METODIKA

pro zefektivnění analýzy a řízení rizik s využitím konceptuálního modelování

Výzkumný projekt TA ČR Zéta č. TJ01000377

Ústav letecké dopravy Fakulta dopravní ČVUT v Praze	Katedra kybernetiky Fakulta elektrotechnická ČVUT v Praze	Letiště Praha, a.s.	Czech Airlines Technics, a.s.
Hanáková Lenka, Ing. Lališ Andrej Ing., Ph.D. Stojić Slobodan Ing., Ph.D.	Ahmad Jana, Ing. Kostov Bogdan, Ing.	Kafková Markéta, Ing.	Szentkeresztiová Katarína, Ing.

Program Zéta

Metodika pro zefektivnění analýzy a řízení rizik s využitím konceptuálního modelování

Obsah

Úvod 2
1. Cíl metodiky 3
2. Dedikace 3
3. Popis metodiky 3
3.1 Teorie bezpečnosti dle modelu STAMP 3
3.2 Ontologie modelu bezpečnosti STAMP 7
3.3 Aplikace vyvinuté ontologie modelu bezpečnosti STAMP 13
3.3.1 Základní informace k aplikaci 13
3.3.2 Aplikace ontologie na kroky metodiky CAST 14
3.3.3 Praktická doporučení 19
3.4 Využití provozní dokumentace a jejích nástrojů 20
3.4.1 Popis řídící smyčky 21
3.4.2 Knihovna řídících prvků 22
4. Srovnání novosti postupů se současnými standardy 22
4.1 Srovnání novosti v kontextu metodiky CAST 23
4.2 Srovnání novosti v kontextu standardu letecké dopravy 24
5. Popis uplatnění certifikované metodiky 24
6. Ekonomické aspekty 25
Seznam použité literatury 26
Seznam publikací, které předcházely metodice 27
Příloha 1: Volný překlad klíčových pojmů z teorie STAMP 28
Příloha 2: Ukázka aplikace ontologie STAMP na průmyslové situace z domény letišť 29

Úvod

Sběr, zpracování a vyhodnocení dat o bezpečnosti patří mezi základní a zcela nezbytné funkcionality každého systému řízení provozní bezpečnosti (Safety Management System - SMS [1,2]). V komplexních socio-technických systémech jako je letectví je značně nepraktické, ne-li zcela nemožné, aby informace o provozu leteckých společností byly uchovávány v jednoduchých softwarových nástrojích navržených např. v prostředí MS Excel nebo MS Access a přitom kvalita a obsah dat odpovídaly potřebám dnešního provozu, zejména v kontextu výkonnostně orientovaných procesů řízení bezpečnosti. Ve skutečnosti trpí celou řadou nedostatků i pokročilejší systémy pro sběr a zpracování dat o bezpečnosti a je to právě komplexita leteckého provozu, která prakticky znemožňuje zaznamenání úplného obrazu řízeného systému, nebo konkrétní události, čímž se stává běžnou praxí, že bezpečnostní záznamy do značné míry odpovídají konceptualizaci konkrétního bezpečnostního analytika, který je vytváří a dále spravuje [3]. Zatím co existují snahy o standardizaci postupů a obsahu dat pomocí platné legislativy a předpisů [4,5], nebo také vývojem leteckých bezpečnostních taxonomií, tyto vychází z dlouholeté praxe leteckého provozu a zažitých modelů jako je SHELL nebo Reasonův model [6], známý také jako model švýcarského sýra. Jedná se nepochybně o ověřenou praxi, která umožnila dosažení dnešní vysoké úrovně bezpečnosti civilního letectví, nicméně teorie bezpečnosti se vyvíjí dále a již dnes existují zcela konkrétní vize dalšího pokroku v této oblasti [7].

Potřeba dalšího zlepšování se může s ohledem na dnešní úroveň bezpečnosti zdát ne příliš zásadní, je potřeba si však uvědomit, že letectví samotné se vyvíjí a že jedním z rysů tohoto vývoje je neustále se zvyšující komplexnost a provázanost provozu, která se projevuje ve složitosti a omezené schopnosti predikovat moderní letecké nehody a incidenty. Dále je možné pozorovat zvyšující se tempo obměny a inovace využívané technologie, častokrát nelze nabýt dostatečné zkušenosti s konkrétním systémem, jelikož dochází k jeho změně, aktualizaci nebo nahrazení dřív, než by bylo možné nabýt dostatečný vzorek dat z jeho provozu [8]. V neposlední řadě se také objevují nová nebezpečí, jako např. provoz bezpilotních prostředků nebo zavádění nových druhů automatizace, které přispívají k tvorbě nových relací mezi účastníky letového provozu, a které mohou rezonovat napříč celým leteckým odvětvím a přispívat tak k novým druhům leteckých nehod a incidentů. Nelze tedy s jistotou tvrdit, že současná úroveň bezpečnosti letecké dopravy je stabilní a že bude s využitím současných nástrojů zachována i v kontextu budoucího vývoje průmyslu.

V současné situaci existuje příležitost dalšího vývoje s pomocí dostupné teorie bezpečnosti, která je dnes orientována na celosystémový přístup k řízení bezpečnosti a která se snaží uchopit systémové jevy komplexity, rezonance nebo emergence [3,8,9]. Tato metodika staví na jednom z prvních systémových modelů bezpečnosti – modelu STAMP (System-Theoretic Accident Model and Processes) [8], který byl vyvinut na univerzitě MIT (Massachusetts Institute of Technology) ve Spojených státech amerických. Tento model byl vybrán zejména proto, že je svým obsahem nejbližší současnému stavu řízení bezpečnosti v letecké dopravě a nabízí další možnosti pro vývoj, bez zásadních změn v chápání bezpečnostních problémů. Metodika se zaměřuje na využití systémové teorie a modelu STAMP v systémech pro sběr a vyhodnocení bezpečnostních dat v letecké dopravě. Pro dosažení potřebné praktické aplikovatelnosti je zde využita moderní technologie ontologického inženýrství [10], které umožňuje tvorbu technicky pokročilých systémů pro sběr a vyhodnocení bezpečnostních dat. Tato technologie zároveň umožňuje tvorbu a správu kvalitních dat a díky ukotvení jejich

konceptualizace redukuje negativní dopad individuální interpretace bezpečnostního analytika na jejich kvalitu.

1. Cíl metodiky

Metodika si klade za cíl diseminovat výsledky realizovaného výzkumu Českým vysokým učením technickým v Praze ve spolupráci se společnostmi Letiště Praha, a.s. a Czech Airlines Technics, a.s. v projektu č. TJ01000377 s podporou Technologické agentury České republiky. Metodika je souhrnem znalostí z projektu a obsahuje klíčové postupy pro zavedení nových funkcionalit pro podporu analýzy a řízení rizik pomocí návrhu nového schématu pro sběr a vyhodnocení dat o bezpečnosti a tímto cílí na další zvyšování úrovně provozní bezpečnosti zejména v leteckém průmyslu, ale také s přesahem do ostatních rizikových průmyslů.

2. Dedikace

Metodika je primárně určena pro střední a větší podniky v letecké dopravě, které plánují zavést anebo již mají zaveden systém pro sběr a zpracování dat o bezpečnosti letového provozu, obvykle v rámci systému řízení bezpečnosti SMS, a které chtějí tento systém dále rozšiřovat s využitím nejnovější teorie bezpečnosti. Metodiku lze také aplikovat i v jiných rizikových průmyslech jako je jaderná energetika, chemický průmysl nebo v armádě, zejména jako podporu pro detailnější identifikaci nebezpečí a následné zefektivnění analýzy a řízení rizik, s využitím celosystémového přístupu k řízení bezpečnosti. I když je vlastní postup popsán v této metodice obecně, v případě aplikace na jiné domény, než je letecká doprava, metodika nezaručuje úplnou shodu se specifikacemi těchto domén a je proto třeba zvážit potřebu její modifikace.

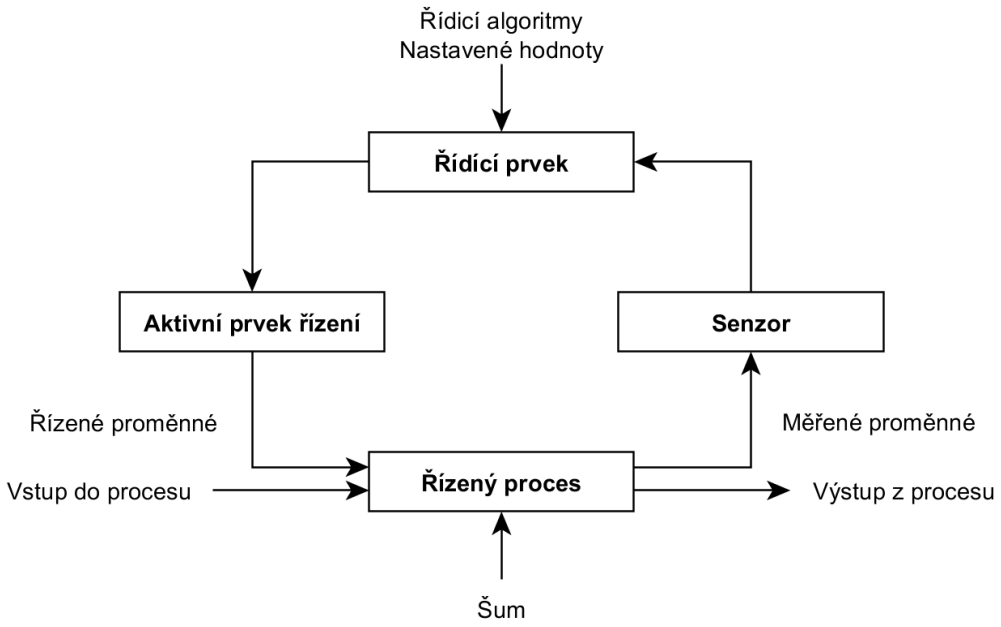
3. Popis metodiky

Tato kapitola obsahuje vlastní popis klíčových postupů nového schématu pro sběr a vyhodnocení dat o bezpečnosti. Metodika nabízí technické prostředky pro realizaci systému sběru a zpracování dat o bezpečnosti kompatibilního s jinými systémy a technologiemi, které se využívají v letecké dopravě, a je primárně určena pro technický a inženýrský personál zabývající se vývojem a implementací těchto systému v leteckých organizacích. Protože je metodika založena na teorii modelu STAMP a na jeho formální reprezentaci pomocí vyvinuté ontologie, je v prvních podkapitolách popsána relevantní teorie a zmiňovaná ontologie. V další podkapitole následuje detailní popis postupů a zásad nového schématu pro sběr a vyhodnocení dat o bezpečnosti.

3.1 Teorie bezpečnosti dle modelu STAMP [8]

STAMP (System-Theoretic Accident Model and Processes) je prediktivní model bezpečnosti. Jedná se o jeden z prvních systémových modelů bezpečnosti, který vysvětluje bezpečnost jako problém řízení. Model pracuje se základním předpokladem, že každá bezpečnostní událost (nehoda nebo incident) se sebou nese selhání nastavené bezpečnostní řídicí

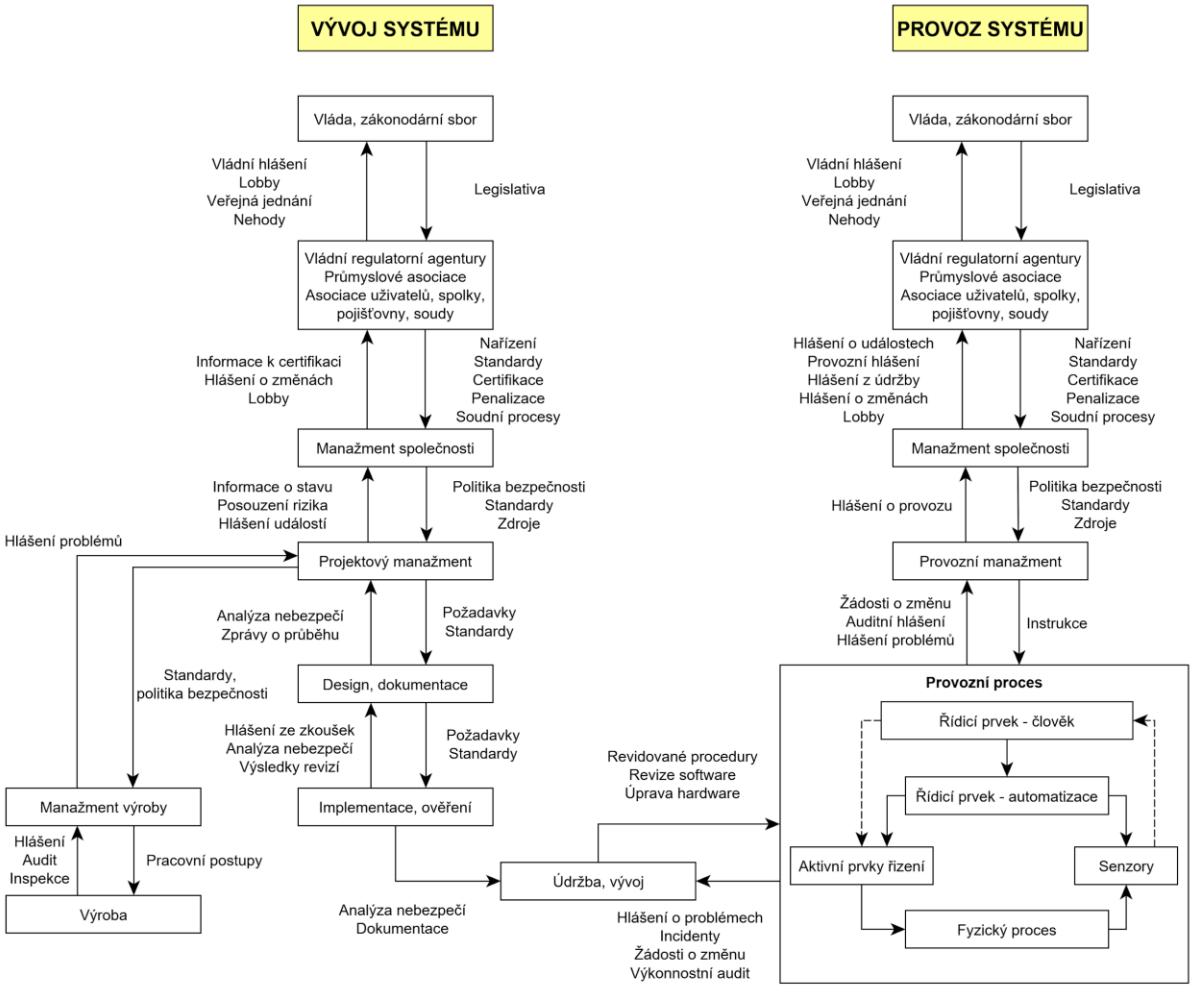
struktury, tedy hierarchicky uspořádaného socio-technického systému, ve kterém jsou lidé organizováni do provozních a manažerských pozic v interakci s různými druhy technologie, a který je navržen jako aktivní bariéra proti selhání rizikových systémů, tedy bariéra proti nehodám a incidentům. Kromě samotné organizace, distribuce práce, povinností a odpovědnosti je zde systémový aspekt, zejména potřeba řízení interakcí napříč celým systémem. V takto nastaveném systému je klíčová zejména distribuce informací, především zpětná vazba z řízených procesů do řídící struktury. Proto také STAMP pracuje s reprezentací systému dle "feedback control theory" [11], tedy teorie zpětnovazebního řízení, a od bezpečnostního analytika vyžaduje zobrazení zájmové části systému pomocí schémat kompatibilních s touto teorií. Výhodou analýz dle modelu STAMP je využití systémového pohledu pro vysvětlení bezpečnostních událostí, na rozdíl od zažitého vysvětlování událostí pomocí lineárního modelování kauzálních řetězců, bariér nebo s využitím deskriptivní statistiky pro identifikaci základních trendů ve sledovaných typech událostí (indikátorech bezpečnosti) [4]. Systémový pohled navádí analytika, aby pomocí schémat popisujících zájmovou část systému vysvětlil bezpečnostní události z pohledu systému, tedy analyzoval, proč systém selhal jako celek. Tímto teorie modelu STAMP vytváří základ pro preventivní opatření na úrovni systému a ne jenom na úrovni jednotlivých faktorů a událostí.



Obr. 1 Řídící smyčka dle teorie zpětnovazebního řízení (upraveno a přeloženo z [8])

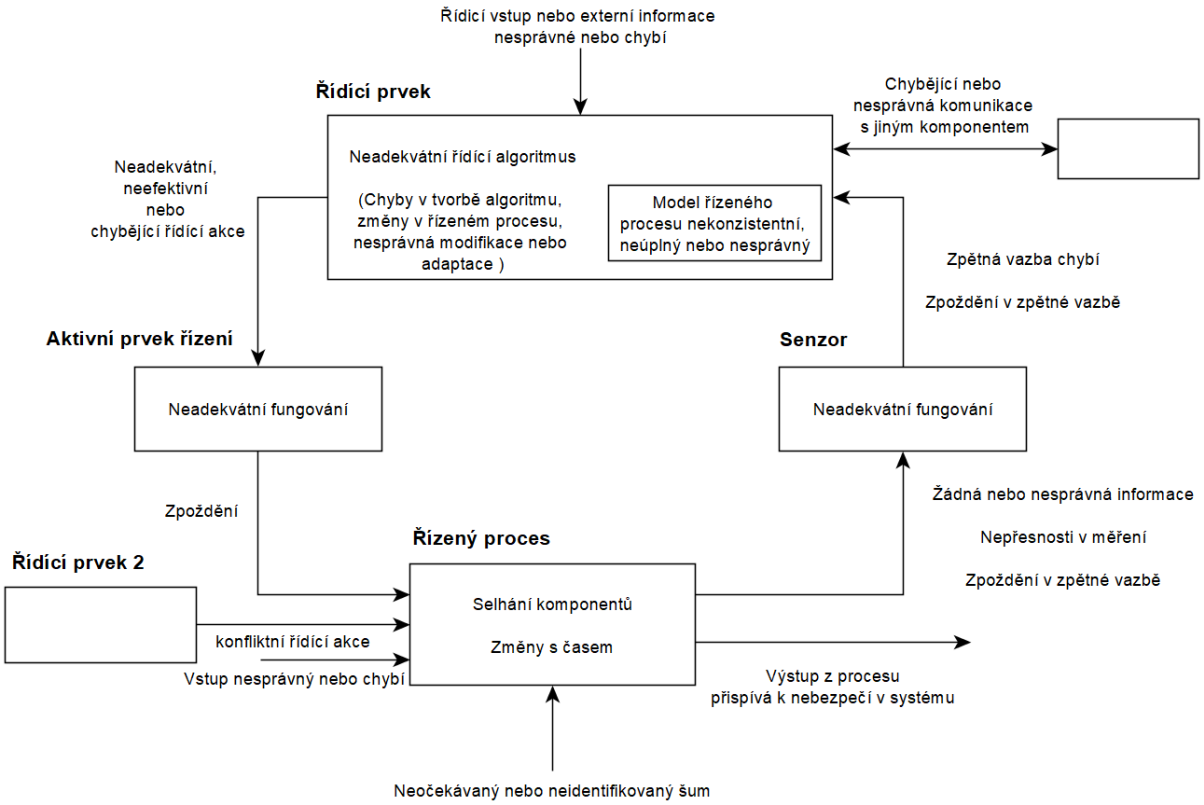
Jak již bylo zmíněno, základem pro realizaci analýzy STAMP je popis zájmové části systému s pomocí diagramů kompatibilních s teorií zpětnovazebního řízení. Základním stavebním blokem takového popisu je řídící smyčka zobrazená na obr. 1. Obrázek ukazuje základní elementy smyčky – řízený proces, senzory, aktivní prvky řízení a řídící prvek. Řídícím prvkem může být člověk nebo automatizace. Aby řídící prvek mohl řídit proces, je potřeba, aby měl aktuální informace o současném stavu procesu pomocí senzorů měřících stavové proměnné a také aby existovaly v systému aktivní prvky řízení, kterými řídící prvek řídí, resp. žádoucím způsobem ovlivňuje konkrétní stavové proměnné v řízeném procesu. Diagram na obr. 1 lze rozšiřovat/upřesňovat dle konkrétního kontextu a postupně tak tvořit diagramy reprezentující

celkový socio-technický systém. Příklad obecného socio-technického systému se zaměřením se na relevantní procesy z pohledu bezpečnosti je zobrazen na obr. 2. Obrázek reprezentuje zjednodušenou hierarchii zpětnovazebních smyček bez detailního popisu aktivních prvků řízení a senzorů. Jak je z obr. 2 patrné, popis systému dle teorie modelu STAMP je obvykle objektový diagram.



Obr. 2 Schéma obecného socio-technického systému (upraveno a přeloženo z [8])

Pro podporu úplnosti bezpečnostních analýz nabízí teorie modelu STAMP obecnou taxonomii všech možných problémů na úrovni běžné zpětnovazební smyčky dle obr. 1. Tato taxonomie je vyobrazena na obr. 3 a pro bezpečnostního analytika slouží jako podpora pro identifikaci faktorů v konkrétním hlášení události, resp. auditního nálezu v rámci běžného sběru a zpracování dat o bezpečnosti z provozu. Taxonomie slouží také k identifikaci úplného seznamu nebezpečí v posuzovaném systému, nicméně tento případ užití není předmětem tohoto dokumentu.



Obr. 3 Základní schéma identifikace nebezpečí a taxonomie problémů bezpečnosti dle STAMP (upraveno a přeloženo z [8])

Z pohledu sběru dat o bezpečnosti STAMP nabízí podporu především pomocí metodiky CAST (Causal Analysis based on STAMP). Tato metodika je primárně určena pro šetření nehod a incidentů, obsahem však odpovídá klíčovým částem běžného procesu sběru a zpracování dat v letecké dopravě, ať už z pohledu zpracování dat o nehodách a incidentech, tak z pohledu hlášení běžných událostí bez významnějšího vlivu na bezpečnost. Metodika CAST sestává konkrétně z následujících kroků [8]:

1. Identifikace relevantní části systému nebo seznamu nebezpečí
2. Identifikace platných bezpečnostních požadavků souvisejících s relevantní částí systému nebo nebezpečí
3. Tvorba popisu systému (diagramu smyček řízení)
4. Stanovení řetězce událostí, který vedl k bezpečnostní události
5. Analýza události na fyzické úrovni
6. Stanovení jak a proč přispěly jednotlivé části systému (konkrétní hierarchie smyček) k neadekvátnímu řízení v dané události
7. Ověření celkové koordinace a komunikace, která přispěla k události
8. Určení relevantní dynamiky a změn v sledovaném systému
9. Tvorba doporučení

Ze samotného postupu metodiky CAST je zřejmé, že základem je právě tvorba objektového diagramu (krok 3) popisující relevantní část řídící struktury, dle vzoru z obr. 2. Základem pro vytvoření tohoto diagramu jsou kroky 1 a 2, které napomáhají správné selekci zájmové části systému, která je relevantní v konkrétní šetřené události. Z praktického hlediska je žádoucí,

aby takový diagram byl pouze relevantní částí hodnoceného systému, jelikož úplný popis celého systému obvykle není možný nebo je značně nepraktické takový popis vytvořit.

Další část metodiky CAST (kroky 4 a 5) jsou typické kroky z oblasti šetření nehod a incidentů z provozu. V případech, kdy se sběr a zpracování dat o bezpečnosti týká těchto událostí, je vhodné kroky 4 a 5 realizovat bez úpravy. V případě prvotního hlášení se může jednat jen o základní rámcové informace, které budou iterativně zpřesněny v průběhu procesu šetření. V případech, kdy předmětem sběru a zpracování dat jsou běžné události z provozu, které nejsou klasifikovány jako incidenty nebo nehody dle platných standardů ICAO (Mezinárodní organizace pro civilní letectví) [12] je možné tyto kroky realizovat zjednodušeně, tedy bez podrobnější identifikace celkového řetězce faktorů hlášené události.

Kroky 6, 7 a 8 metodiky CAST jsou kroky systémové analýzy, kdy bezpečnostní analytik má za úkol zvážit hodnocený systém a jeho podobu v kontextu dat o bezpečnosti, která jsou zpracována. Jedná se o inovativní analytické kroky modelu STAMP, jelikož v současně využívaných systémech pro sběr a zpracování dat o bezpečnosti není potřeba data korelovat s popisem systému, který je vytvořil; postačuje pouze základní analýza pomocí deskriptivní statistiky pro stanovení trendů a závislostí. V metodice CAST naopak takováto analýza absentuje, jelikož analýza a interpretace dat bez popisu systému neposkytuje dostatečnou podporu pro přijímání cílených preventivních opatření. Korelace dat o bezpečnosti s popisem systému naopak vytváří základní návod, jak řízený systém upravit, aby byl přijatelně bezpečný. Poskytuje také základ pro lepší pochopení rizika a následné prioritizace bezpečnostních problémů.

Krokem 9 metodika CAST končí a jedná se o obvyklý krok každého procesu šetření nehod a incidentů. V případech, kdy předmětem zájmu jsou běžné události z provozu, nemusí být nutně generována nová doporučení.

3.2 Ontologie modelu bezpečnosti STAMP

Klíčové části a aspekty vyvinuté ontologie jsou blíže popsány v této kapitole. Ontologie STAMP byla navržena na základě dvou požadavků; (1) umožnit formální specifikaci tvrzení o konceptech dle teorie STAMP a jejich vzájemných relací, jako např. specifikace tvrzení o řídící struktuře a šetřené události jak je obvyklé v metodice CAST a (2) navrhnout ontologii tak, aby umožnila integraci dat s jinými informačními systémy a metodikami.

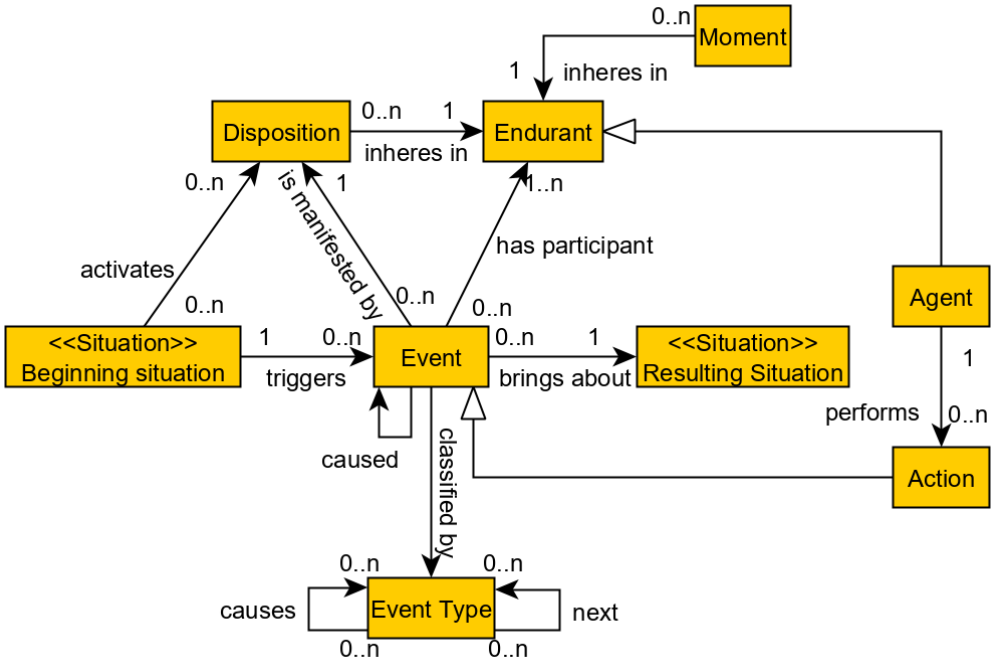
Ontologie STAMP byla formalizována s pomocí jazyka OWL 2 a propojena s ontologií Unified Foundational Ontology (UFO). Ontologie je dostupná online[1].

Všechna schémata v tomto dokumentu jsou ponechána v anglickém jazyce, jelikož neexistuje oficiální překlad konceptů a vzorců ontologie UFO do českého jazyka a také z praktických důvodů, jelikož programovací jazyky pro potenciální implementaci ontologie do vlastního softwarového prostředí jsou také výhradně v anglickém jazyce.

Obrázek 4 zobrazuje fragment z ontologie UFO, který reprezentuje kauzální síť s pomocí objektově-událostního modelu. Události (“Event”) jsou charakterizovány jejich spouštěcí

[1] http://onto.fel.cvut.cz/ontologies/stamp/

situací (“Beginning situation”) a situací, kterou způsobují (“Resulting situation”). Akce (“Actions”) jsou speciálními typy událostí, které jsou vykonávány (“performs”) agenty (“Agent”), tedy objekty s vnitřním/mentálním stavem. Situace reprezentují stav objektů a relací mezi nimi, např. rychlost vozidla nebo strukturální pevnost letadla. Situace popisují stavy systému před a po nastání událostí. Kromě toho mohou situace aktivovat dispozice (“Disposition”) předmětů, jako je strukturální pevnost trupu letadla. Aktivace dispozice se projevuje jako událost, která přináší novou situaci. Všimněte si, že není nutné popisovat všechny aspekty modelu UFO, aby se vytvořila síť. Uvedení dalších informací však umožňuje automatické odvozování znalosti podle formalizace událostí v UFO. Například při popisu kauzálních sítí lze použít vztah kauzality (“causes”) mezi událostmi a vztah vykonání (“performs”) mezi agenty a akcemi, a vynechat / odložit popis situací, dispozic a momentů objektů.

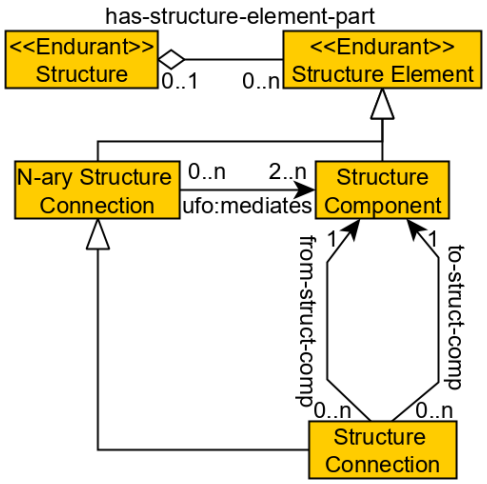


Obr. 4 Základní kauzální síť objektů a událostí v UFO.

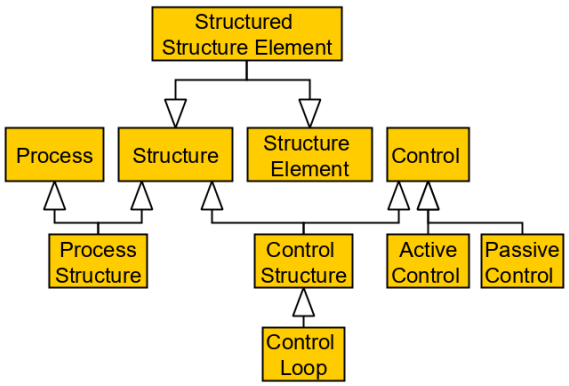
STAMP je založen na několika často používaných konceptuálních modelech. Hlavním modelem používaným v ontologii je model řízení se zpětnou vazbou. Tento model se používá k určení struktury řízení. Kromě toho se STAMP odkazuje na objektově-událostní model, kauzální model, model omezení a model obchodního procesu. Objektovo-událostní model se používá k popisu skutečných událostí, např. nehod v CAST a scénářů hypotetických nehod v metodice STPA (Systems-Theoretic Process Analysis), ačkoli STPA je mimo záběr tohoto dokumentu. Kauzální modely se používají k reprezentaci zjištění v rámci šetření scénářů nehod (skutečných i hypotetických). Kauzální model obvykle zachycuje kauzální síť událostí, stavů a dispozic objektů. Z pohledu bezpečnosti právě tato síť vede k nehodě. Modely obchodních procesů se používají k reprezentaci vzorců chování a omezení potřebných k tomu, aby se zabránilo nehodám, nebo aby se minimalizovaly jejich následky.

Tato metodika navrhuje použití obecné struktury, která umožňuje reprezentovat jak strukturu řízení, tak strukturu řízeného procesu, viz obr. 5a. Struktura (“Structure”) se skládá z několika částí, zde strukturálních prvků (“Structure Element”), specifikovaných pomocí vztahu „has-structure-element-part“ v ontologii. Existují dva hlavní typy strukturálních prvků, a to strukturní

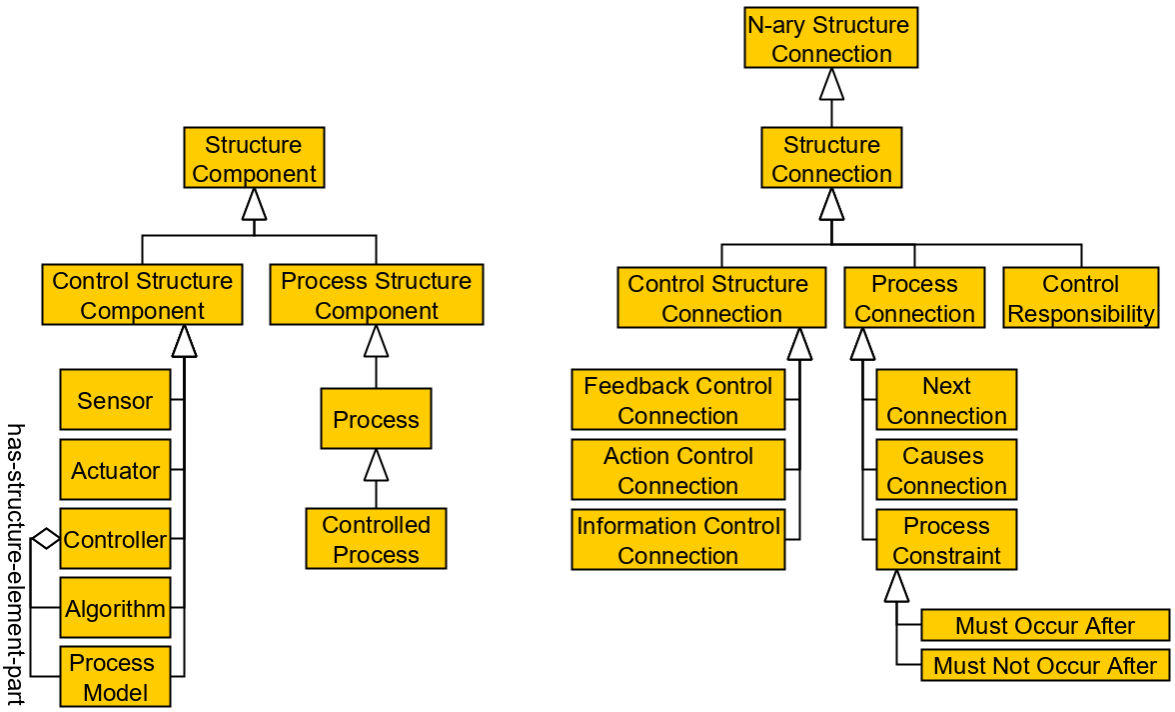
komponenta (“Structure Component”) a relační element s názvem “N-ary Structure Connection”. Vztah *ufo:mediates* určuje komponenty, ze kterých je relační element složen. Strukturální propojení (“Structure Connection”) je binární vazba definována jako specializace relačního elementu, se dvěma mediačními vztahy, konkrétně from-*structure-component* and *to-structure-component.* Obr. 5b ukazuje typy struktur použitých v STAMP, tj. kontrolní strukturu (“Control Structure”) a strukturu procesu (“Process Structure”). Ontologie dále umožňuje specifikovat strukturální prvky, v případě potřeby tak umožňuje podrobnější popis prvků. Ve výsledku je ontologie schopna zachytit různé pohledy na řídící strukturu, kde některé prvky jsou zobrazeny více podrobně, zatímco jiné méně. Obr. 5c dále ukazuje různé druhy komponentů (vlevo) a relací (vpravo) použitých k reprezentaci řídících a procesních struktur.



Obr. 5a STAMP model struktury



Obr. 5b STAMP taxonomie struktury

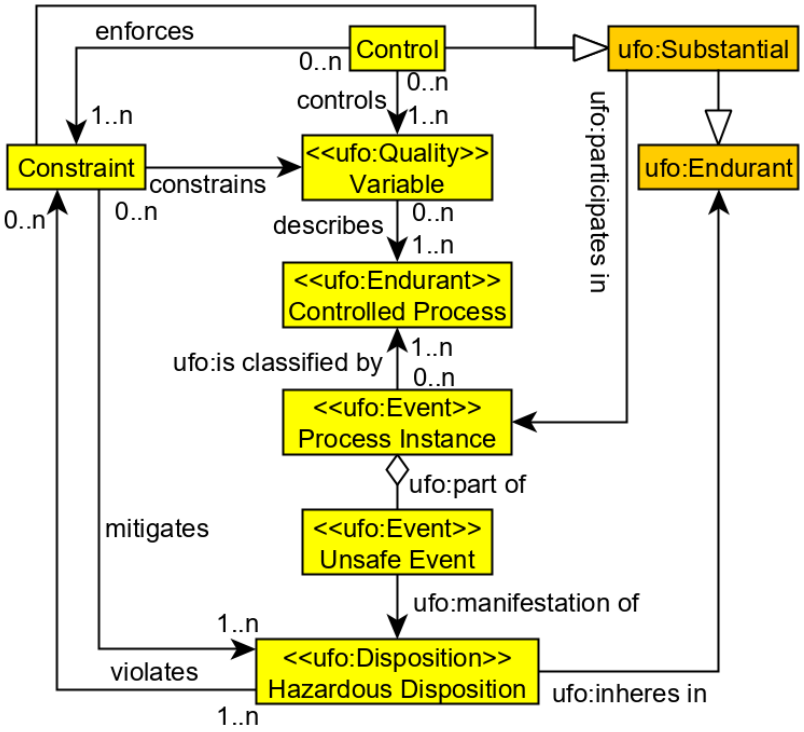


Obr. 5c Taxonomie strukturálních prvků

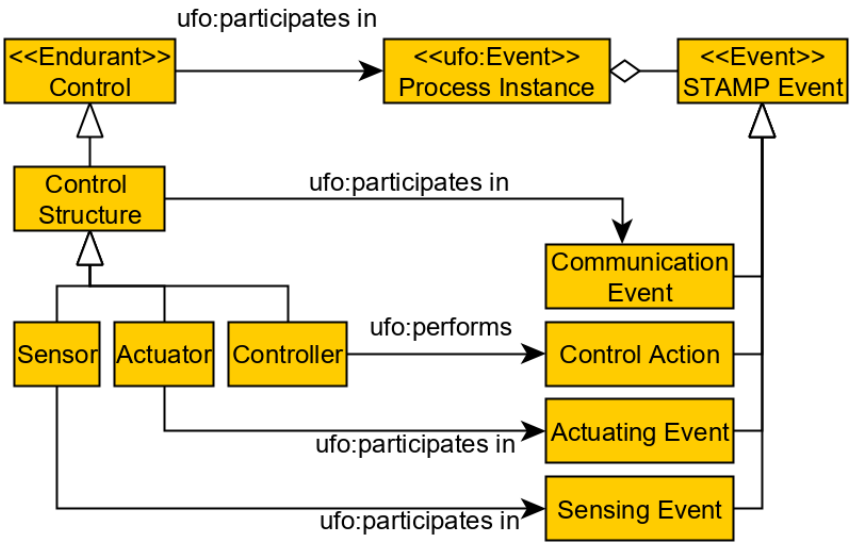
STAMP specifikuje pět druhů komponent struktury řízení (“Control Structure Component”), konkrétně řídící prvek (“Controller”), model procesu (“Process Model”) senzor (“Sensor”) a aktivní prvek řízení (“Actuator”), i když tento seznam může být v případě potřeby dále rozšířen. Dále STAMP specifikuje tři typy relací, reprezentovaných v ontologii STAMP jako relace řízení (“Action Control Connection”, reprezentující řízení pomocí aktivních prvků řízení), relace zpětné vazby (“Feedback Control Connection”, reprezentující zpětnou vazbu pomocí senzorů) a informační relace (“Information Control Connection”, reprezentující koordinaci a informační vazby mezi řídícími prvky). Struktura procesu je popsána z hlediska komponent daného procesu, které mohou být spojeny vazbou *Next Connection* (tj. uspořádány do toků).

Jádro ontologie je znázorněno na obr. 6. Ústředním konceptem je řízený proces (“Controlled Process”), který obvykle sestává z posloupnosti úkolů a je běžně popsán v provozní dokumentaci. V kontextu ontologie UFO je tento proces modelován jako typ události (“Event Type”), kde se mohou účastnit (*participate in*) různé objekty a agenti. Objekty a agenti jsou společně reprezentovány pomocí konceptu *Substantial* (oranžový box na obr. 6). Účastníkem řízeného procesu je řízení (“Control”), které je modelováno jako specializace konceptu *Substantial*. Řízení je odpovědné za řízení konkrétních proměnných (“Variable”) a jedná se o souhrn objektů a agentů podle teorie STAMP (tj. řídících prvků, senzorů a aktivních prvků řízení), které se mohou časem měnit, ale zachovávají si svou identitu. Za nebezpečí (“Hazard”) se považuje schopnost nebo vlastnost předmětů a agentů, nebo jejich funkce. STAMP však definuje pojem nebezpečí jako stav. V navržené ontologii je místo těchto stavů použit termín nebezpečný stav (“Hazardous State”), aby se zabránilo nejednoznačnosti v terminologii. Nebezpečí jsou v ontologii modelována jako dispozice (“Disposition”), které jsou inherentní entitám *Endurant* a projevují se (*manifest in*) v nežádoucích událostech (“Unwanted Events”), čímž porušují existující bezpečnostní omezení (“Safety constraint”) dle teorie STAMP. Bezpečnostní omezení jsou modelována jako *Substantial* a jejich cílem je zmírnit následky nebezpečí v nežádoucích událostech. To se provádí omezením proměnných, které popisují různé aspekty řízeného procesu. Kromě toho lze proměnné definovat z hlediska objektů a událostí (na obrázku nejsou znázorněny). Například proměnnou „vzdálenost mezi letadlem a vozidlem“ lze modelovat jako formální vztah UFO mezi objekty „letadlo“ a „vozidlo“. Účelem tohoto a podobných ontologických vzorců je lepší definice řízení a uchopení kvantifikovatelných aspektů řízených procesů, které jsou v kontextu teorie STAMP využívány jako proměnné v řízeném procesu, a které lze měřit nebo jimi manipulovat. Prosazování (“enforcing”) bezpečnostních omezení je realizováno konceptem řízení (“Control”).

Další klíčovou součástí publikované ontologie je popis událostí spojených s komponentami řídicí struktury (“Control Structure Component”) z obr. 5 a řízeným procesem (“Controlled Process”), viz obr. 7. Například řízení může být složeno z řídícího prvku, několika senzorů a aktivních prvků řízení. Řízený proces (“Controlled Process”) je modelován z několika částí (událostí), které jsou předmětem zájmu v teorii STAMP (proto třída “STAMP Event”) a které lze rozdělit na události související s komunikací (“Communication Event”), aktivním řízením (Control Action), ovládáním (Actuating Event) a měřením (Sensing Event). Účastníci v těchto událostech jsou specifikováni prostřednictvím relace *participates in* a také relace *performs*, která propojuje řídící prvek s aktivním řízením. Pro ilustraci a srozumitelnost obsahuje Příloha 2 k tomuto dokumentu několik konkrétních příkladů použití ontologie v letectví.



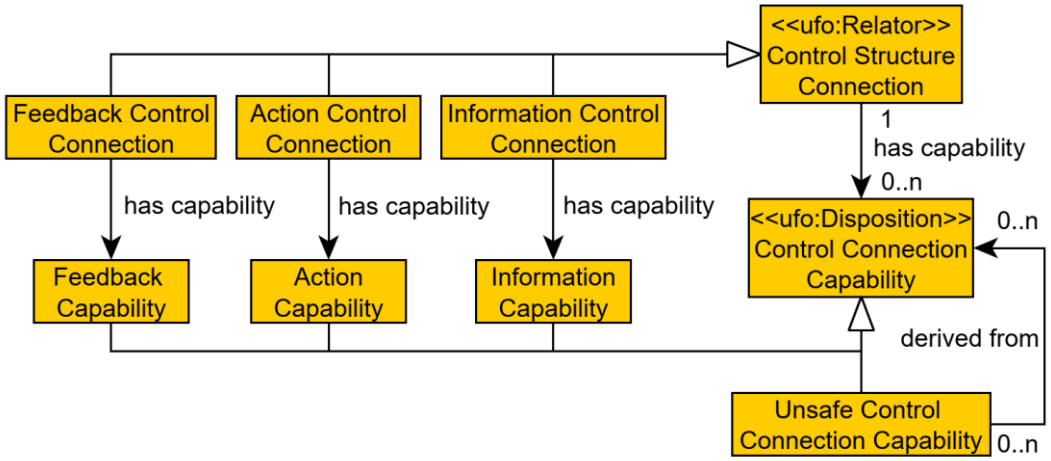
Obr. 6 Jádro vyvinuté ontologie STAMP



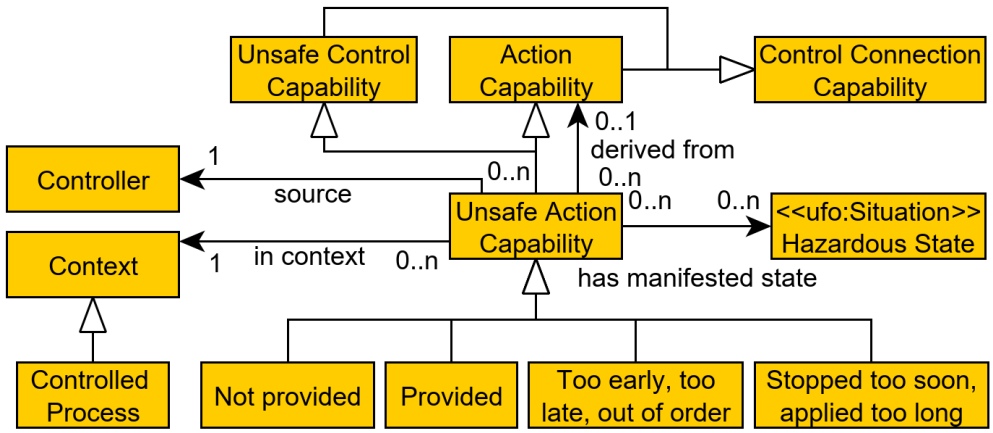
Obr. 7 Klíčové koncepty související s řízením v ontologii STAMP

Model STAMP popisuje řídicí akce (“Control Actions”) a další události v řídící struktuře, jako je rozhodování řídícího prvku nebo provoz senzorů. Ontologie STAMP toto modeluje jako schopností (“Capability”, specializace konceptu “Disposition”). Obr. 8 znázorňuje schéma pro přiřazení schopností k prvkům řídící struktury (“Control Structure Elements”), v tomto případě schopností asociovaných s relacemi řízení, zpětné vazby a informačními relacemi. Relace použitá k reprezentaci této asociace je *has capability*. Obr. 9 dále ukazuje, jak určit konkrétní schopnost nebezpečného řízení (“Unsafe Action Capability”, neboli nebezpečné řízení (unsafe control action) v terminologii STAMP). Schéma umožňuje popsat schopnost, ze které je odvozena schopnost nebezpečného řízení, např. „schopnost brzdit nebezpečně“ je

odvozena od „schopnost brzdit“. Schéma také umožňuje specifikovat konkrétní typ schopnosti nebezpečného řízení podle STAMP, např. aktivní řízení nebylo provedeno nebo bylo provedeno příliš brzy. Schéma dále umožňuje specifikovat nebezpečný stav (“Hazardous State Type”), ke kterému schopnost potenciálně vede, zdroj, tj. *Control Component Controller* (např. řídící prvek, který akci provedl)) a kontext (“Context”, např. proces nebo činnost, během níž je konkrétní schopnost nebezpečná).

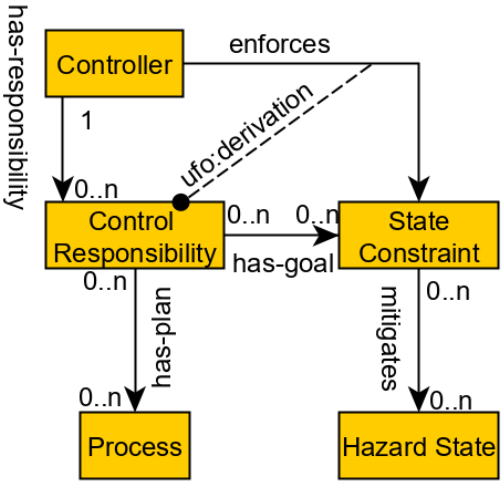


Obr. 8 Specifikace schopností řídící struktury



Obr. 9 Schéma schopnosti nebezpečného řízení

STAMP k předešlým schématem navíc požaduje specifikaci odpovědnosti za řízení (“Control Responsibility”), viz obr. 10. Řídící prvek má přiřazenu odpovědnost za řízení prostřednictvím vztahu *has responsibility*. Odpovědnost za řízení má za cíl (*has goal*) omezení stavu (“State Constraint”) a je provázána s procesem (“Process”) prostřednictvím relace has *plan*. Tato část vysvětluje, že řídící prvek je navržen tak, aby prováděl předdefinovaná opatření za určitých podmínek tak, aby se předešlo nežádoucím událostem, které by mohly vést k realizaci nebezpečí, tj. aktivní prvek řízení prosazuje (*enforces*) omezení stavu. Omezení stavu a nebezpečný stav odráží bezpečnostní omezení a rizika, jak je využívá teorie modelu STAMP.



Obr. 10 Schéma odpovědnosti za řízení

3.3 Aplikace vyvinuté ontologie modelu bezpečnosti STAMP

Tato část metodiky popisuje využití vyvinuté ontologie STAMP v kontextu procesu sběru a zpracování dat o bezpečnosti.

3.3.1 Základní informace k aplikaci

Postup aplikace ontologie je kompatibilní s teorií modelu bezpečnosti STAMP jakož i metodikou CAST, nicméně přináší nové technické možnosti pro archivaci dat a také pro realizaci některých kroků metodiky CAST. Základním rozdílem je definice konceptů z teorie STAMP s využitím ontologií. Toto nejvíc ovlivňuje provádění kroku 3, tedy tvorbu popisu systému, který vytvořená ontologie omezuje podle definovaných vzorců. Protože ontologie je strojově čitelný artefakt, nevyžaduje nutně tvorbu popisu systému pomocí objektových diagramů podobných tomu na obr. 2, i když takováto reprezentace může být v některých ohledech přínosná. Ontologie však umožňuje především strojový popis systému, který je obvykle archivován ve formátu RDF (Resource Description Framework), tedy v úložišti triplů (subjekt, predikát, objekt) jako je RDF4J.

Realizace strojově čitelného popisu systému může být provedena buď přímo s využitím publikovaného artefaktu ontologie (např. ve volně dostupném nástroji Protégé[2]), nebo může být implementována do vlastního softwarového nástroje, který slouží jako podpora řízení bezpečnosti nebo provozní dokumentace v konkrétní organizaci. Zejména v případě implementace ontologie do vlastního nástroje se zde nabízí možnost její implementace do prostředí integrovaného systému řízení (tzv. Integrated Management System – IMS), který obvykle již obsahuje řadu informací potřebných pro analýzu STAMP a které lze tímto využít pro několik účelů v rámci jednoho systému. Obzvlášť vhodné je využít standardní provozní dokumentaci, pokud tato existuje, protože obsahuje základní popis procesů, jejich účastníků jakož i distribuci odpovědnosti. V případě, že provozní dokumentace není zpracována elektronicky, vhodným řešením je využít běžně dostupné nástroje pro modelování procesů

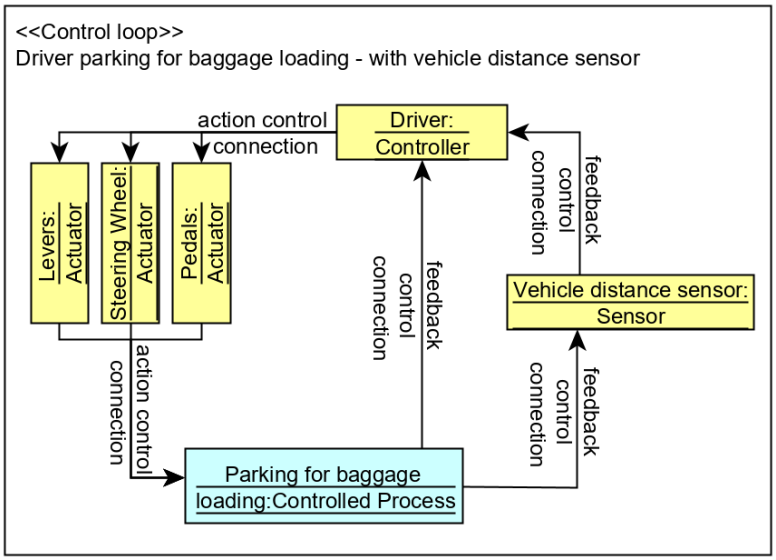
[2] https://protege.stanford.edu

společností s využitím jazyka BPMN (např. volně dostupný nástroj Modelio[3] nebo komerčně dostupné produkty jako je Adonis[4] nebo Bizagi Modeler[5]). Vytvořený popis systému je pak nutné obohatit o doplňující informace dle publikované ontologie, čímž vznikne popis systému dle kroku 3 metodiky CAST a zároveň provozně využitelný artefakt pro běžné řízení společnosti. Jediný rozdíl je, že takový popis systému je kompletní a není tedy filtrovaný v kontextu konkrétní nehody nebo bezpečnostní události. Aplikací této metodiky v kombinaci s procesy řízení společností vzniká synergický efekt a tím unikátní možnost udržovat úplný a aktuální popis systému kompatibilní s teorií modelu STAMP. Tímto je možné výrazně zjednodušit a zrychlit proces sběru a zpracování dat o bezpečnosti dle modelu STAMP. Krok 3 metodiky CAST se totiž redukuje na jednoduchou filtraci existujícího popisu systému dle zaměření konkrétního zpracování dat o bezpečnosti, tedy dle výstupu z kroků 1 a 2 metodiky CAST. Realizace počátečních kroků (1 a 2) metodiky CAST tedy závisí na způsobu realizace kroku 3. Pokud je krok 3 realizován formou integrovaného řešení, pak se jedná o zmíněnou filtraci již existující dokumentace ve všech třech počátečních krocích. Pokud je však ontologie STAMP využita samostatně (např. v nástroji Protégé), pak je nutné obraz systému vytvořit v každém procesu sběru a zpracování zvlášť, jak je obvyklé v teorii STAMP. Ze zmiňovaných důvodů je proto výhodnější využít první z možností, tedy filtraci již existujícího artefaktu.

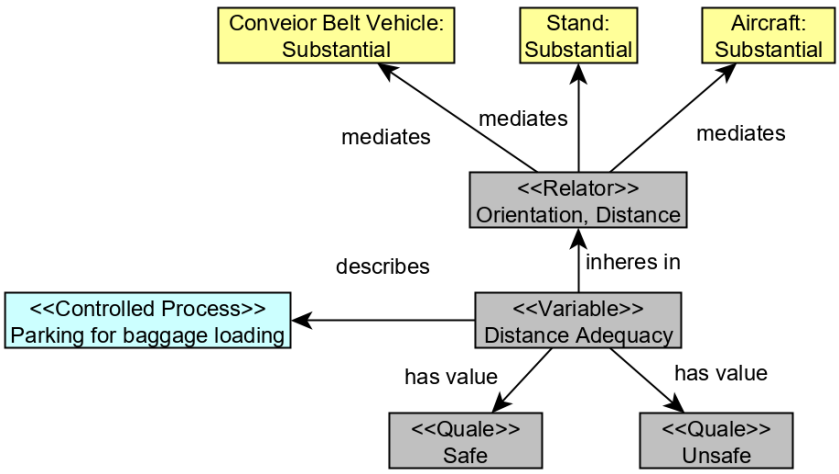
3.3.2 Aplikace ontologie na kroky metodiky CAST

Popis systému dle kroku 3 metodiky CAST vyžaduje definici řídících smyček, řídící struktury, řízených procesů, bezpečnostních omezení a všech objektů a relací, které je vzájemně propojují a které jsou relevantní vůči konkrétní nehodě nebo bezpečnostní události. Základem celého modelu STAMP je řídící smyčka a obr. 11 zobrazuje příklad definice jedné smyčky dle vzorců ontologie STAMP. Konkrétně je zde vidět řídící prvek - řidič vozidla s dopravníkem pro nakládání zavazadel do letadla, který řídí proces parkování vozidla se senzorem měřícím vzdálenost mezi vozidlem a letadlem. Kromě základních elementů smyčky je zde i podpora pro definici proměnných (variables), které jsou v řízeném procesu ovlivňovány řídícím prvkem, zde konkrétně vzdálenost a relativní orientace vozidla s dopravníkem pro nakládání zavazadel vůči letadlu (viz obr. 12). Obr. 13, 14, a 15 obsahují podrobný popis částí řídicí smyčky z obr. 11 znázorňující podrobností o relacích, objektech a událostech souvisejících se smyčkou. Obr. 11 (jakož i následující obrázky) je pouze snahou o vizualizaci výsledku procesu sběru a zpracování dat s využitím jazyka UML, i když uchování záznamu v jazyce RDF takovou vizualizaci nevyžaduje. Stereotypy (názvy tříd uvedené v dvojitých hranatých závorkách) odpovídají typům objektů dle vyvinuté ontologie STAMP. Všechny ilustrativní obrázky jsou uvedeny v anglickém jazyce, jelikož dosud neexistuje ověřený překlad terminologie ontologie, resp. teorie modelu STAMP do českého jazyka. Volný překlad klíčových termínů lze nalézt v příloze 1.

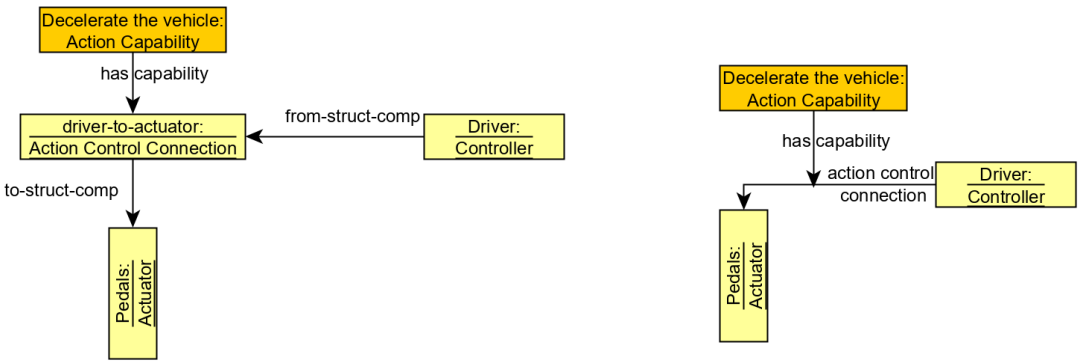
[3] https://www.modelio.org
[4] https://www.adonis-community.com
[5] https://www.bizagi.com/products/bpm-suite/modeler



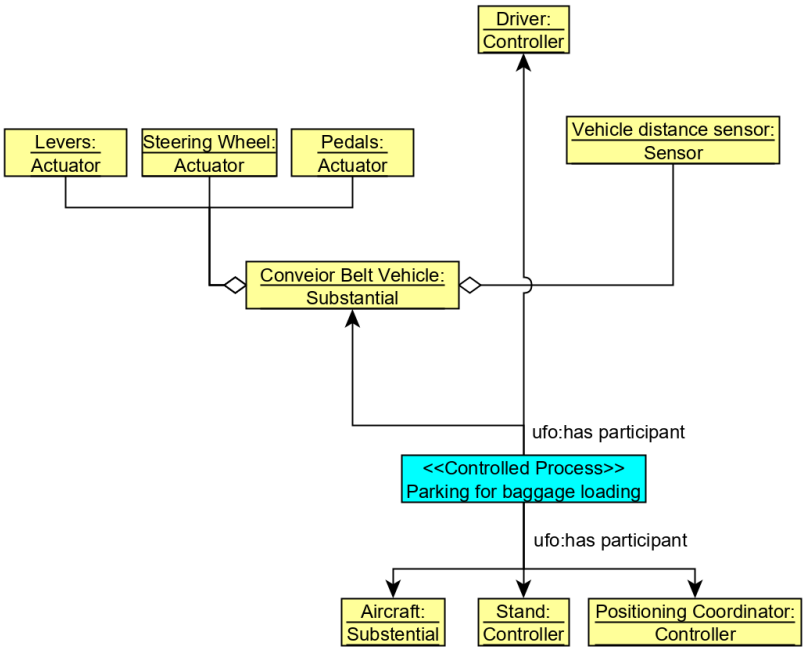
Obr. 11 Příklad modelování řídící smyčky s využitím ontologie STAMP.



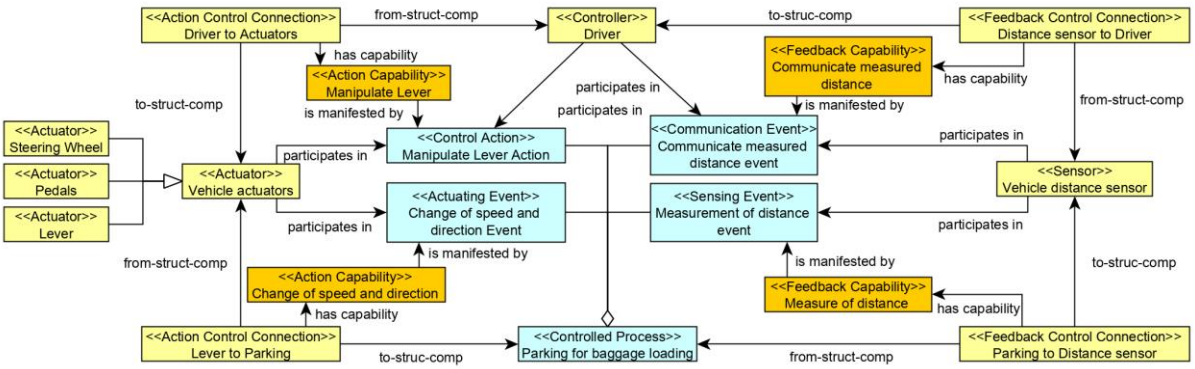
Obr. 12 Specifikace řízených proměnných, které podporují řízení procesu



Obr.13 Notace pro reprezentaci relací v diagramech

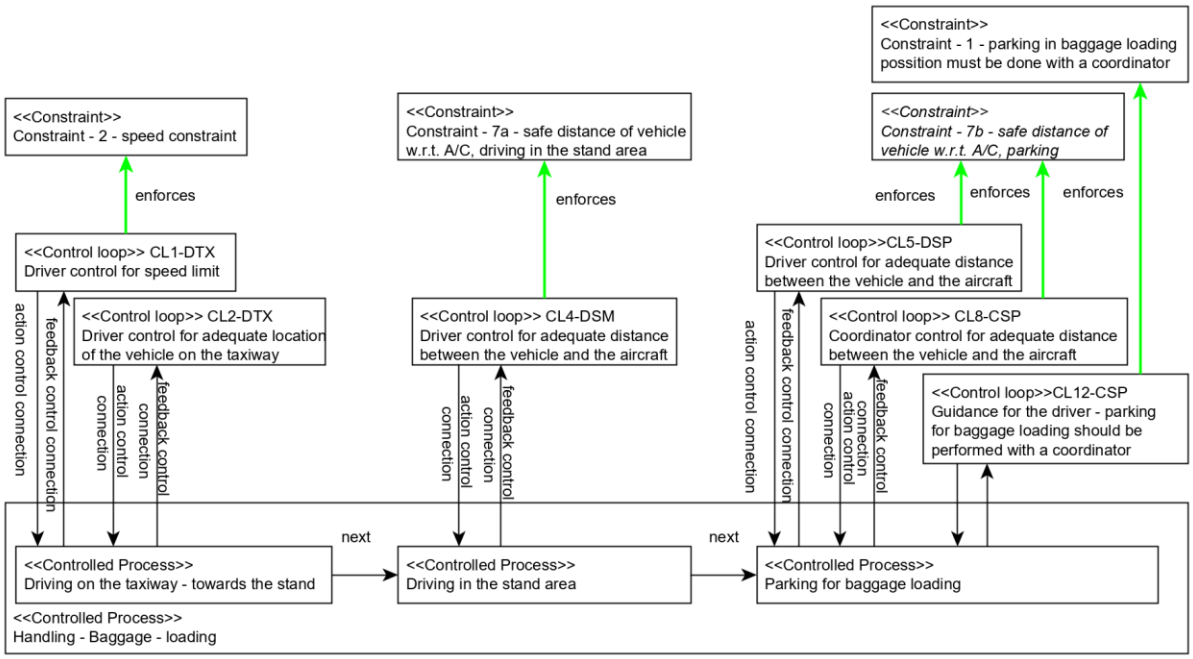


Obr. 14 Detailní specifikace objektů relevantních pro konkrétní řídící smyčku



Obr. 15 Detailní specifikace událostí relevantních pro konkrétní řídící smyčku

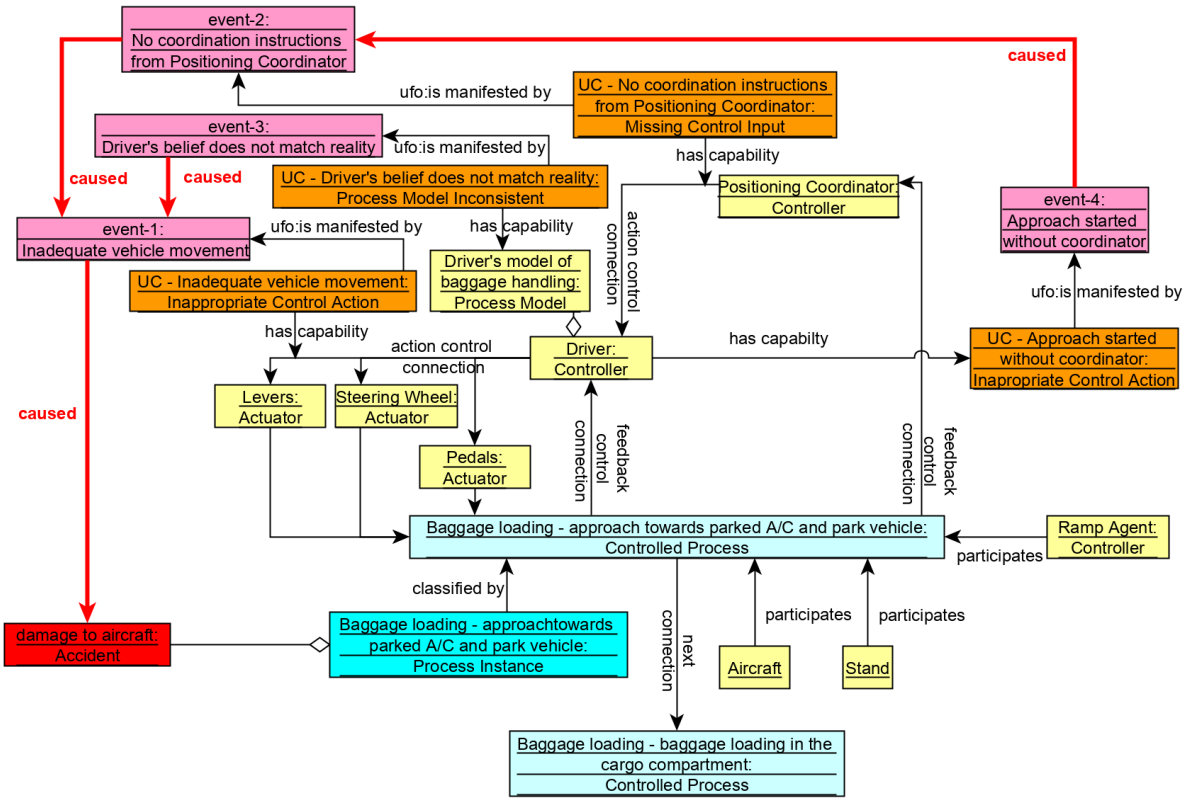
Po definici a modelování řídících smyček je nutné určit rozdělení smyček s ohledem na řízené procesy a bezpečnostní omezení. Distribuce je graficky znázorněna na obr. 16, kde jsou řídící smyčky vázány na konkrétní řízené procesy (s relacemi řízení a zpětné vazby) podle procesní dokumentace a jejich úkolem je prosazovat stanovená bezpečnostní omezení. Ontologie STAMP stanovuje, že každé bezpečnostní omezení musí být vynuceno nějakou řídící smyčkou. Příkladem je bezpečnostní omezení - 1 z obr. 16, které vyžaduje, aby proces parkování pásového dopravníku nemohl být zahájen bez koordinátora parkování, který je součástí procesu nakládání zavazadel, konkrétně součástí řídící smyčky CL12-CSP koordinátora parkování. Jistě je možné a v praxi spíše obvyklé, že jedna řídící smyčka prosazuje několik bezpečnostních omezení a také, že jedno bezpečnostní omezení může být prosazováno několika řídícími smyčkami. Z hlediska bezpečnosti je však nepřijatelné, pokud některá bezpečnostní omezení neprosazuje žádná řídící smyčka.



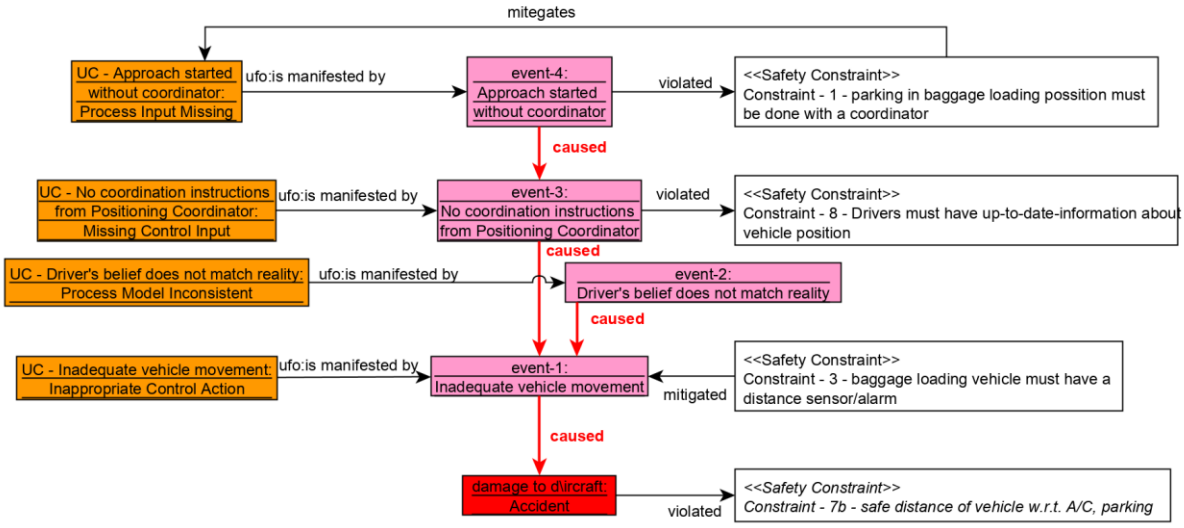
Obr. 16 Modelování provozních procesů a jejich propojení s bezpečnostními omezeními dle ontologie STAMP.

Kroky 4 a 5 dle metodiky CAST jsou podpořeny ontologií STAMP podobným způsobem jako je to u kroků 1, 2, a 3. Zde je potřeba nejen stanovit řetězec událostí, jak je obvyklé v každém procesu šetření, ale tento navíc provázat s vytvořeným popisem systému z kroku 3, tedy v kontextu schémat z obr. 11-16. Obr. 17 v tomto ohledu zobrazuje ukázku fiktivní události, ve které došlo ke kolizi vozidla s pásovým dopravníkem (pro nakládání zavazadel) s letadlem. Ke kolizi došlo v průběhu parkování vozidla do pozice, ve které je možné do letadla naložit zavazadla a náklad s pomocí dopravníku. Řidič vozidla nesprávně odhadl relativní vzdálenost a pozici vozidla vůči letadlu a narazil s dopravníkem do trupu letadla, čímž ho poškodil. Přispívající faktory této události byly zahájení procesu parkování bez přítomnosti koordinátora parkování, absence zpětné vazby od koordinátora během procesu parkování, nesprávné vnímání řidiče vzdálenosti vozidla od letadla a neadekvátní pohyb vozidla vůči letadlu. Řetězec událostí je zobrazen fialovou barvou, popis systému barvou žlutou (objekty), modrou (události) a oranžovou (schopnosti), samotná nehoda pak barvou červenou. Vazby mezi fialovými/červeným a oranžovými elementy zobrazují provázání popisu systému (dokumentací řídící struktury bezpečnosti) s řetězcem události.

Po dokončení základního popisu události dle příkladu z obr. 17 je dále nutné definovat, jak a proč přispěly jednotlivé části systému k neadekvátnímu řízení v dané události, tedy realizovat krok 6 dle metodiky CAST. V tomto ohledu jsou důležité dva typy informací, kterých specifikaci vyžaduje ontologie STAMP: která bezpečnostní omezení byla narušena a jak jsou tato omezení provázána s modelem procesů, tedy s popisem systému z kroku 3 metodiky CAST. Obr. 18 zobrazuje specifikaci narušených bezpečnostních omezení dle ontologie STAMP. Navázání bezpečnostních omezení na řídicí smyčky lze odvodit z již vytvořených schémat, konkrétně ze schématu z obr. 16. Při implementaci ontologie do softwarového prostředí lze toto odvodit automaticky.



Obr. 17 Modelování fiktivní události poškození letadla v průběhu procesu parkování mobilního manipulačního prostředku s využitím ontologie STAMP.



Obr. 18 Modelování fiktivní události poškození letadla a její provázání s bezpečnostními omezeními dle ontologie STAMP.

Jak je patrné z obr. 18, ontologie STAMP upřesňuje proces sběru a zpracování dat. Ontologie zde vyžaduje definici relací narušení (*violates*) mezi faktory události a bezpečnostními

omezeními. Zmiňovaný příklad omezení č. 1 z obr. 16 je v obr. 18 narušeno konkrétním faktorem – zahájením parkování bez přítomnosti koordinátora. I když je příklad z této kapitoly spíše jednoduchý a popisuje pouze dvě řídicí smyčky, stejný postup se využije i v případě několikaúrovňové hierarchie řídících smyček.

3.3.3 Praktická doporučení

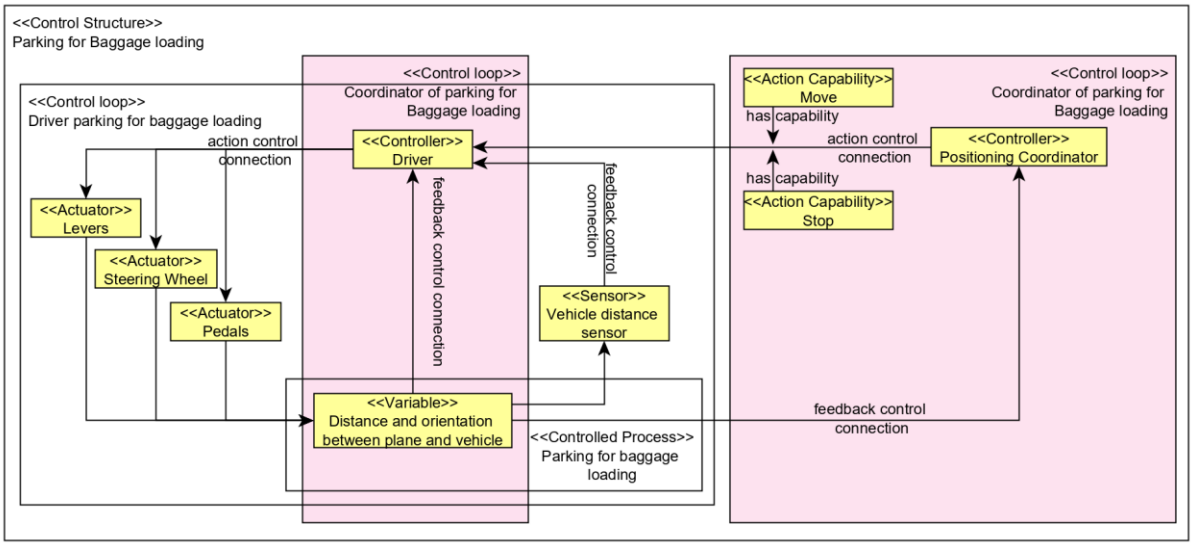
Realizace sběru a zpracování dat o bezpečnosti s využitím vyvinuté ontologie STAMP přináší několik příležitostí, jak proces sběru a zpracování zrychlit, zjednodušit, a přitom nadále zachovat výhody aplikace ontologie z pohledu podpory realizace některých kroků metodiky CAST dle teorie modelu STAMP.

První z možností zjednodušení je zavedení knihovny typů objektů, rolí zaměstnanců atp. Ontologie přirozeně pracuje s typy a není nevyhnutelné, aby byly specifikovány všechny jejich instance. V jistých ohledech může být vhodné pracovat s instancemi (např. definovat konkrétní zaměstnance s osobními údaji, kteří zastávají různé role v procesech nebo konkrétní vozidla s identifikátorem jako je SPZ, které se v procesech využívají), nicméně STAMP cílí na systémový pohled, a tedy spíš na vzájemné souvislosti, propojenost a uspořádanost objektů, řídicích smyček atp. vystupujících v provozu, s využitím abstraktního popisu (funkčního, tedy nezávislého na konkrétních objektech). V tomto ohledu postačuje definice rolí a typů objektu (např. řidič pásového dopravníku, nebo letadlo, resp. flotila atp.) a vytvořením knihovny všech takových typů vzniká relativně praktická množina, ze které může bezpečnostní analytik vybírat jak při definici procesů v provozní dokumentaci, tak při vázání události na provozní dokumentaci.

Další z praktických doporučení se týká modelování složitého řízení v případech, kdy je potřebná vyšší úroveň detailu pro účely konkrétní analýzy. Teorie STAMP připouští existenci překrývajících se řídících smyček, neposkytuje však způsoby reprezentace detailů takového překryvu v reálných podmínkách. Problém spočívá v tom, že v procesech běžně vystupuje několik řídících prvků a řízených procesů, které se různě prolínají. Příklad takové situace je uveden na obr. 19. Příklad obsahuje již zmiňovanou řídící smyčku řidiče vozidla s pásovým dopravníkem, na obrázku je však detailněji znázorněna také řídící smyčka koordinátora parkování (zvýrazněna fialovou) a vzájemné provázání obou smyček. Podobně jako u všech předešlých obrázků, je i obr. 19 pouze snahou o vizualizaci, jeho obsah by však měl být zaznamenán pomocí specifikace tříd popisující objekty, řízené proměnné a vzájemné relace, např. ve formátu RDF. Tímto způsobem je možné s využitím ontologie STAMP vytvořit věrný popis složitého systému s potřebnou úrovní detailu, který nemusí být snadno vizualizovatelný, a nad tímto popisem přitom praktickým způsobem realizovat sběr a zpracování dat o bezpečnosti z provozu.

Poslední doporučení se týká možnosti využití taxonomie modelu STAMP zobrazené na obr. 3. Tato taxonomie je obecná a využitelná pro klasifikaci záznamů o událostech z provozu. V kontextu praktické aplikace vyvinuté ontologie STAMP může být tato ontologie využita ve své obecné formě k popisu událostí tak, jak zobrazuje obr. 18 (oranžové boxy), tedy jako třída, která klasifikuje konkrétní události. Protože se obecná taxonomie modelu STAMP vztahuje na konkrétní objekty z řídící smyčky (např. neadekvátní model procesu se váže na řídící prvek), modelováním obecné taxonomie pomocí ontologie vzniká možnost filtrace taxonomie podle

objektu zájmu, a tedy i možnost tvorby praktických číselníků pro klasifikaci jednotlivých událostí z provozu.



Obr. 19 Modelování detailního propojení řídicích smyček dle ontologie STAMP.

3.4 Využití provozní dokumentace a jejích nástrojů

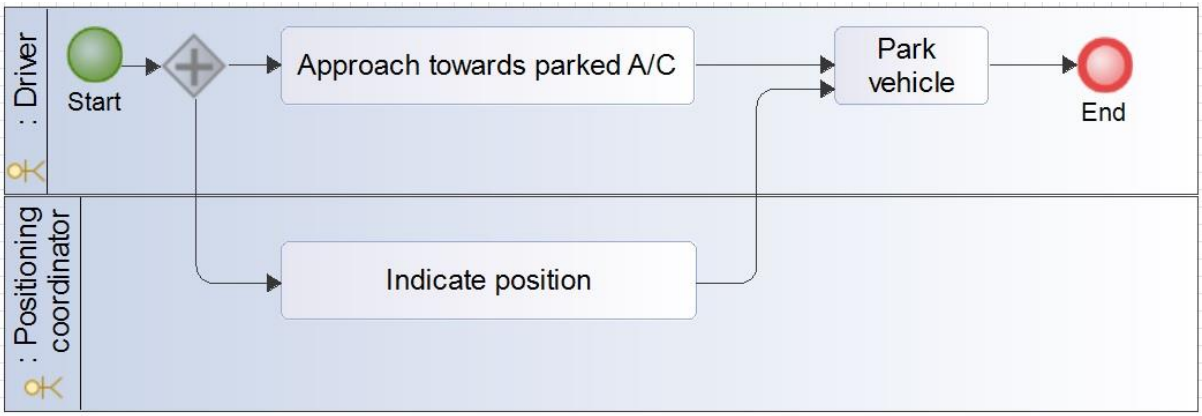
Provozní dokumenty stanovují pravidla a postupy při vykonávání a řízení procesů a činností v dané společnosti s cílem dosáhnout jednotného a efektivního řízení. Dokumentace je vydávána v jednotném systému i jednotné formě a jsou jednoznačně stanovena pravidla a odpovědnosti její tvorby a správy. Definuje závazná pravidla nutná pro správné fungování procesů ve společnosti, popisuje tyto procesy, jejich posloupnosti nebo návaznosti včetně odpovědností a pravomocí. Z toho důvodu lze konstatovat, že provozní dokumentace je vhodným základem pro tvorbu modelu analyzovaného systému.

Grafické znázornění podnikových procesů pomocí procesních diagramů, které je vhodným a platným nástrojem tvorby modelu, se řídí souborem pravidel a principů BPMN. Procesní diagram je soubor jednoho či více propojených postupů nebo činností prováděných ve stanoveném pořadí. Dále mohou být zaznamenány i různé další vnější okolnosti. Dostupné nástroje pro modelování procesů s využitím BPMN umožňují integrovat do modelu všechny principy popsané v předchozích kapitolách způsobem, který je popsán v této kapitole.

Procesy společnosti lze obecně rozdělit do tří základních skupin na procesy hlavní, procesy podpůrné a procesy řídící. Model takového členění poskytne analytikovi základní pohled. Skupiny lze dále rozpracovávat členěním na nižší úrovně, protože každá činnost v řetězci procesu může představovat celý proces na nižší úrovni pohledu, kdy lze dojít až k popisu jednotlivých akcí v rámci aktivit. Taková úroveň detailu však není většinou nutná. Při popisu procesů je nezbytné zaznamenávat jejich skutečný průběh.

Diagram základního procesu lze vidět na obr. 20. Jeho elementárními prvky jsou start, tedy začátek aktivit v procesu, jednotlivé činnosti uspořádané do požadované struktury a

provázané pomocí vazeb a cíl (end), neboli konec aktivit v procesu. Obrázek zobrazuje proces parkování vozidla s pásovým dopravníkem, který byl využit již v předešlých kapitolách. Specifikuje dvě paralelně probíhající aktivity dle osob, které je vykonávají (řidič a koordinátor).



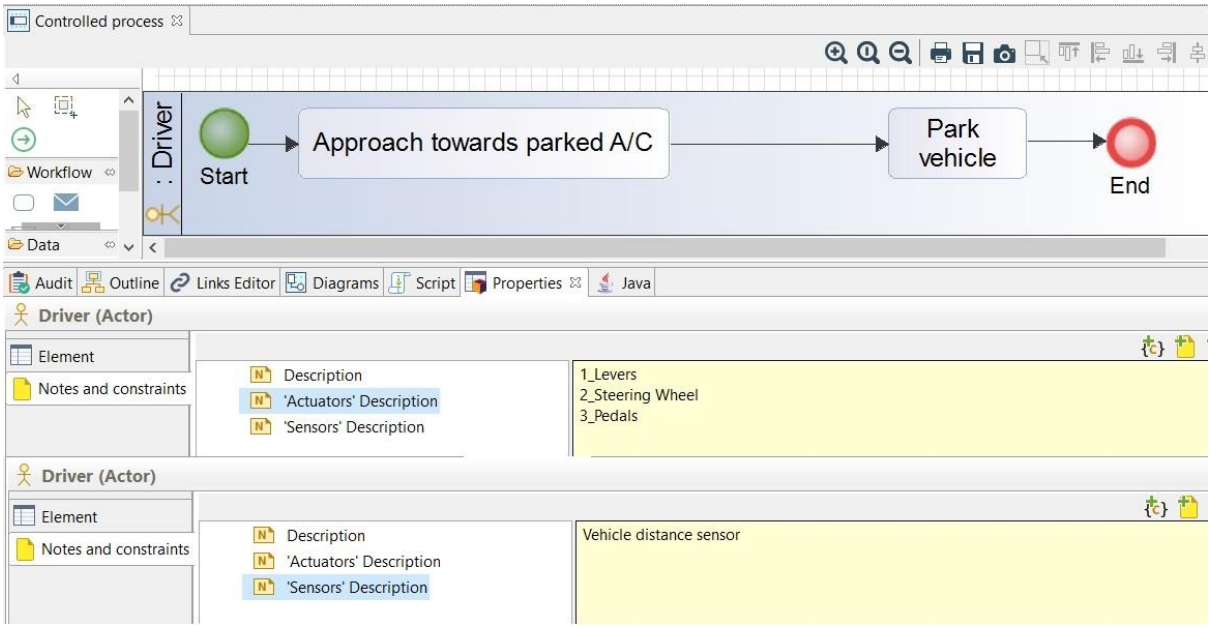
Obr. 20 Ukázka diagramu procesu dle notace BPMN v prostředí nástroje Modelio

Jak lze vidět z obr. 20, procesní diagram obsahuje funkční dokumentaci systému, tedy dokumentaci, co systém dělá spíše než co systém je (tedy popis konkrétních objektů, které funkce systému poskytují). Taková dokumentace je užitečná pro využití v rámci realizace metodiky CAST protože může podpořit práci analytika, který již nemusí pracovat s extrémně detailním popisem systému. Takový popis by mohl z pohledu konkrétní analýzy omezovat rozsah analýzy na módy selhání jednotlivých komponent a odvádět pozornost od řešení systémových problémů.

Dostupné nástroje pro modelování procesů lze využít pro tvorbu základu metodikou popsaného konceptuálního modelu, neboť tyto disponují možností ukládání dat v potřebném rozsahu. Následující podkapitoly uvádí, jak lze za tímto účelem modelovací nástroje využít.

3.4.1 Popis řídící smyčky

Řídící smyčka, která je dle teorie zpětnovazebního řízení využita v teorii STAMP, se skládá ze čtyř základních elementů, kterými jsou řízený proces, senzory, aktivní prvky řízení a řídící proces. Řízeným procesem je v modelu BPMN každá činnost uspořádaná v procesním diagramu. Každé z činností má být přidělena právě jedna role, která je za její provedení odpovědná. Z pohledu STAMP je taková odpovědná role řídícím prvkem. Do atributů odpovědné role lze doplnit seznam aktivních prvků řízení a seznam senzorů, které má daný řídící prvek k dispozici. Příklad implementace popisu řídící smyčky dle teorie zpětnovazebního řízení do modelu BPMN uvádí obr. 21. Obrázek ukazuje doplnění popisu dostupných aktivních prvků řízení (‘Actuators’ Description) a senzorů (‘Sensors’ Description), konkrétně pák (“1_Levers”), volantu (“2_Steering Wheel”), pedálů (“3_Pedals”), a senzoru vzdálenosti (“Vehicle distance sensor”). Tímto je možné vložit část potřebných dat pro analýzu dle modelu STAMP přímo do provozní dokumentace letecké organizace.



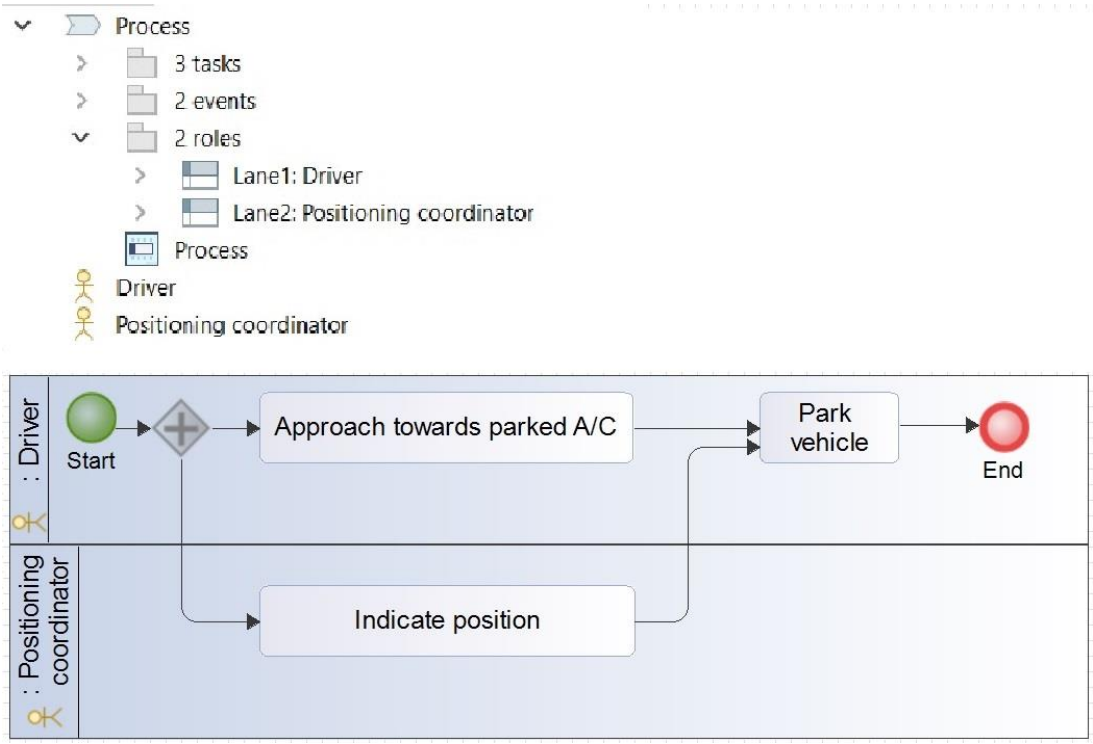
Obr. 21 Ukázka implementace popisu řídící smyčky dle notace BPMN v prostředí nástroje Modelio

3.4.2 Knihovna řídících prvků

Role zaměstnanců, kteří jsou odpovědní za jednotlivé procesy, lze zobrazit v knihovně odpovědných rolí. Pro účely popisované metody jsou role definovány tím, jaké aktivní prvky řízení a senzory má řídící prvek pro danou činnost k dispozici. Příklad náhledu do knihovny řídících prvků uvádí obr. 22. Knihovna na tomto obrázku obsahuje dvě role – konkrétně řidiče vozidla (“Driver”) a koordinátora parkování (“Positioning coordinator”). Jak již bylo zmíněno v kapitole 3.3.3., zavedení knihovny zjednodušuje správu provozní dokumentace s ohledem na doplnění informací potřebných pro provádění analýzy STAMP. S pomocí běžných nástrojů pro modelování procesů postačuje zavést knihovnu řídících prvků, nicméně v závislosti od konkrétního použitého nástroje lze také uvážit zavedení dalších knihoven, které správu provozní dokumentace můžou v konkrétních případech ulehčit. Zavedení jiných knihoven sleduje stejný princip jako zavedení knihovny řídících prvků.

4. Srovnání novosti postupů se současnými standardy

Metodiku lze srovnat z pohledu novosti postupů současných standardů ve dvou ohledech: vůči metodice analýzy nehod CAST dle teorie modelu bezpečnosti STAMP, a také vůči současnému standardu sběru a zpracování dat v letecké dopravě. Následující kapitoly přibližují oba pohledy.



Obr. 22 Ukázka využití knihovny řídících prvků dle notace BPMN v prostředí nástroje Modelio

4.1 Srovnání novosti v kontextu metodiky CAST

Vlastní popis metodiky již obsahuje přímé srovnání metodiky CAST dle teorie modelu bezpečnosti STAMP. Metodika CAST je založena na teorii modelu STAMP stejně jako i vyvinutá ontologie pro tento dokument. Obě metodiky jsou vzájemně kompatibilní, nicméně tento dokument popisuje nové technické možnosti jak podpořit realizaci vybraných kroků metodiky CAST s pomocí vyvinuté ontologie a jak dosáhnout prakticky využitelných výstupů v letecké dopravě, zejména v rámci standardů pro řízení bezpečnosti, které se zde využívají. Na rozdíl od metodiky CAST je zde díky aplikaci ontologie nová možnost pro integraci procesu sběru a zpracování dat o událostech z provozu. Ontologie umožňuje využít běžnou provozní dokumentaci jako zdroj potřebných informací pro realizaci sběru a zpracování dat o bezpečnosti a data o bezpečnosti posléze ukládat v kontextu té samé provozní dokumentace. Tato skutečnost přináší kromě výhod samotné integrace, tedy výhod jednotného systému pro několik manažerských případů užití, i několik nových možností: (1) metodiku CAST je možné realizovat s kompletním udržovaným popisem systému, který data vytvořil a nejen ad-hoc reprezentací systému, který je nutné v každé analýze vytvořit zvlášť; (2) ukládání dat o bezpečnosti přímo v kontextu provozní dokumentace vytváří lepší a efektivnější podporu pro identifikaci problémových částí systému jakož i nápravných opatření, která mají potenciál bezpečnostní problémy řešit; (3) v případě využití technologie ontologického modelování i v jiných doménách než je ta bezpečnostní, bude možné částečně automatizovaným způsobem identifikovat souvislosti v datech o bezpečnosti s daty o kvalitě, spolehlivosti, finanční efektivitě apod. a navrhovat v kontextu provozní dokumentace celosystémová řešení.

4.2 Srovnání novosti v kontextu standardu letecké dopravy

V kontextu současných standardů sběru a zpracování dat o bezpečnosti v letecké dopravě se jedná především o novost, kterou do letecké dopravy přináší teorie modelu STAMP a podpora pro realizaci metodiky CAST a která je (díky vyvinutému technologickému řešení) nyní dostupnější z pohledu již existujících a využívaných systémů sběru a zpracování dat o bezpečnosti v letectví.

Současné standardy pro tyto systémy jsou stanoveny především dokumentem ICAO Doc. 9859 Safety Management Manual od Mezinárodní organizace civilního letectví ICAO, dnes již v 4. edici z roku 2018. Tento dokument stanovuje, že organizace v letecké dopravě a také státy by měly zřídit systém pro sběr a zpracování dat o bezpečnosti a také stanovuje principy, jaká data a jakým způsobem sbírat a zpracovávat. Tyto principy jsou dodnes založeny na modelech bezpečnosti SHELL a na Reasonově modelu švýcarského sýra, tedy na identifikaci nehod a incidentů společně s faktory těchto událostí dle zmiňovaných modelů bezpečnosti. Jedná se především o snahu klasifikovat události dle existujících taxonomií bezpečnosti, v letectví zejména taxonomie ICAO ADREP a v Evropě taxonomie ECCAIRS, resp. její redukovaná verze známá jako RIT (Reduced Interface Taxonomy). Takto zpracovaná data se využívají pro analýzu pomocí tzv. ukazatelů bezpečnosti, které je možné vyhodnocovat na trend, resp. závislosti vůči jiným ukazatelům bezpečnosti. Ostatní procesy definované ICAO se v tomto kontextu týkají úplnosti či ochrany dat a jako takové nejsou touto metodikou inovovány.

Novost vůči uvedeným standardům letecké dopravy se týká především posunu v modelu bezpečnosti, který vysvětluje bezpečnostní události. V kontextu této metodiky je tedy modelem bezpečnosti model STAMP, který se snaží o celosystémové posouzení úrovně bezpečnosti, resp. o identifikaci problémů bezpečnosti na úrovni systému jako celku s využitím teorie zpětnovazebního řízení. Metodika přináší klíčové inovace a technické možnosti, díky kterým je možné překonat rozdíl mezi teorií a reálnými procesy sběru a zpracování dat a ulehčit tak implementaci teorie modelu STAMP do letecké dopravy. Metodika v souladu s teorií vede uživatele na tvorbu záznamů o událostech, které jsou úzce propojeny s popisem systému, který data vytvořil, a tím umožňuje právě celosystémové analýzy bezpečnosti, kde klíčem není sledování vybraných ukazatelů bezpečnosti v čase tak, jak je tomu dnes v letectví, ale právě sledování chování jednotlivých částí systému a úvaha, které části systému nebo která bezpečnostní opatření navzájem souvisí a jakým způsobem je možné efektivně řídit bezpečnost z pohledu systému jako celku. V tomto ohledu metodika svým technickým řešením založeným na ontologickém inženýrství vytváří nové funkcionality, které umožňují rychlejší, jednodušší a přesnější analýzy a řízení rizik v kontextu současných systémů řízení bezpečnosti v letectví.

5. Popis uplatnění certifikované metodiky

Tato metodika popisuje možnosti pro zefektivnění analýzy a řízení rizik s využitím konceptuálního modelování, tedy vyvinuté ontologie STAMP, na základě úpravy procesu sběru a vyhodnocení bezpečnostních dat. Je určena leteckým organizacím, v prostředí kterých je možné ji implementovat do systémů řízení bezpečnosti, resp. do prostředí kterých nabízí technické a metodické řešení pro integraci procesů řízení provozní dokumentace a

řízení bezpečnosti. Metodiku lze uplatnit v několika kontextech uvedených v následujících odstavcích. I když se jedná o inovativní řešení, které není dnes vyžadováno žádnou platnou legislativou nebo leteckým standardem, nabízí potenciál pro zlepšení v oblastech, které se legislativa a letecké standardy snaží řešit a tak přispívá k efektivnímu naplnění jejich cílů.

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 zavádění a udržování systému pro sběr a zpracování dat o bezpečnosti (Safety Data Collection and Processing System - SDCPS).

Metodiku lze uplatnit v kontextu platné evropské legislativy týkající se sběru a zpracování dat o bezpečnosti leteckého provozu, tedy zejména nařízení Evropské komise č. 996/2010, č. 376/2014 a č. 2015/1018.

Metodiku lze také uplatnit v kontextu hlášení událostí dle regulatorních požadavků ESARR2 (EUROCONTROL Safety Regulatory Requirement) od Evropské organizace pro bezpečnost leteckého provozu EUROCONTROL.

6. Ekonomické aspekty

Aplikace metodiky přináší několik nákladů souvisejících s její implementací. Pokud je metodika implementována do vlastního softwarového řešení, pak zde vznikají náklady na takovou implementaci, dále pak náklady na proškolení personálu a úpravu relevantních procesů v konkrétní organizaci. V některých případech může být vhodné navýšit počet zaměstnanců bezpečnostní jednotky/oddělení konkrétní organizace, nicméně tato metodika takové opatření nepokládá za zcela nezbytné pro její implementaci. Pokud je metodika implementována nezávisle vůči existujícím softwarovým řešením, zejména s využitím volně dostupných nástrojů, pak odpadají náklady související s úpravou existujících systémů, ale také dochází ke ztrátě z příležitostí, které přináší integrované řešení.

Potenciální ekonomické přínosy nelze přesně vyčíslit, nicméně tyto primárně souvisí se zlepšením v procesech systému řízení bezpečnosti, a tedy s vyšší efektivitou tohoto systému. Efektivní řízení bezpečnosti přináší také zlepšení ve finanční kondici organizací, jelikož se díky tomu v provozu vyskytuje méně událostí celkově, a události lze lépe předvídat, a tedy i lépe alokovat finanční rezervy na jejich případné řešení a nápravu [14]. Samostatnou ekonomickou příležitostí je realizace integrovaného řešení, které má potenciál snížit pracovní zátěž pracovníků bezpečnosti v kontextu sběru a zpracování dat o bezpečnosti a také zlepšit schopnost identifikace systémových příležitostí pro zlepšení fungování konkrétní organizace a tím zlepšit schopnost alokace zdrojů organizací na problémy, které jsou prioritní k zachování bezpečného a efektivního provozu.

Seznam použité literatury

[1] Gabbar, H. A. *The design of a practical enterprise safety management system*. Dordrecht: Kluwer Academic Publishers, 2004. ISBN 9781402029493.

[2] Stolzer, A. J. a Goglia, J. J. *Safety management systems in aviation*. Second edition. Burlington, VT: Ashgate, 2015. ISBN 978-1472431783.

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

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

[5] Regulation (EU) No 376/2014 of the European Parliament and of the Council on the reporting, analysis and follow-up of occurrences in civil aviation. Brussels: Official Journal of the European Union, 2014, L122/18.

[6] Reason, J. T. *Managing the risks of organizational accidents*. Brookfield, Vt., USA: Ashgate, 1997. ISBN 978-1840141054.

[7] Grant, E., Salomon, P. M., Stevens, N.J., Goode, N. a Read, G.J. Back to the future: What do accident causation models tell us about accident prediction?. *Safety Science*. 2018, 104, 99-109. DOI: 10.1016/j.ssci.2017.12.018. ISSN 09257535.

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

[9] Hollnagel, E. *FRAM, the functional resonance analysis method: modelling complex socio-technical systems*. Burlington, VT: Ashgate, 2012. ISBN 978-1409445517.

[10] Hitzler, P., Gangemi, A., Janowicz, K., Krisnadhi, A. a Presutti, V. *Ontology engineering with ontology design patterns: foundations and applications*. Amsterdam, Netherlands: IOS Press. Studies on the Semantic Web, v. 025. ISBN 978-1614996750.

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

[12] International Civil Aviation Organization (ICAO). Annex 13 to the Convention on International Civil Aviation. Eleventh Edition. Montréal, 2016. ISBN 978-92-9249-968-6.

[13] Guizzardi, G. a Wagner, G. Using the Unified Foundational Ontology (UFO) as a Foundation for General Conceptual Modeling Languages. Poli, R., Healy, M. a Kameas, A. ed. *Theory and Applications of Ontology: Computer Applications*. Dordrecht: Springer Netherlands, 2010, 2010-8-12, s. 175-196. DOI: 10.1007/978-90-481-8847-5_8. ISBN 978-90-481-8846-8.

[14] Lališ, A., Červená, V., Stojić, S. a Kraus J. Methodology for Justification of Aviation Safety Investments. In: *2018 XIII International Scientific Conference - New Trends in Aviation Development (NTAD)*. IEEE, 2018, 2018, s. 87-90. DOI: 10.1109/NTAD.2018.8551627. ISBN 978-1-5386-7918-0.

Seznam publikací, které předcházely metodice

Kostov, B., Ahmad, J., Křemen P. Towards Ontology-Based Safety Information Management in the Aviation Industry. Ciuciu, I., Debruyne Ch., Panetto, Weichhart, H. G., Bollen, P., Fensel, A. and Vidal, M.-E., ed. *On the Move to Meaningful Internet Systems: OTM 2016 Workshops*. Cham: Springer International Publishing, 2017, 2017-03-29, s. 242-251. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-55961-2_25. ISBN 978-3-319-55960-5.

Křemen, P., Kostov, B., Blaško, M., Ahmad J., Plos, V., Lališ, A., Stojić, S. a Vittek P. Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems. *Journal of Aerospace Information Systems*. 2017, 14(5), 279-292. DOI: 10.2514/1.I010441. ISSN 2327-3097.

Ledvinka, M., Lališ, A. a Křemen, P. Toward Data-Driven Safety: An Ontology-Based Information System. *Journal of Aerospace Information Systems*. 2019, 16(1), 22-36. DOI: 10.2514/1.I010622. ISSN 2327-3097.

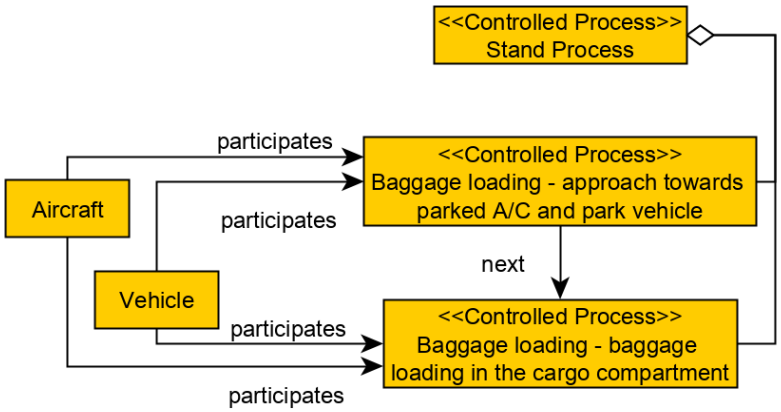
Saeeda, L. Iterative Approach for Information Extraction and Ontology Learning from Textual Aviation Safety Reports. Blomqvist, E., Maynard, D., Gangemi, A., Hoekstra, R., Hitzler, P. a Hartig, O. ed. *The Semantic Web*. Cham: Springer International Publishing, 2017, 2017-05-07, s. 236-245. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-58451-5_18. ISBN 978-3-319-58450-8.

Underwood, P., Waterson, P. a Braithwaite, G. 'Accident investigation in the wild' – A small-scale, field-based evaluation of the STAMP method for accident analysis. *Safety Science*. 2016, 82, 129-143. DOI: 10.1016/j.ssci.2015.08.014. ISSN 09257535.

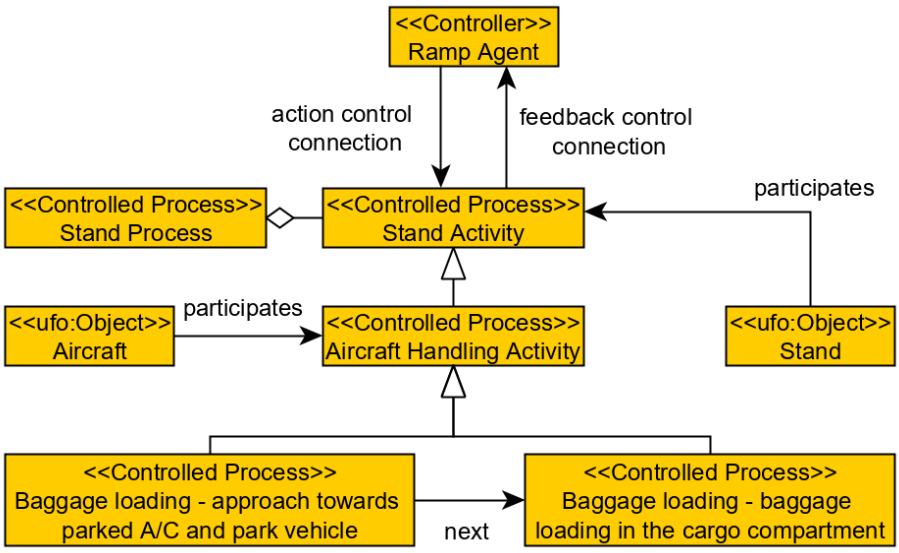
Příloha 1: Volný překlad klíčových pojmů z teorie STAMP

anglický výraz	český ekvivalent
accident	nehoda
actuator	aktivní prvek řízení
control loop	řídící smyčka
controller	řídící prvek
controlled process	řízený proces
enforce	prosazovat
feedback	zpětná vazba
process model	model řízeného procesu
safety constraint	bezpečnostní omezení
sensor	senzor
variable	řízená proměnná
violate	narušit

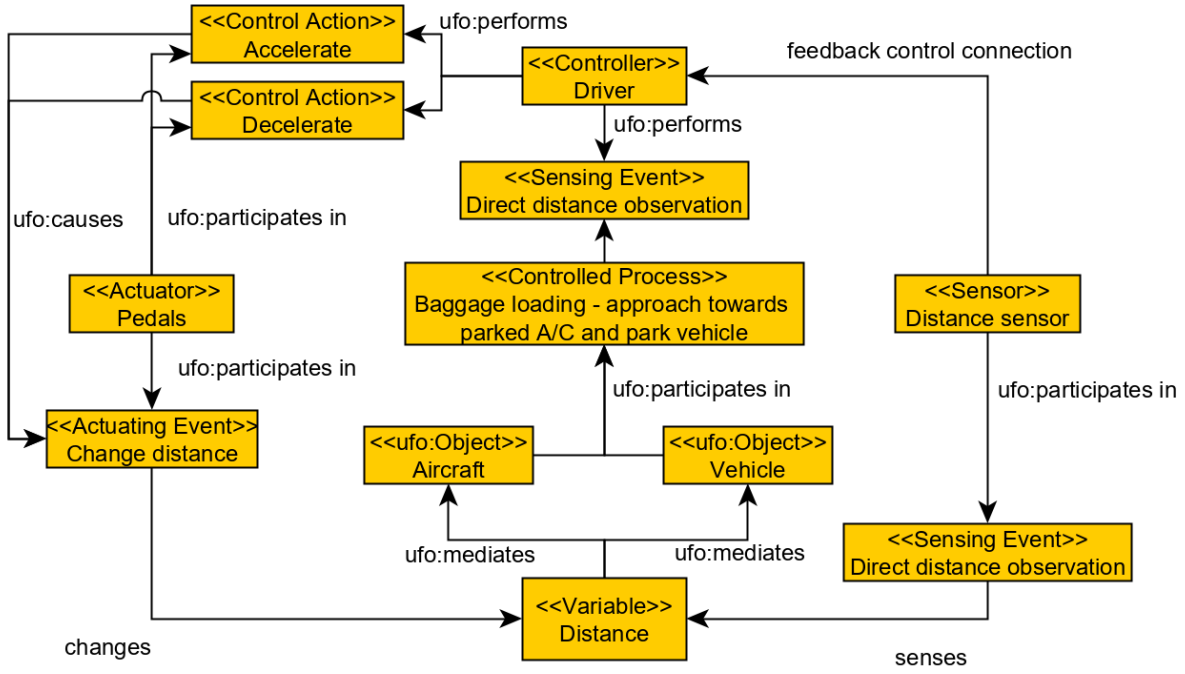
Příloha 2: Ukázka aplikace ontologie STAMP na průmyslové situace z domény letišť



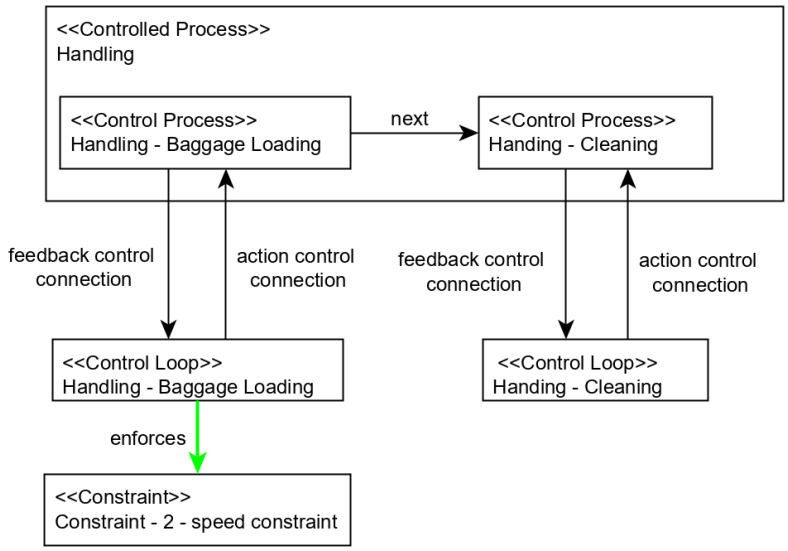
P1: Popis procesu nakládání batožiny do letadla v průběhu pozemního odbavení letadla.



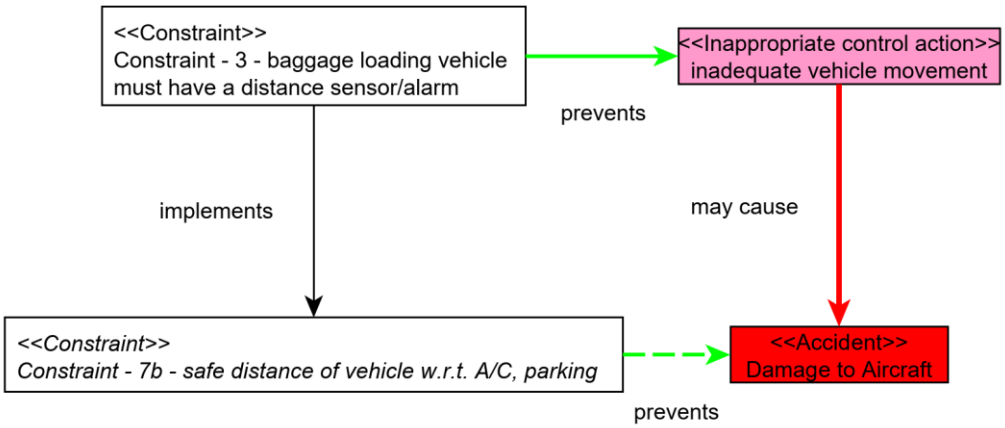
P2: Specifikace účastníků a relací řízení/zpětné vazby v kontextu popisu procesu nakládání batožiny do letadla



P3: Modelování řízení a událostí souvisejících s řidičem pásového dopravníku pro nakládání batožiny do letadla



P4: Modelování vztahu řízeného procesu, řídící struktury a bezpečnostních omezení v kontextu pozemního odbavení letadel



P5: Modelování vztahu bezpečnostních omezení v kontextu nežádoucích událostí, kterým mají předcházet