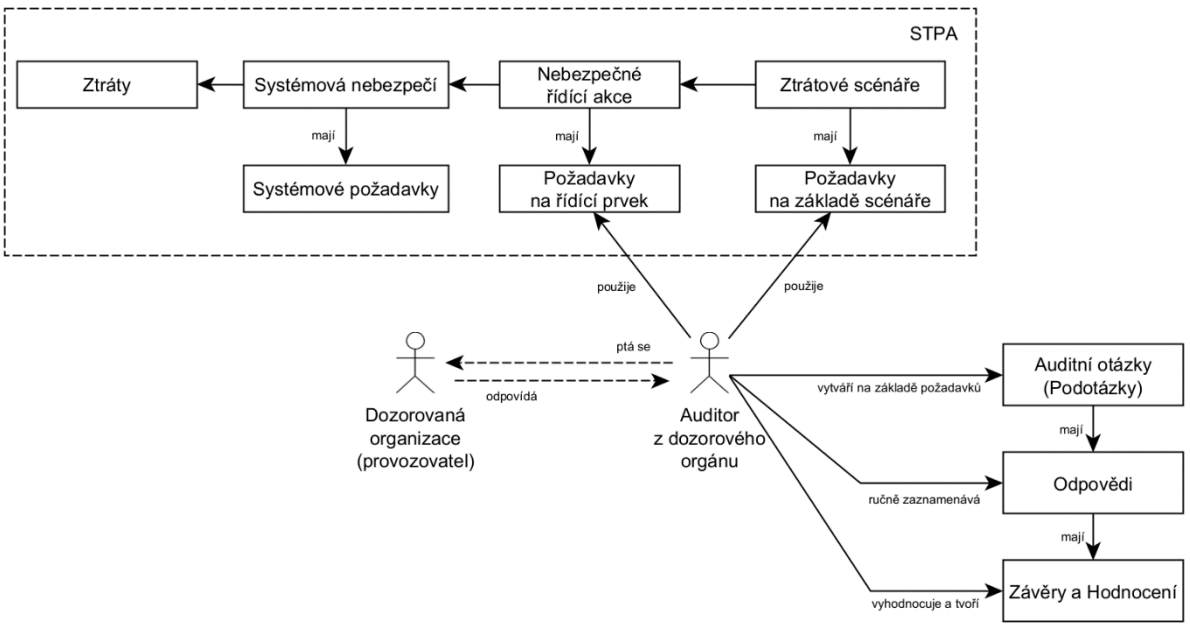
Následuje tvorba požadavků vztahující se k jednotlivým ztrátovým scénářům (viz tab. 5). Tyto požadavky mohou být taktéž připraveny předem, opět je ale třeba ověřit jejich aktuálnost a případně je upravit. Stejně tak by měly být vytvořeny či aktualizovány i předpoklady pro daný typ organizace. Poté, co jsou požadavky a předpoklady vytvořeny nebo aktualizovány, může auditor tvořit auditní otázky. Pro prioritizaci požadavků (či auditních otázek) je dobré také předem zkontrolovat výkonnost v bezpečnosti dané organizace pomocí např. počtu nastalých událostí, typů problémů či nápravných opatření z předchozích auditů.

Následujícím krokem auditora je tedy tvorba auditních otázek. V tomto kroku auditor převede předpoklady a bezpečnostní požadavky do auditních otázek a tímto způsobem nastaví kontrolní seznam neboli checklist pro audit (viz tab. 5). Auditor se podívá na vybrané bezpečnostní požadavky a převede je do otázek a podotázek. Alternativně by mohl být tento krok i automatizován, nicméně je vhodné, aby auditor otázky upravil pro konkrétní potřeby auditu. Automaticky generovaná otázka by totiž nemusela být úplně přesná či samovysvětlující, pokud by jí auditor nedodal potřebný kontext. Upřesňující kontext lze doplnit pomocí propojení otázky (vytvořené z požadavků a předpokladů na základě ztrátových scénářů) a konkrétnějšího požadavku vztahujícího se k řídícímu prvku a potažmo i ke konkrétní činnosti tohoto řídícího prvku. Jak ukazuje tab. 5, červený požadavek je pro auditní otázku základem a modrý požadavek dodává patřičný kontext, v jakém by se měl auditor organizace dotazovat. Tvorba auditních otázek je do značné míry založena na zkušenostech a znalostech auditora, a to je důvodem, proč plná automatizace ve tvorbě auditních otázek tohoto typu zatím není plně využitelná.

Obr. 10 ukazuje schematicky, jak probíhá příprava auditních otázek, následný audit v dozorované organizaci, záznam odpovědí a jejich následné vyhodnocení.

Tab. 5 - Příklad převodu požadavků na auditní otázky

Ztrátový scénář	Požadavek na základě scénáře	Požadavek na řídící prvek		Auditní otázka
Provozovatel nedefinuje parametry leteckých dat, když je původce dat [UCA-1a], protože nemá dostatek personálu.	- provozovatel musí mít dostatek personálu	CC-1a Provozovatel musí definovat parametry leteckých dat, když je původce dat.		Má provozovatel dostatek personálu (pro definování parametrů leteckých dat)?
Provozovatel nezavede postupy posuzování a zmírňování rizik v oblasti zabezpečení údajů, když je původce dat [UCA-5a], protože neví, že má takové postupy zavést.	- provozovatel musí mít povědomí o tom, že má zavést postupy pro posuzování a zmírňování rizik	CC-5a Provozovatel musí zavést postupy posuzování a zmírňování rizik v oblasti zabezpečení údajů, když je původce dat.		Má provozovatel k dispozici potřebnou dokumentaci pro zavádění postupů (posuzování a zmírňování rizik v oblasti zabezpečení údajů)? - Jak postupy vypadají? - Jak reálně postupy fungují?
Provozovatel zavede postupy pro sledování dat a dostupných služeb se zpožděním, když už sběr dat probíhá [UCA-2c], protože musí udělat ještě dodatečnou úpravu.	- provozovatel musí zavést postupy způsobem, kdy veškeré úpravy jsou zapracovány před jejich plánovaným zavedením	CC-2c Provozovatel musí zavést postupy pro sledování dat a dostupných služeb včas, když ještě sběr dat neprobíhá.		Má provozovatel dostatek času na zavádění nových postupů a počítá se závěrečnými úpravami/změnami před uvedením do provozu? - Jak se řeší dodatečné úpravy dokumentů? - Jak se změna propaguje, aby o ní měli zaměstnanci povědomí?



Obr. 10 - Schéma přípravy a provedení auditu na základě STPA

3.5.2 Záznam výsledků auditu

V rámci provádění samotného auditu se auditor ptá na předem připravené auditní otázky a musí být připraven otázky v případě potřeby organizaci dodatečně vysvětlit, pokud by jí nebylo něco jasné. Organizace následně zodpovídá položenou otázku a auditor si její odpověď podrobně zaznamenává a případně se doptává na nejasné části či připravené podotázky (viz tab. 5). Po dokončení auditu musí auditor provést zhodnocení jednotlivých otázek, a to ve formě, zda organizace požadavek splňuje, nesplňuje nebo splňuje částečně (implementováno, neimplementováno, implementováno částečně), jak je možné vidět v posledním sloupci tab. 6.

Tab. 6 - Záznam odpovědí z auditu a jeho zhodnocení

Ztrátový scénář	Požadavek na základě scénáře	Požadavek na řídící prvek		Auditní otázka	Odpověď	Zhodnocení
Provozovatel nedefinuje parametry leteckých dat, když je původce dat [UCA-1a], protože nemá dostatek personálu.	- provozovatel musí mít dostatek personálu	CC-1a Provozovatel musí definovat parametry leteckých dat, když je původce dat.		Má provozovatel dostatek personálu (pro definování parametrů leteckých dat)?	Podrobný záznam odpovědi	nesplňuje
Provozovatel nezavede postupy posuzování a zmírňování rizik v oblasti zabezpečení údajů, když je původce dat [UCA-5a], protože neví, že má takové postupy zavést.	- provozovatel musí mít povědomí o tom, že má zavést postupy pro posuzování a zmírňování rizik	CC-5a Provozovatel musí zavést postupy posuzování a zmírňování rizik v oblasti zabezpečení údajů, když je původce dat.		Má provozovatel k dispozici potřebnou dokumentaci pro zavádění postupů (posuzování a zmírňování rizik v oblasti zabezpečení údajů)? - Jak postupy vypadají? - Jak reálně postupy fungují?	Podrobný záznam odpovědi	splňuje částečně
Provozovatel zavede postupy pro sledování dat a dostupných služeb se zpožděním, když už sběr dat probíhá [UCA-2c], protože musí udělat ještě dodatečnou úpravu.	- provozovatel musí zavést postupy způsobem, kdy veškeré úpravy jsou zapracovány před jejich plánovaným zavedením	CC-2c Provozovatel musí zavést postupy pro sledování dat a dostupných služeb včas, když ještě sběr dat neprobíhá.		Má provozovatel dostatek času na zavádění nových postupů a počítá se závěrečnými úpravami/změnami před uvedením do provozu? - Jak se řeší dodatečné úpravy dokumentů? - Jak se změna propaguje, aby o ní měli zaměstnanci povědomí?	Podrobný záznam odpovědi	splňuje

Záznam kompletní odpovědi během auditu slouží tedy primárně k závěrečnému zhodnocení auditu. Nicméně zaznamenané odpovědi organizace dobře slouží i v případě následujícího auditu, kdy po daném časovém období provádí auditor audit znovu a potřebuje ověřit, zda organizace zlepšila své postupy či zda zavedla účinná nápravná opatření.

4 Popis uplatnění certifikované metodiky

Metodiku lze uplatnit několika způsoby, a to z pohledu obsahu a formy uplatnění. Dozorovým orgánům uplatňujícím metodiku se doporučuje zvážení obou aspektů při zavádění postupů popsaných v tomto dokumentu.

Z pohledu obsahu lze uplatnit metodiku jako celek, nebo některé z jejích částí samostatně. Všechny postupy jsou na sebe navázané a nabízejí synergický efekt při jejich uplatnění jakožto celku, technicky však lze některé uplatnit i samostatně a pro další účely, které nejsou předmětem této metodiky. Lze např. aplikovat tvorbu řídící struktury dle STAMP a tu použít pro pochopení skutečného fungování dozorového orgánu nebo dozorované organizace, formou organizačního diagramu. Některé postupy jsou však závislé na jiných a nelze je aplikovat samostatně. Jedná se zejména o postupy zpracování a vyhodnocení hlášení od organizací a tvorbu auditních otázek či záznam odpovědí na ně. Tyto postupy vyžadují existenci artefaktů na bázi STPA, které jsou produktem ostatních postupů a je tak potřebné je aplikovat společně. Rozhodnutí o uplatnění metodiky z pohledu obsahu je vhodné provést ve spolupráci s kvalifikovaným personálem, který je schopen posoudit uplatnitelnost a potenciální přínos konkrétních postupů v daném dozorovém orgánu, s ohledem na jeho specifika.

Z pohledu formy uplatnění existuje také několik možností. Jako základní uplatnění se předpokládá převzetí postupů uvedených v tomto dokumentu a jejich zavedení do stávající infrastruktury a softwarového vybavení konkrétní organizace. Takové uplatnění předpokládá, že stávající infrastruktura dozorového orgánu umožňuje implementaci daných postupů buď přímo, nebo formou její přímé modifikace. Rozsáhlejší formou uplatnění této metodiky je implementace dodatečných softwarových nástrojů, které jsou zmíněny v tomto dokumentu. V takovém případě organizace přijímá externí softwarové řešení pro vybrané části postupů a je nezbytné zvážit otázky začlenění takových nástrojů do stávající infrastruktury dozorového orgánu. Rozhodnutí o formě uplatnění je také vhodné provést na základě odborného posouzení možností uplatnění kvalifikovaným personálem.

Pro dosažení maximálního synergického efektu při aplikaci této metodiky lze doporučit uplatnění všech postupů uvedených v tomto dokumentu při současném využití dedikovaných softwarových nástrojů pro podporu tvorby procesních diagramů (editory pracující s BPMN a dalšími typy procesních diagramů) a STPA artefaktů (grafické editory pro tvorbu blokových schémat, aplikace MS Office pro ukládání tabulek). Pro archivaci dat z hlášení o událostech, auditních otázek a výsledků auditů lze použít aplikace MS Office.

5 Ekonomické aspekty

Uplatnění metodiky s sebou nese několik nákladů, které je potřeba zvážit. Postupy uvedené v tomto dokumentu jsou jako celek časově náročnější, než postupy obvyklé v dozorových orgánech a vyžadují navíc rozšíření kvalifikace personálu, který pracuje s daty o bezpečnosti. Důvodem je zejména udržování modelů na bázi STPA, které

reprezentují vlastní fungování dozorového orgánu, jakož i fungování dozorovaných organizací. U postupů, které formalizují procesní dokumentaci dozorového orgánu lze naopak očekávat dopad opačný a sice, že po zavedení takového postupu bude čas potřebný na udržování procesní dokumentace menší, a to i navzdory zvýšení její kvality. Důvodem je absence potřeby analyzovat textové dokumenty jako celek, aby byly identifikovány části, které je nutné aktualizovat, a absence potřeby upravovat jednotlivé části textu při snaze zachovat jeho celistvost a návaznost. Schematicky a graficky modelovaná procesní dokumentace vyžaduje pouze úpravu náležitých částí schémat, které jsou snáze dohledatelná softwarovými nástroji určenými pro správu takových modelů, v porovnání s běžnými textovými editory jako je Microsoft Word. Tato skutečnost omezuje negativní dopad celkově zvýšených pracovních nároků. Výsledná bilance časové náročnosti úplného uplatnění této metodiky však závisí na množství dozorovaných institucí a komplexitě procesů konkrétního dozorového orgánu a nelze jí stanovit stejnou pro každý dozorový orgán.

Z pohledu zavádění postupů této metodiky vyvstává zejména otázka školení personálu, který má za úkol zpracovávat data o bezpečnosti, a dále otázka úpravy či rozšíření softwarové infrastruktury. Z pohledu školení lze předpokládat přibližně třídenní workshop, který zajistí dostatečnou kvalifikaci veškerého personálu pracujícího s modelem bezpečnosti STAMP a artefakty, které z této práce vyplývají. Z pohledu úpravy či rozšíření softwarové infrastruktury náklady závisí na formě uplatnění metodiky. Pro snížení nákladů s tím spojených lze doporučit využití nástrojů uvedených v této metodice, které všechny existují ve volně dostupné verzi, tedy bez licenčních poplatků. Komplexnější integrace postupů ve formě úpravy existující softwarové infrastruktury nese spolu s integrací i potenciál automatizace částí postupů této metodiky, např. formou využití dat a číselníků z jednoho artefaktu (např. BPMN modelu) v artefaktu druhém (např. řídící struktuře dozorového orgánu). Jedná se o nákladnější variantu díky potřebě programátorských prací, která ale z dlouhodobého hlediska může být výhodná zejména tím, že šetří pracovní čas jednotlivých zaměstnanců dozorového orgánu. Náklady spojené se softwarovou infrastrukturou také závisí na množství dozorovaných institucí a na komplexitě procesů konkrétního dozorového orgánu a nelze tak jednoznačně stanovit preferovaně výhodnou formu uplatnění.

Z pohledu ekonomických přínosů přináší využití modelu bezpečnosti STAMP pro dozorové orgány nové možnosti identifikace nebezpečí a hodnocení rizik či výkonnosti v bezpečnosti, které vedou k lepší identifikaci bezpečnostních problémů. Lepší identifikaci lze chápat ve smyslu časovém, formou včasné predikce, oproti stávajícím postupům, nebo také ve smyslu odhalení podstaty bezpečnostních problémů, díky vysvětlování bezpečnosti jakožto problému řízení, a to navíc pouze s popisem běžného fungování leteckých organizací, bez potřeby historických dat či expertní znalosti v doméně konkrétní organizace. Včasná identifikace bezpečnostních problémů a větší kontrola nad zajišťováním bezpečnosti přináší úspory v nákladech na prevenci a odstraňování následků bezpečnostních událostí, které zvyšují dostupnost a konkurenceschopnost letecké dopravy.

Ekonomické přínosy lze spatřit také v oblasti procesního řízení dozoru nad bezpečností. Postupy s využitím modelu bezpečnosti STAMP díky svému holistickému přístupu vytváří modely, které kromě řízení bezpečnosti a dozorové činnosti lze využít také pro optimalizací procesů dozorového orgánu, např. formou úpravy odpovědností a distribuce práce napříč jednotlivými organizačními jednotkami či rolemi zaměstnanců. Toto ve výsledku může vést ke krácení časové náročnosti konkrétních pracovních postupů a v důsledku k úsporám ve formě snížení personálních nákladů.

Seznam použité literatury

[1] LEVESON, N. Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. ISBN 978-0-262-01662-9.

[2] LEVESON, N. a J. THOMAS. STPA Handbook, 2018. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[3] LEVESON, N. CAST Handbook: How to Learn More from Incidents and Accidents, 2019. Dostupné z: http://sunnyday.mit.edu/CAST-Handbook.pdf.

[4] CASTILHO, D. Active STPA: Integration of Hazard Analysis into a Safety Management system Framework. Dissertation, Massachusetts Institute of Technology (MIT), 2019.

[5] ICAO. Doc. 9859: Safety management manual (SMM). 4th edition. Montréal, Quebec: International Civil Aviation Organization (ICAO), 2018. ISBN 978-92-9258-552-5.

[6] ŘEPA, Václav. Podnikové procesy: procesní řízení a modelování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2007. Management v informační společnosti. ISBN 97880-247-2252-8.

[7] LEDVINKA, M., P. KŘEMEN, L. SAEEDA a M. BLAŠKO. TermIt: A Practical Semantic Vocabulary Manager. In: Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 1: ICEIS. 22nd International Conference on Enterprise Information Systems (ICEIS 2020), Prague. Porto: SciTePress - Science and Technology Publications, 2020. s. 759-766.

[8] STRIPPEL, Christian, Laura LAUGWITZ, Sünje PAASCH-COLBERG, Katharina ESAU a Annett HEFT. BRAT Rapid Annotation Tool. Medien & Kommunikationswissenschaft [online]. 2022, 70(4), 446-461. ISSN 1615-634X.

Seznam publikací, které předcházely metodice

GRÖTSCHELOVÁ, K., A. LALIŠ a N. GUSKOVA. Systemic Safety Data Collection and Processing in Aviation Safety Oversight. In: 2021 International Conference on Military Technologies (ICMT). Brno, 2021-06-08/2021-06-11. Praha: IEEE Czechoslovakia Section, 2021. ISBN 978-1-6654-3724-0. DOI 10.1109/ICMT52455.2021.9502826. Dostupné z: https://ieeexplore.ieee.org/document/9502826/

KAFKOVÁ, M., S. STOJIĆ a A. LALIŠ. Improving Safety Studies through Application of Deviation Concept. In: HANÁKOVÁ, L. a V. SOCHA, eds. Safety & Security Conference Prague 2019. Praha, 2019-11-20/2019-11-21. Praha: IRIS - Rudolf Valenta, 2019. s. 49-55. ISBN 978-80-907724-0-3.

KŘEMEN, P. et al. Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems. Journal of Aerospace Information Systems. 2017, 14(5), 279-292. ISSN 1940-3151. DOI 10.2514/1.I010441.

LEDVINKA, M., A. LALIŠ a P. KŘEMEN. Toward Data-Driven Safety: An Ontology-Based Information System. Journal of Aerospace Information Systems. 2019, 16(1), 22-36. ISSN 1940-3151. DOI 10.2514/1.I010622.