ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. ADAM KOHOUTEK

Ověření modelu STAMP v procesech bezpečnostní kontroly

DIPLOMOVÁ PRÁCE

2021

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K621 ..... **Ústav letecké dopravy**

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Adam Kohoutek

Studijní program (obor/specializace) studenta:

navazující magisterský – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Využití modelu STAMP v procesech bezpečnostní kontroly letišť**

Název tématu (anglicky): Application of STAMP model in airport security control processes

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cíl práce: Aplikace modelu STAMP a jeho metodiky STPA v procesech bezpečnostní kontroly letišť
- Analyzujte model bezpečnosti STAMP a metodiku STPA
- Analyzujte současné postupy bezpečnostní kontroly na letištích
- Vyberte a definujte vhodnou část bezpečnostní kontroly jako systém pro analýzu pomocí STPA
- Aplikujte metodu STPA na vybraný systém a procesy bezpečnostní kontroly
- Vyhodnoťte dosažené výstupy

Rozsah grafických prací: dle pokynů vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.

Leveson, N., Thomas, J. STPA Handbook, 2018.

Vedoucí diplomové práce: **Ing. Roman Vokáč, Ph.D.**

Ing. Andrej Lališ, Ph.D.

Datum zadání diplomové práce: **17. července 2020**

(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **1. prosince 2021**

a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní L. S.

doc. Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy

doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Adam Kohoutek
jméno a podpis studenta

V Praze dne 17. srpna 2021

Poděkování

Za odborné vedení práce, podporu a pomoc s vypracováním bych tímto rád poděkoval Ing. Romanu Vokáčovi, Ph.D. a doc. Ing. Andreji Lališovi Ph.D. Zároveň bych rád poděkoval své rodině za nestálou a neúnavnou podporu při mém studiu i práci.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze, dne 27.11.2021

podpis

Autor: Adam Kohoutek

Název: Ověření modelu STAMP v procesech bezpečnostní kontroly

Instituce: České Vysoké Učení Technické v Praze, Fakulta dopravní

Obor: Provoz a řízení letecké dopravy

Rok: 2021

Abstrakt:

V dnešní době velice komplexních systémů a neustále zvětšujících se nároků na bezpečnost je potřeba, i v těch nejvíce složitých systémech, odhalit možná rizika či ztráty. Tato práce se soustředí na identifikaci možných rizik při plánování směn v socio-technickém systému bezpečnostní kontroly. K tomuto účelu je využita metoda STPA a model STAMP. V práci jsou podrobně popsány činnosti jednotlivých řídících prvků a vazby mezi nimi, čímž vznikl celkový model a popis všech činností při plánování směn v komplexním systému bezpečnostní kontroly. Cílem práce je provedení STPA analýzy v procesu plánování směn a pokrytí provozu u bezpečnostní kontroly na Letišti Praha.

Klíčová slova:

Bezpečnostní kontrola, Safety I., Safety II, Safety III, STAMP, STPA, Plánování směn

Author: Adam Kohoutek

Title: STAMP model verification in security control processes

Institution: Czech Technical University in Prague, Faculty of Transport

Study program: Air Transport

Academic year: 2021

Abstract:

In today's very complex systems and ever-increasing security requirements, it is necessary, even in the most complex systems, to detect possible risks or losses. This work focuses on the identification of possible risks in shift planning in the socio-technical system of security control. The STPA method and the STAMP model are used for this purpose. The work describes in detail the activities of individual controls and the links between them, which created an overall model and description of all activities in shift planning in a comprehensive security control system. The aim of the work is to perform STPA analysis in the process of shift planning and traffic coverage at security control at Prague Airport.

Key words:

Security control, Safety I., Safety II, Safety III, STAMP, STPA, Shift planning

Obsah

1 Úvod 9
2 Přístup Safety I. 11
2.1 Koncept Safety I 11
2.2 Problematika vývoje systému a přístupu Safety I 12
2.3 Určení bezpečnosti systému pomocí Safety I 15
2.3.1 Bimodální předpoklad 16
2.3.2 Předpoklad dekompozice 16
2.4 Shrnutí Safety I 17
3 Přístup Safety II. 18
3.1 Variabilita člověka v systému 18
3.2 Řízení bezpečnosti 19
3.3 Princip emergence (vzniku) 20
4 Přístup Safety I. vs Safety II. vs Safety III 22
5 STAMP 24
6 STPA 28
6.1 Definovat účel analýzy 29
6.1.1 Identifikace možných ztrát 30
6.1.2 Identifikace nebezpečí na úrovních systému 31
6.1.3 Identifikace omezení na úrovni systému 32
6.1.4 Upřesnění nebezpečí 33
6.2 Modelace řídící struktury 34
6.3 Identifikace nebezpečných řídících akcí 38
6.4 Identifikace scénářů ztrát 39
6.4.1 Identifikace scénářů, které vedly k nebezpečné řídící akci 40
7 STPA v procesech bezpečnostní kontroly 43
7.1 Definice účelu analýzy 43

7.1.1 Identifikace možných ztrát 43
7.1.2 Identifikace nebezpečí na úrovních systému 43
7.1.3 Identifikace omezení na úrovni systému v procesech bezpečnostní kontroly....44
7.2 Modelace řídící struktury v procesech bezpečnostní kontroly 45
7.2.1 Popis jednotlivých řídících prvků v řídící struktuře 48
7.2.2 Popis řídících akcí a zpětných vazeb....51
7.3 Identifikace nebezpečných řídících akcí v procesu bezpečnostní kontroly...58
7.4 Omezení řídícího prvku 59
7.5 STPA a lidský činitel....60
7.6 Identifikace scénářů vedoucích k nebezpečné řídící akci....62
8 Diskuse 64
9 Závěr 66
Zdroje……...70
Příloha 1 – Identifikované nebezpečné řídící akce……73
Příloha 2 – Identifikované omezení řídícího prvku……..……...74
Příloha 3 – Scénáře pro jednotlivé nebezpečné řídící akce....……77

1 Úvod

Bezpečnostní kontrola je nedílnou součástí každého cestování letadlem. Nejedná se však pouze o pravidla, omezení a samotnou kontrolu cestujících. Nezbytnou součástí jsou také zaměstnanci samotní. Právě oni zaručují a zabezpečují bezpečnost (security) jako takovou. Počet potřebných zaměstnanců je závislý na objemu provozu. Zajištění zaměstnanců pro pokrytí provozu letadel – pro kontrolu všech cestujících včas, aby nedošlo ke zpoždění letadla, nepokrytí provozu, neobsazení stanoviště nebo vytvoření velké řady čekajících cestujících – je velice komplikovaný proces. Tato práce se zaměří právě na analýzu zabezpečení dostatečného množství pracovníků bezpečnostní kontroly pro pokrytí provozu na Letišti Václava Havla v Praze. K analýze systému bude využit model STAMP (Systems-Theoretic Accident Model and Processes), přesněji STPA analýza (Systems-Theoretic Process Analysis).

STAMP byl vytvořen prof. Levenson z MIT a jedná se o model kauzalit nehod založený na systémové teorii a systémovém myšlení. STAMP model zahrnuje software, hardware, lidské rozhodování, lidský činitel a organizační strukturu. V současné době jsou STAMP a STPA využívány především v oblasti provozní bezpečnosti (safety) v letectví. Pro security jsou využíván hlavně v oblasti kybernetické bezpečnosti [1]. V této práci se zaměřím na aplikaci STPA do systému bezpečnostní kontroly. Cílem STPA je odstranit, zmírnit nebo kontrolovat nebezpečí, která mohou vést k identifikovaným ztrátám ze strany zúčastněných stran.

V současné době je většina systémů velice komplexních a již nelze používat staré metody vyvinuté v minulém století pro jejich analýzy. Systémy jsou velice složité, zahrnují do sebe mnoho faktorů, které je ovlivňují, a již nemůžou podléhat přístupu dekompozice a analýze kořenových příčin. Pro pochopení nového přístupu k bezpečnosti bude v práci rozebrán i rozdíl mezi jednotlivými typy safety (Safety I, Safety II a Safety III). Safety III je nejnovějším přístupem k safety. STAMP a STPA zapadají právě do tohoto přístupu. V práci je vytvořen řídící model dle pravidel definovaných prof. Levenson, která je autorkou STAMP. Dále jsou v práci identifikovány všechny nebezpečné řídící akce, které se mohou v systému objevit.

Současné systémy značně propojují člověka a techniku, hovoříme tedy o socio-technickém systému, ve kterém spolupracuje člověk a technika pro dosažení zadaného cíle. Takovým systémem je i zabezpečení dostatečného počtu pracovníků

bezpečnostní kontroly. Za technickou část systému lze považovat programy, aplikace a systémy, ve kterých lidé v systému pracují.

2 Přístup Safety I.

Prvním a nejdůležitějším krokem při rozboru jednotlivých přístupů safety je samotná definice safety: *„Stav, ve kterém jsou rizika spojená s letectvím, činnosti související s provozem letadel nebo s přímou podporou provozu letadel omezeny a kontrolovány na přijatelnou úroveň“.* [2].

Model STAMP a STPA analýza jsou proaktivní přístupy ke zvládání hrozeb a řízení rizik. Proaktivní přístupy jsou relativně nové ve všech odvětvích. V dnešní době převládají především tzv. reaktivní přístupy k provozní bezpečnosti (safety). Stejný přístup má i security. Z historie víme, že změny v postupech či technologiích využívaných u bezpečnostní kontroly se vždy staly až poté, co došlo k teroristickému činu nebo k pokusu o něj. Security reaguje vždy zpětně, příkladem může být případ odhalení plánovaného útoku na více letadel za použití tekutých výbušnin. Po tomto odhalení došlo k zavedení limitu objemu tekutin na 100 ml a v maximálním celkovém objemu 1 litru. [6]

Reaktivní přístupy jsou založeny na reakci po nežádoucí či nepředpokládané situaci nebo akci. S příchodem nových systémů a technologií, které jsou složitější a více komplexní, již reaktivní přístupy nebyly dostačující. Z tohoto důvodu se začaly objevovat proaktivní přístupy, tedy přístupy, které aktivně sledují systém a snaží se predikovat či předcházet nežádoucím událostem nebo slouží k detekci nežádoucích akcí v řízení systému [7]. V případě safety se rozlišují 3 přístupy k safety – Safety I, Safety II a Safety III.

2.1 Koncept Safety I

Přístup Safety I byl z historického hlediska logický, a i v dnešní době je v určitých systémech použitelný. Avšak bezpečnostní kontrola je velice složitý systém a v takovém systému nelze využít předpoklady Safety I. Přístup Safety I spočívá v reakci na nechtěnou událost, tedy použití tohoto přístupu je podmíněno vznikem nechtěné události nebo identifikace potenciálního rizika. Po takové události nastane šetření příčiny nehody nebo vzniku potenciálního rizika [1].

Z historického hlediska byly systémy v 70. letech minulého století relativně jednoduché v porovnání s dnešními. Využití a závislost systému na informačních technologiích byla silně omezena především kvůli samotnému výkonu informačních technologií v té době. Omezenost IT znamenala málo podpůrných funkcí pro fungování systému, a i když tyto podpůrné funkce existovaly, bylo jich málo, byly většinou jednoduché a na sobě nezávislé. Integrace mezi jednotlivými odvětvími byla malá, jednalo se spíše o samostatně fungující systémy, které pokud už byly spojené, bylo toto spojení velmi volné. V takovýchto systémech bylo relativně jednoduché pochopit, kde se stala chybná událost a sledovat její důsledky. Z tohoto důvodu se v safety pracovalo s následujícími předpoklady [1]:

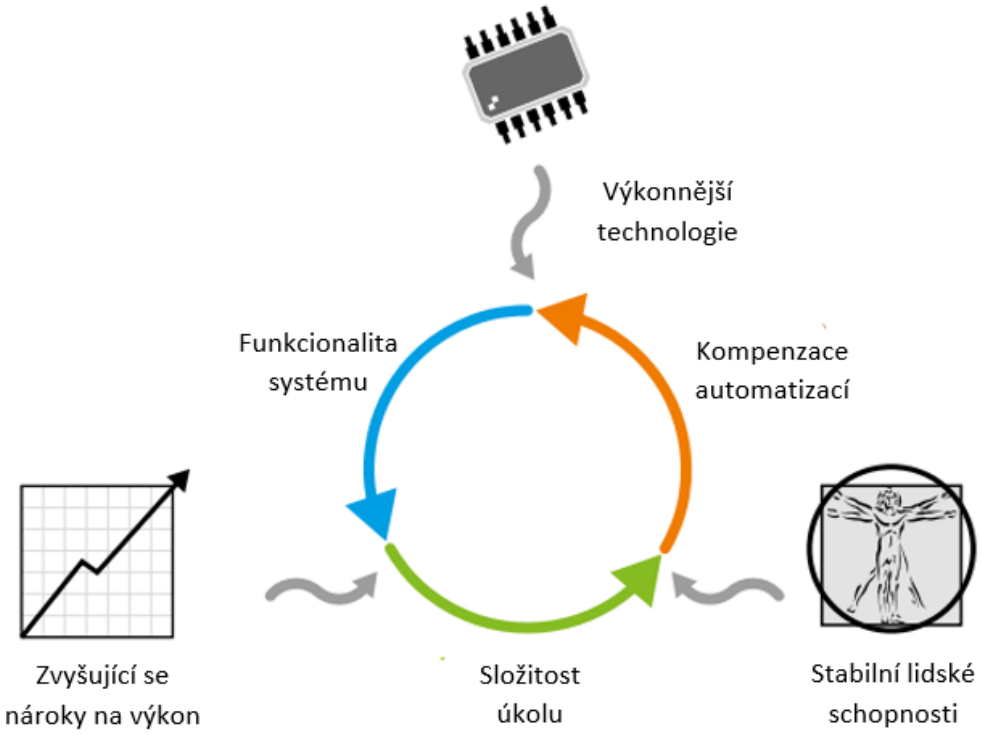
- Systém a pracovní prostředí jsou navrženy správně a jsou udržovány správně a podle pravidel
- Postupy práce jsou srozumitelné, kompletní a správné
- Lidé pracující v systému (operátoři) se chovají dle předpokladů. Práci vykonávají přesně tak, jak byli vytrénováni a naučeni. Pracují tak, jak mají a dle představ
- Návrháři předpověděli každou eventualitu systému a poskytli systému dostatek možností na odpovídající reakci. Pokud by mělo dojít k naprostému zhroucení systému, systém bude degradovat, protože operátoři dokážou porozumět a řídit každou nepředvídatelnou situaci

2.2 Problematika vývoje systému a přístupu Safety I

Postupem času docházelo k postupnému rozvoji každého systému. Tento rozvoj byl umožněn především díky dvěma faktorům. Prvním z nich je vývoj informačních technologií, které za poslední tři desetiletí prošly obrovským vývojem a v dnešní době jsou všudypřítomné a téměř žádný systém bez nich není schopný efektivně pracovat. Druhým faktorem je zvýšení požadavků od samotných uživatelů systému. Vývoj technologií a zvyšování požadavků uživatelů poté vede k neustálé nutnosti rozvoje systému, hovoříme o tzv. *Zákonu napnutého systému* [3].

Jedná se o zákon, který stanoví, že pokud systém dosáhne své meze, je nutné aplikovat nějaké vylepšení. Postupem času však využití systému dosáhne této nové meze a tento nekonečný kruh se stále opakuje. Dalo by se říct, že bychom novou mez systému mohli posunout ještě dále díky automatizaci, automatizace zvýší funkcionalitu

a výkonnost systému, avšak také zvyšuje požadavky na systém. Koncept zákona napnutého systému je znázorněn na obrázku 1.



Obrázek 1: Zákon napnutého systému (Zdroj: [3] Upraveno autorem)

Obrázek 1 ukazuje kruh nutného neustálého posunu meze ve využívaném systému. Práce a schopnosti lidí jsou stabilní, avšak požadavky na systém překračují možnosti lidí a musí tedy dojít k automatizaci nebo zavedení chytrých technologií pro zvládnutí větších požadavků. Nové technologie s sebou přináší i větší funkcionalitu systému a nová funkcionalita systému opět zvyšuje požadavky na systém a nové požadavky zvyšují náročnost úkolů. Tím je kruh kompletní a systém se tak musí neustále zvětšovat a rozvíjet.

Přesným příkladem takového systému je bezpečnostní kontrola na letišti. S vývojem letectví docházelo ke stále zvětšujícímu se počtu cestujících. Bezpečnostní kontrolu zpočátku vykonávali pouze lidé bez pomoci technologií. S příchodem více sofistikovaných hrozeb terorismu však došlo ke zvýšení složitosti požadavků na pracovníky bezpečnostní kontroly. Zvyšující se počty cestujících a větší požadavky na pracovníky kvůli terorismu bychom mohli označit jako zvyšující se požadavky na výkon (increasing performance demands). Z těchto požadavků na výkon poté vychází větší složitost úkolů pro pracovníky (task complexity). Pracovníci bezpečností kontroly již nemohli tento nápor zvládat, byla tedy nutná kompenzace v podobě

automatizace a zavedení chytrých technologií. Kompenzace s sebou přinesla nárůst schopnosti systému a tím je uzavřen neustále opakující se kruh.

Zde je nutné zmínit obrovský vliv legislativních požadavků na bezpečnostní kontrolu a na využívanou techniku. Legislativa se vždy snaží předcházet a eliminovat rizika pro letectví především tím, že předpisy pravidelně vyžadují využívání novějších a bezpečnějších technologií.

S vývojem techniky a systémů docházelo k nepředpokládaným nehodám. Tyto nové nehody byly vysvětleny zavedením nových typů příčin. Mezi nové typy příčin patřil lidský činitel (např. pracovní zátěž nebo chyba člověka), typy chyb vztahující se k technologiím (únava kovů) nebo chyby vztahující se k organizaci systému (pohled na bezpečnost ve společnosti či firmě). Tyto přístupy byly velice účinné v poskytování krátkodobých řešení. Člověk si velice snadno zvykne na věci, které mu relativně rychle přinesou kýžený výsledek, v tomto případě objasnění příčiny nehody či ohrožení. Z toho důvodu je přístup Safety I velice rozšířený a pevně zakořeněný ve většině společnostech a systémech [1].

Účelem šetření nehod s principem využití Safety I je zjistit příčiny a přispívající faktory, které vedly k nehodám nebo ohrožení. Součástí tohoto přístupu je také snaha určit co nejpřesněji pravděpodobnost rizika a jeho posouzení. Je tedy stanovena linie mezi přijatelným a nepřijatelným rizikem. Principem Safety I je reagovat, pokud došlo k překročení této linie. Pro lepší představu o přístupu Safety I je zde obrázek 2.

Obrázek 2: Princip přístupu Safety I [1].

Obrázek 2 naznačuje přístup Safety I, kdy se soustředíme pouze na jednu chybnou událost. V tomto případě jednu chybnou událost (failure) z celkového počtu 10 000 událostí. Safety I se zaměřuje právě na tuto událost a snaží se najít příčinu, rizika a řešení, aby se taková událost již neopakovala. Typickým přístupem je zavedení určitých nových pravidel či bariér. Tento přístup k šetření má i většina úřadů a regulačních orgánů [3].

Vyšetřovatelé sepisují podrobné a velmi rozsáhlé zprávy o nehodách a událostech. Nepředpokládanou událost lze definovat jako událost, která není součástí standardních procesů systému [2]. Výsledkem je obrovské množství informací o tom, jak se všechny popsané věci zhoršují a degraduje jejich bezpečnost, a co musí být učiněno nebo vytvořeno pro zabránění dalším selháním. Obecným pravidlem pro Safety I je „najít a opravit“, tedy pokusit se najít poruchy a selhání, poté najít jejich příčiny a z těchto příčin vyvodit nutné kroky k předcházení takovým situacím. Typickým příkladem je vytvoření bariéry nebo eliminace příčin [3].

2.3 Určení bezpečnosti systému pomocí Safety I

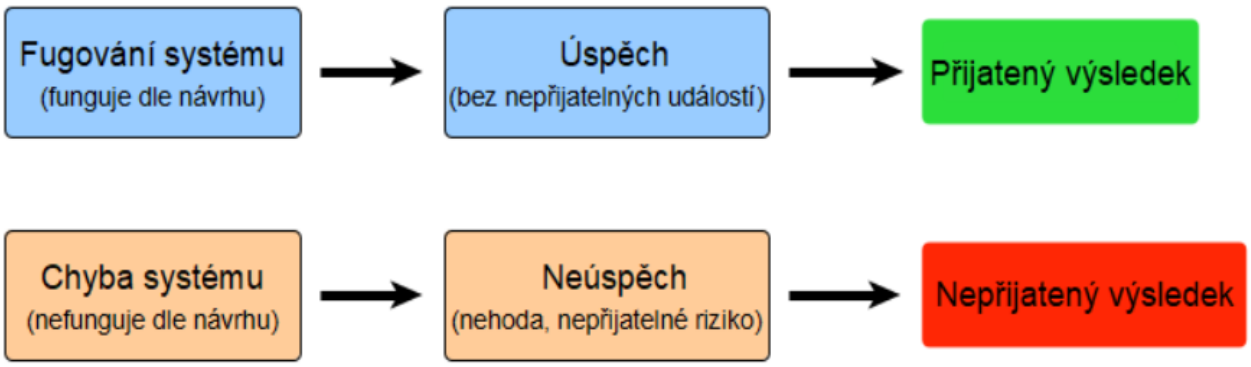
Výchozím bodem pro Safety I je nepřijatelné riziko nebo chybná událost. Zde však nastává problematika tohoto přístupu. Pokud se v systému nestaly žádné události, které by překračovaly stanovenou úroveň rizika nebo nedošlo k žádným chybným událostem, lze tento systém považovat za bezpečný?

Úroveň bezpečnosti, s využitím Safety 1, totiž nepřímo souvisí s počtem nepříznivých výsledků, tedy čím méně se pokazí věcí, tím větší je úroveň bezpečnosti a naopak. Pokud by nedocházelo k žádným chybným událostem ani překročení rizika, dalo se by říct, že úroveň bezpečnosti je 100 %. V takovém případě by to však znamenalo, že zároveň nejde naměřit žádná data a tím pádem nelze ani stanovit úroveň bezpečnosti [3].

Pokud bychom se znovu podívali na obrázek 2, tentokrát bychom se soustředili na jeho zelenou část. Zelená část ukazuje, že 9999 událostí k chybné události nevedlo. Těmto událostem však ve většině systémů není věnována pozornost. V dnešní době nejsou nastaveny žádné požadavky od regulačních orgánů, které by vyžadovaly kontrolu, průzkum či šetření těchto nechybných událostí [10].

2.3.1 Bimodální předpoklad

Bimodální pohled předpokládá, že přijatelné výsledky (riziko) a nepřijatelné výsledky (riziko) jsou zapříčiněny různými způsoby chování systému. Pokud systém a lidé v něm fungují správně, pracují přesně podle toho, jak je od nich a od systému očekáváno, je vše v pořádku. Pokud se něco pokazí, je to z důvodu poruchy systému nebo lidského selhání (obr. 3) [1].



Obrázek 3: Bimodální přístup Safety 1 (Zdroj: [14] Upraveno autorem)

2.3.2 Předpoklad dekompozice

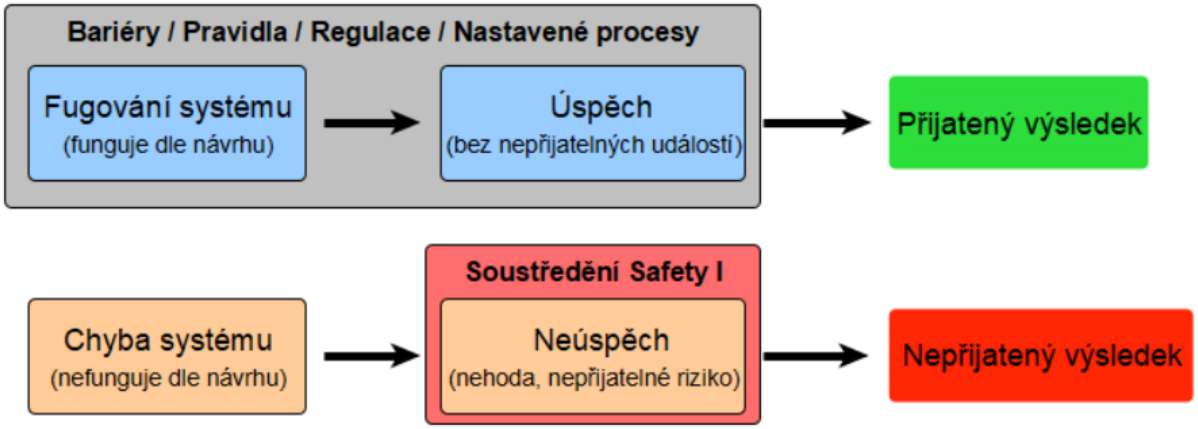
Jedná se o předpoklad, že každý systém lze rozložit na jednotlivé části systému. Při konstrukci systému dochází k pečlivému skládání jednotlivých komponentů tak, aby vznikl výsledný produkt. Safety I předpokládá, že systém lze logicky rozložit na části, tyto části pak analyzovat a eventuálně nalézt chybu. Zároveň pracuje s předpokladem, že všechny tyto části jsou schopny nezávislého fungování na ostatních částech.

Po nalezení chyby v jedné části dojde ke složení a od identifikované chyby se dále vytváří podrobná analýza [3]. Zároveň je zde stále nutné pracovat s prvním předpokladem, tedy s bimodálním modelem. Části systému buď fungují správně nebo nesprávně.

Tento odhad je v případě Safety I použit i v socio-technických systémech. Tedy v systémech, kde dohromady pracuje technologie a člověk. Navzájem spolupracují pro správné řízení systému. Předpokládá se, že dekompozici lze vytvořit pro jakoukoliv činnost nebo událost. Všechny předpoklady u dekompozice systému ale nelze použít pro moderní, složité a velice komplexní systémy. Většina nových systémů je ovlivněna obrovským množstvím vnitřních i venkovních pravidel a regulí [3].

2.4 Shrnutí Safety I

Všechny výše zmíněné body a předpoklady je možné shrnout do upraveného diagramu bimodálního přístupu Safety I. Tento obrázek ukazuje přístup Safety I jak k pozitivním událostem správnému fungování systému, tak i k chybným událostem.



Obrázek 4: Princip Safety I (Zdroj: [14] Upraveno autorem)

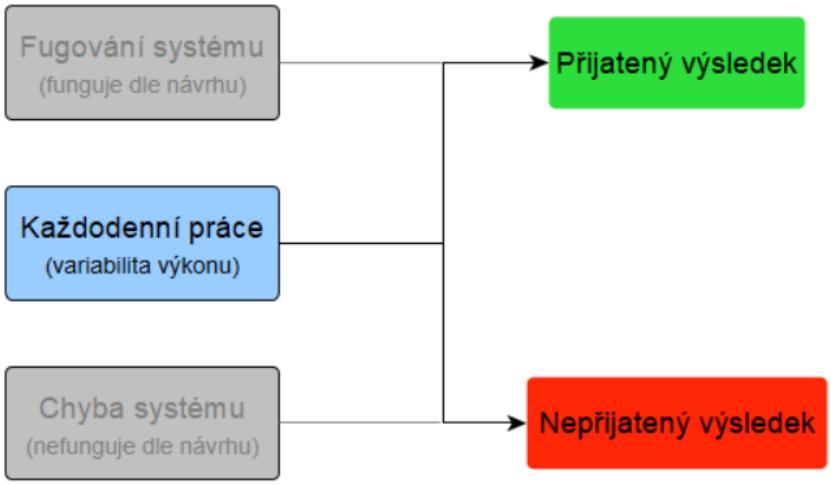
V Safety I je výchozím bodem pro řízení bezpečnosti buď identifikace nepřijatelného rizika nebo chybná událost. Oba tyto přístupy používají výše zmíněné pravidlo „najít a opravit“. V případě chybné události je snaha nalézt příčinu této události a vytvořit odpovídající úpravu v systému tak, aby se tato událost již nemohla opakovat (nová pravidla apod). V případě identifikace nepřijatelného rizika jde o jeho identifikování a odstranění nebo zmírnění [3].

3 Přístup Safety II.

Jak již název naznačuje, Safety II je novější a modernější přístup k bezpečnosti. Dalo by se říct, že je přesným opakem Safety I. Rozdílů mezi Safety I. a II. je mnoho, v následující části se zaměřím na několik z nich a vysvětlením rozdílů mezi typy zároveň definuji princip Safety II a jejího přístupu k řízení bezpečnosti.

3.1 Variabilita člověka v systému

Safety II již nevidí člověka v systému pouze jako potenciální zdroj nebezpečí a nepředpokládaných situací. Řadu dnešních systémů lze považovat za socio-technologické, kdy technologie a lidé pracují společně pro splnění jejich úkolu. Nový přístup safety totiž člověka považuje za klíčovou součást systému. V přístupu Safety II je člověk chápaný jako funkční součást systému. Člověk v systému, s přístupem Safety I, byl viděn pouze jako potenciální zdroj chybných událostí [10].



Obrázek 5: Přístup Safety II k výsledkům. (Zdroj: [1] Upraveno autorem)

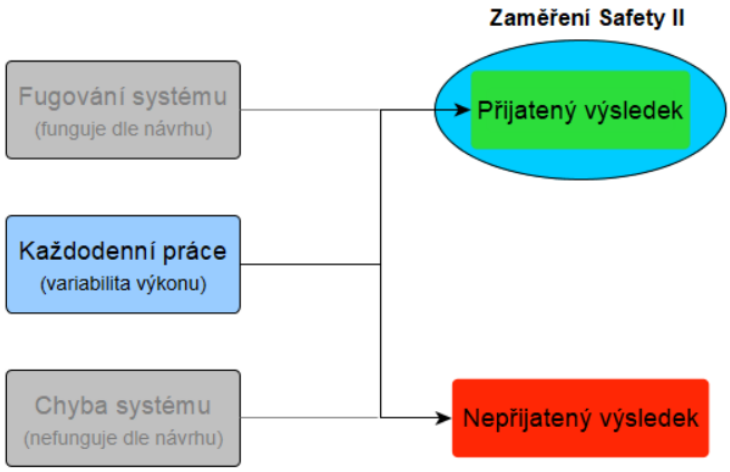
Obrázek 5 ukazuje, jak Safety II přistupuje k lidské variabilitě v každodenních procesech v systému. Zároveň zobrazuje další důležitý rozdíl v přístupech safety a tím je neexistence bimodálního modelu. Safety II vychází z předpokladu, že úspěchy i neúspěchy vychází právě z variability v systému samotném a nedějí se kvůli fungování, respektive nefungování systému jako u Safety I. V Safety II je člověk považován za zdroj větší bezpečnosti systému, a to především díky své variabilitě, tedy přizpůsobení se každodennímu výkonu. Člověk, jakožto součást systému, může být považován za lepší bariéru než například nová pravidla či omezení. Člověk dokáže

reagovat a rozhodovat se vždy podle nastalé situace. Nelze žádným způsobem popsat každou jednu situaci, která může v systému nastat, lze popsat pouze ty situace, které jsou nejvíce pravděpodobné nebo jsou velice jednoduché [3,15]. Pokud bychom se podívali na bezpečnostní kontrolu, je naprosto jasné, že v žádném případě není možné popsat všechny situace a varianty toho, co se může stát. Jedná se o velice složitý systém, ve kterém pracovníci bezpečnostní kontroly pracují za pomoci techniky takovým způsobem, aby co nejefektivněji a nejlépe odbavili cestující. Tedy máme v podstatě dva lidské činitele v systému, cestující a pracovníky, a nelze přesně definovat každou situaci, která může nastat. U bezpečnostní kontroly je variabilita a přizpůsobení se rozdílným situacím klíčová.

Variabilita je velice obtížná na sledování a kontrolu. Bezpečnostním principem řízení je usnadnit každodenní práci, předvídat vývoj a události, a udržovat adaptivní schopnost účinně reagovat na nevyhnutelné nepředpokládatelné situace. Lidé jsou považováni za nezbytný zdroj pro flexibilitu a odolnost systému. Bezpečnost je zajišťována pozorováním, vyhodnocováním a řízením (přímým nebo nepřímým) lidské výkonnosti a její variability [8].

3.2 Řízení bezpečnosti

Dalším velkým rozdílem je samotný přístup k řízení bezpečnosti. Řízení bezpečnosti při použití Safety II přešlo od – čím méně věcí se pokazí, tím lépe – k naprosto opačnému přístupu, tedy k zajištění, že co nejvíce věcí se stane správně [3]. Dle Safety II bychom neměli poruchy v systému brát jako individuální události, ale spíše ji považovat za výchylku každodenního pracovního výkonu [3]. Z toho vyplývá, že je velice podstatné pochopit a porozumět, proč se události v systému dějí tak, jak mají, abychom dokázali najít a pochopit, proč se dějí chybné události (viz. obr.6.) Toto je další z významných rozdílů mezi přístupy Safety I a Safety II. Nejde primárně o nalezení příčiny, ale spíše o nalezení rozdílu mezi normálním průběhem a průběhem při chybné události.



Obrázek 6: Přístup Safety II k nalezení chybné události (Zdroj: [1] Upraveno autorem)

Některé dnešní systémy jsou tak složité, že nelze předpovědět dopad nově zavedených změn v systému a jejich vedlejší účinky. V systému jsou nejistoty, které nelze předpovědět. Kvůli těmto nejistotám je nutná přítomnost člověka v systému, protože je variabilní a dokáže se přizpůsobit. Komplexnost práce se vyvíjí společně s vývojem technologií, proto je nutné upravit předpoklady pro současné socio-technické systémy:

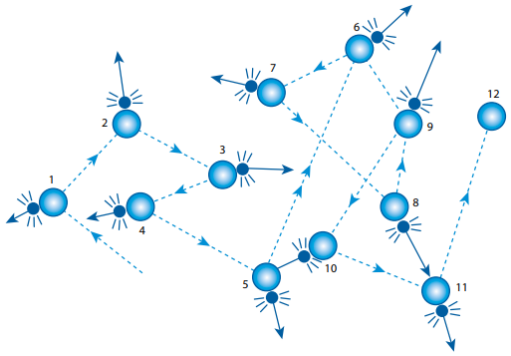
- Systémy nemohou být dekomponovány kvůli jejich složitosti a vzájemné propojenosti jednotlivých částí
- Funkce v systému již nelze považovat za bimodální (fungující / nefungující)
- Variabilita je nutná pro každodenní fungování systému
- Výsledky v systému vycházejí z variability člověka (jak správné, tak chybné)
- Ne všechny chyby musí být spojeny s poruchami, je nutné je chápat i jako výsledky spojení variability v systému

Přístup Safety II je tedy schopnost systému uspět za různých podmínek tak, aby počet zamýšlených výstupů byl co nejvyšší [10].

3.3 Princip emergence (vzniku)

Při hledání příčiny, proč se v systému stalo něco špatně, využívá Safety II tzv. emergence. Tím je myšlen princip, kdy jednotlivé příčiny vzniku chybné události jsou pozorovatelné a reálné, ale není jisté spojení mezi nimi. Při běžném přístupu (Safety I) by došlo k vytvoření stromu událostí nebo podmínek, které vedly k chybné události. Toto spojení je však u Safety II nejasné, protože podmínky, za kterých vznikla chybná událost, mohly být unikátní a neopakovatelné v daný moment nebo mohly

vzniknout z dalších unikátních spojení. Princip emergence nejlépe vystihuje obrázek 7.



Obrázek 7: Princip emergence (vzniku) Safety II [3]

Jak lze vidět na obrázku, kde modré body představují jednotlivé akce a šipky mezi nimi jejich výstupy, události, které ovlivnily koncovou událost, jsou ovlivněny velkým množstvím předchozích unikátních událostí, které nelze předpovídat a tím pádem nelze vyhledat přesné spojení mezi nimi.

Dalším přístupem k safety je Safety III. STAMP (STPA) zapadá právě do přístupu Safety III. Cílem přístupu Safety III je odstranit, zmírnit, nebo kontrolovat nebezpečí, která mohou vést k identifikovaným ztrátám ze strany zúčastněných stran [4].

4 Přístup Safety I. vs Safety II. vs Safety III

STAMP (STPA) zapadá právě do Safety III. Tento přístup definuje safety jako: „Bezpečnost je definována jako oproštění se od nepřijatelných ztrát, které byly definovány zúčastněnými stranami jako nepřijatelné.“ Lineární kauzalita není vůbec uvažována – neexistuje žádný kořen zdroje nebezpečí. V přístupu Safety III se pracuje se všemi součástmi systému, jako je software, hardware, operátoři i vedení. Snahou je navrhnout systém, který si udrží bezpečný stav i pokud se jeho součásti dostanou mimo bezpečné hranice. Nejlepším způsobem k porozumění je porovnání jednotlivých přístupů k safety. [4].

V pozadí jednotlivých přístupů, nebo přechodu od jednoho k druhému přístupu, se samozřejmě skrývají finanční náklady. Je důležité si uvědomit, že každý přístup vidí investice jinak. Jednou věcí je cena přechodu od jednoho k druhému, druhou věcí je vnímání investic, které se v rámci řízení bezpečnosti učiní.

V Safety I jsou investice do zábran viděny jako neproduktivní, negenerující zisk. Pokud je provedena investice a nedojde k žádné nehodě, lze investici vidět jako zbytečnou. Pokud dochází k nehodám a po investici dojde ke zmenšení počtu nehod, je investice považována za opodstatněnou a nutnou. Když nedochází k nehodám a nejsou investovány peníze, jsou tyto peníze viděny jako úspora na systému, pokud dojde k nehodě, prohlásí se za neštěstí nebo špatný úsudek [3].

Investice do systému s přístupem Safety II jsou chápány jako investice do produktivity. Definice Safety II říká, že účelem je, aby se co nejvíce věcí v systému dělo správně, investicí se snažíme podpořit tuto snahu. Pokud v systému nejsou žádné nehody a dojde k investici, může dojít ke zvýšení produktivity a při nehodě budou investice považovány za správné a oprávněné. Při neinvestování zůstává systém bez vývoje a stále stejný. U nehody při neinvestování je nehoda považována za špatný úsudek.

Přístupy Safety I, Safety II a Safety III jsou diametrálně rozdílné. Nelze říct, že přístup Safety I je špatný nebo zastaralý, jedná se pouze o přístup, který nelze aplikovat v dnešních složitých systémech. Dnešní systémy jsou velice úzce propojeny a nelze vždy určit jeden spojující faktor, který vedl k chybné události. Pro lepší přehled rozdílů a pochopení jednotlivých přístupů safety je tabulka 1 [4].

	Safety I.	Safety II.	Safety III.
Definice safety	Co nejméně věcí se nepodaří	Co nejvíce věcí se podaří	Oproštění se od nepřijatelných ztrát, které byly definovány zúčastněnými stranami jako nepřijatelné
Lidský činitel	Je chápán jak zdroj možného nebezpečí	Lidé jsou viděni jako nutná součást systému kvůli své variabilitě	Systém musí být navržen tak, aby umožňoval flexibilitu a odolnost lidí ke zvládnutí nečekaných událostí
Princip safety managementu	Reaktivní, reaguje až po chybné události nebo překročení rizika	Proaktivní, snaha o předvídání vývoje a událostí	Soustředí se na předcházení nebezpečí a ztrát. Učí se z nehod, incidentů a auditů pro lepší pochopení fungování systému
Zjišťování nehod	Všechny nehody jsou způsobeny poruchami, úkolem je zjistit příčinu nehody	Všechny věci v systému se dějí v podstatě stejně. Účelem je přesně porozumět normálnímu (správnému) fungování systému a následné porozumění použít pro vysvětlení, proč se stala chybná událost	Nehody jsou způsobeny nedostatečným řízením během nebezpečí. Celý systém musí být navržen tak, aby zabránil nebezpečí. Cílem vyšetřování je zjistit, proč řídící struktura nepředcházela nebezpečí/ztrátě
Přístup variabilitě	Vidí variabilitu jako škodlivou, mělo by se jí zabránit, pokud je to možné	Variabilita je nevyhnutelná, ale užitečná. Měla by být monitorována a spravována	Systém má být navržen tak, aby byla variabilita bezpečná a konflikty mezi produktivitou, dosahováním cílů a bezpečností byly eliminovány nebo minimalizovány

Tabulka 1: Porovnání Safety I. a Safety II. a Safety III. (Zdroj [4] Upraveno autorem)

5 STAMP

STAMP (System-Theoretic Accident Model and Processes) je v roce 2004 nově vytvořený kvalitativní model pro hledání příčin nehod ve velmi komplexních systémech. Lze ho využít v systémech, které uvažují a zahrnují existenci člověka neboli lidského činitele. STAMP zároveň zahrnuje interakce mezi člověkem, softwarem a hardwarem. Podle Dr. Nancy Levenson, která je autorkou STAMP, je v dnešních komplexních systémech nemožné identifikovat všechny lidské a softwarové chyby. Zároveň je nemožné určit pravděpodobnost chyb, i když jsou všechny chyby známy. Model STAMP byl vytvořen z důvodu velkého vývoje v systémech za posledních několik desítek let. Tradiční modely určování příčin nehod v systémech nejsou schopny vyšetřit nehodu ve velmi komplexních socio-technických systémech, které se dnes využívají [11].

Výhody využití STAMP:

- Zahrnuje všechny součásti systému včetně softwaru, lidí a kultury společnosti. Všechny tyto součásti bere jako potenciální zdroje nehod nebo ztrát bez nutnosti s nimi zacházet odlišně při řešení.
- Umožňuje vytvořit nástroje jako je STPA, CAST (Causal Analysis based on Systems Theory), identifikaci a řízení hlavních indikátorů vedoucích k nebezpečí [14].

Dle modelu STAMP nehody vznikají z důvodu vnějšího narušení systému, selhání komponentů nebo dysfunkčních interakcí mezi komponenty systému, které nejsou následně správně zpracovány řízením systému [12].

STAMP tedy nahlíží na bezpečnost (safety) jako na problémy s řízením a bezpečnost je řízena řídící strukturou vloženou do složitého socio-technického systému. Cílem řídící struktury je prosazovat bezpečnostní omezení (safety constraints) při vývoji, designu nebo provozu systému. Za bezpečnostní omezení lze považovat hranici bezpečnosti systému. Při nehodě je tedy nutné určit, proč došlo k selhání řídící struktury nebo proč byla neúčinná. Při návrhu nebo designu, kdy ještě systém nebyl vytvořen, je předcházení budoucím nehodám podmíněno navržením takové řídící struktury, která bude prosazovat nezbytná bezpečnostní omezení (safety constraints) v systému [12].

Většina konvenčních modelů pro hledání příčin nehod nahlíží na selhání jako na řadu po sobě jdoucích událostí. Velká část takových modelů vychází z předpokladů

převzatých z Dominového modelu, kde jedna chybná událost vede k další a tak dále. Na principu domina jsou založeny analýzy jako je FMEA, FTA nebo ETA. Při šetření je snaha objevit první chybnou událost, od ní pak dále postupovat po řetězu událostí a zabránit jejímu opětovnému výskytu. Tento postup však nebere v potaz důležité součásti moderních systémů jako jsou environmentální, organizační a lidské vlivy na systém. Předchozí zmíněné analýzy nefungují správně v dnešních systémech, protože jsou založeny na myšlence, že všechno je propojeno do řetězce. Velkou nevýhodou těchto systémů je zastavení analýzy v případě nalezení první příčiny vzniku nehody [11].

STAMP má 3 hlavní principy, z nichž první byl definován výše, tedy nezbytná omezení v systému (safety constraints). Druhým je hierarchie řídící struktury, kdy každá úroveň v systému má za úkol prosazovat safety constraints do nižších vrstev v systému. Důležitou součástí hierarchické struktury jsou zpětné vazby, kdy nižší úrovně musí poskytovat zpětnou vazbu vyšším úrovním o tom, jak jsou omezení dodržována. Z toho vyplývá, že vyšší stupně jsou zodpovědné za výkony nižších stupňů prosazování bezpečnostních omezení. Nedostatečné prosazování, chybějící omezení nebo nedostatečná zpětná vazba jsou nečastějšími důvody nedostatečného řízení (inadequte control) [11].

Třetím principem je existence čtyř podmínek, které musí být splněny, aby mohl být proces řízen pomocí STAMP:

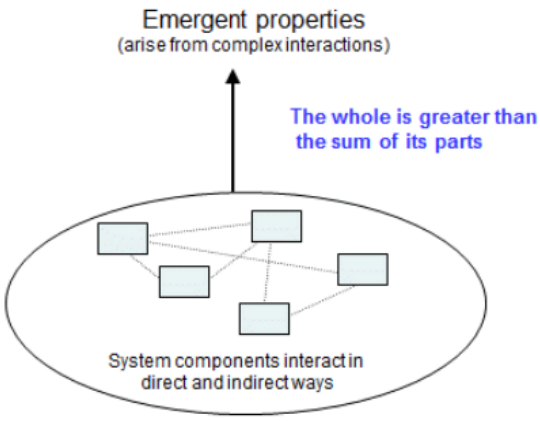
- Existence cíle (goal) – prosazování bezpečnostních omezení v každé úrovni hierarchické struktury
- Podmínka akce (action condition) – implementování řízené akce směrem dolů v hierarchickém systému
- Podmínka pozorování – nutné předávání zpětné vazby od nižších stupňů systému do vyšších
- Podmínka modelu – nutnost vytvoření modelu kontroly řízeného procesu

Součástí STAMP je zároveň teorie systémů (systems theory) a teorie řízení (control theory). Teorie systémů je založena na dvou základních předpokladech (koncept):

1. Emergence a hierarchie
2. Komunikace a kontrola

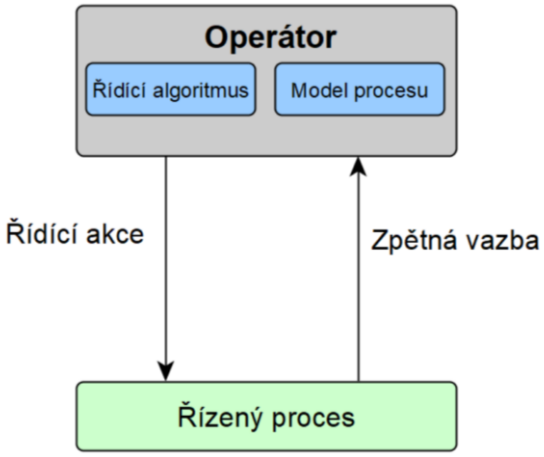
Předpoklad emergence je založen myšlence, že i když se na systém pohlíží jako na celek, a ne jako na jeho jednotlivé části zvlášť, lze model komplexního systému sestavit jako hierarchii řízení, kde je každý stupeň definovaný pomocí svých

emergentních vlastností (emergent properties), které existují pouze v daném stupni díky interakci mezi složkami a neexistují na nižších úrovních. Provozní bezpečnost je emergentní vlastnost a lze ji určit právě pouze v kontextu celku (viz. Obr. 8)



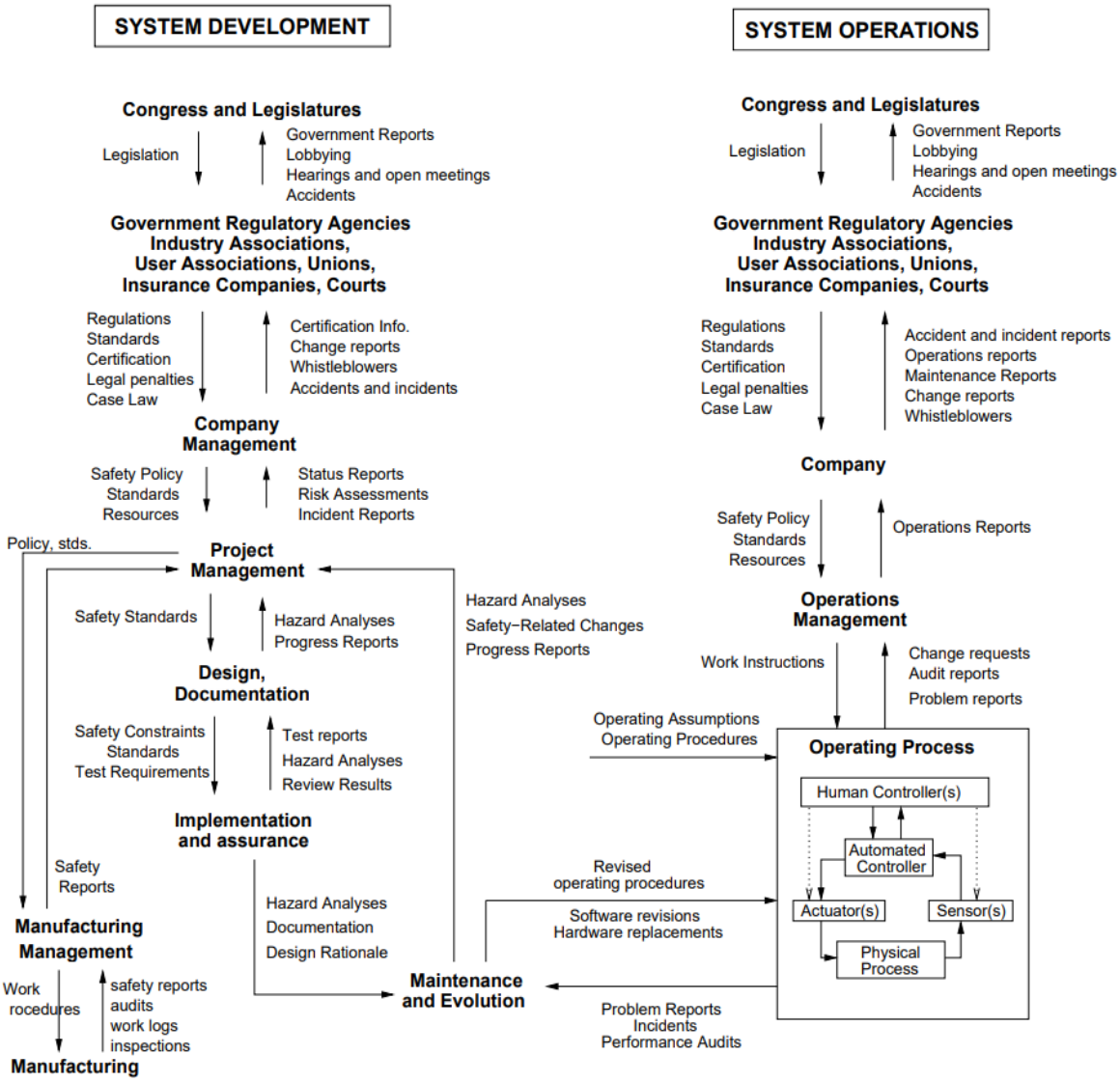
Obrázek 8: Princip emergence [14]

Druhý předpoklad (koncept) vychází z teorie řízení a do STAMP začleňuje pojmy komunikace a řízení. Tento předpoklad úzce souvisí s druhým principem zmíněným výše, tedy principem kontroly v systému pomocí omezení (safety constraints). Na obrázku 9 je znázorněn základní princip řídící struktury.



Obrázek 9: Obecná řídící smyčka Zdroj: [1], upraveno autorem

K nehodám dochází například při selhání součásti systému, vnějším rušení, a / nebo potenciálně nebezpečné interakci mezi komponentami systému, které nejsou adekvátně zpracovány nebo řízeny. Řídící prvky systému mohou být manažerské, organizační nebo provozní. Protože STAMP bere v potaz i okolní prostředí, je nutné si uvědomit, že stupně ovlivňující systém mohou být sledovány až k samotné legislativě nebo tvorbě zákonů ovlivňujících systém [14]. (obr. 10).



Obrázek 10: Oblast zájmu STPA [14].

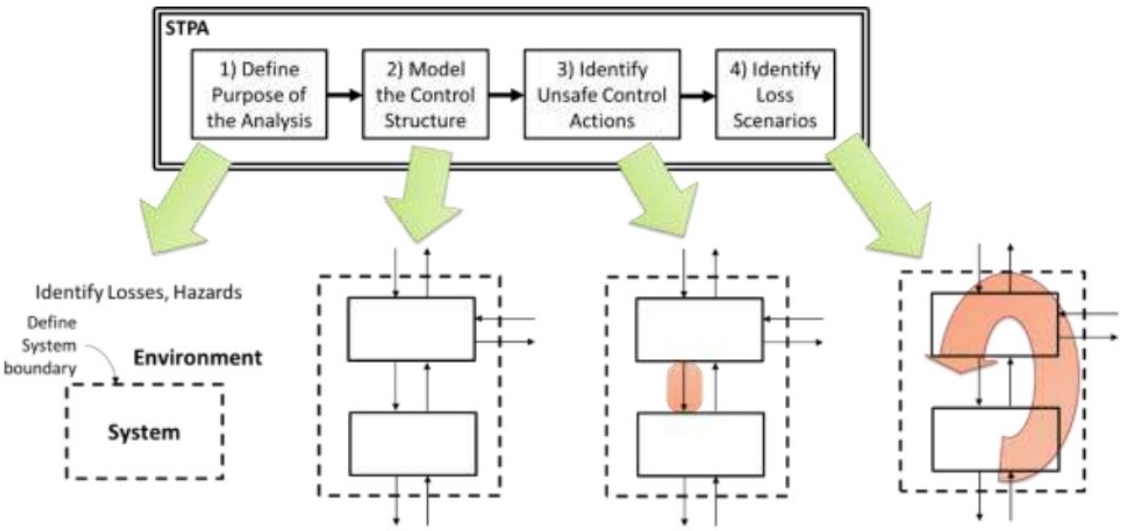
6 STPA

Systems-Theoretic Process Analysis (STPA) je analytická metoda založená na modelu STAMP. Jedná se o systematický přístup k vytvoření modelu systému a jeho následné analýze. Modelem systému je myšleno vytvoření řídící struktury v systému. STPA je schopna identifikovat současné a možné budoucí chyby v řízení systému, tedy v poskytování adekvátní kontroly, nebo prosazovat bezpečnostní omezení (safety constraints) na každém stupni řízení systému. STPA umožňuje analýzu jak při vývoji systému, tak již u zavedené řídící struktury v systému. STPA kromě selhání komponentů předpokládá, že nehody mohou vznikat také nebezpečnými interakcemi mezi jednotlivými komponenty systému, kdy nedošlo k selhání ani jedné z nich [13].
Výhodou STPA analýzy oproti ostatním metodám k identifikaci rizik a nebezpečí v systému je, že [16,17]:

- Dokáže analyzovat velmi složité systémy. STPA dokáže identifikovat neznámé, které by bylo možné identifikovat až při provozu systému, již ve vývojové fázi.
- Lze ji zahájit již v rané fázi koncepčního vývoje, kde následně pomůže identifikovat bezpečnostní požadavky a omezení. Požadavky a omezení mohou být následně použity k návrhu a implementaci dostatečných bezpečnostních požadavků do systému. Nalezení nedostatků ještě před spuštěním systému eliminuje budoucí nákladné přepracování, pokud by byly nedostatky nalezeny po spuštění systému.
- STPA umožňuje zapracovávat podrobnější rozhodnutí o návrhu a tím analýzu vylepšovat.
- Zahrnuje do analýzy software i lidský činitel, to následně zajistí, že analýza obsáhne všechna potenciální rizika.
- STPA poskytuje dokumentaci funkčnosti systému, která se velice často ve velkých systémech těžko hledá nebo chybí její části.
- STPA lze snadno integrovat do procesu systémového inženýrství a do systémového inženýrství založeného na modelech.

STPA má 4 základní kroky k vytvoření a analýze modelu systému [14] (obr.11.):

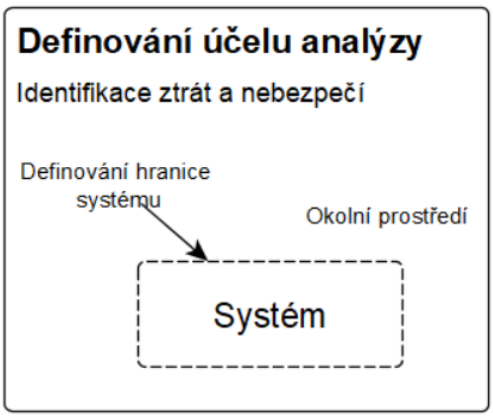
1. Definovat účel analýzy
2. Modelování řídící struktury
3. Identifikace nebezpečných řídících akcí
4. Identifikace možných ztrátových scénářů



Obrázek 11: 4 kroky STPA analýzy. Zdroj: [14].

6.1 Definovat účel analýzy

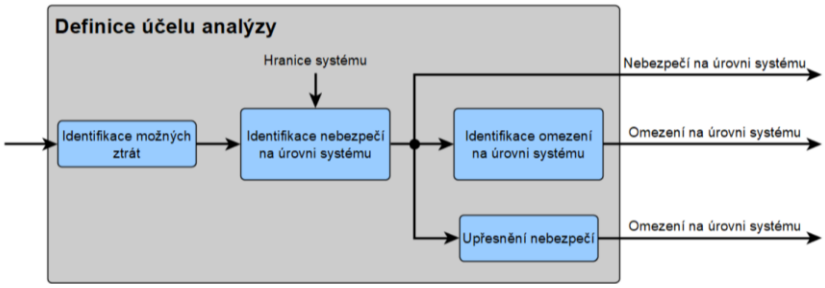
Definování účelu analýzy je prvním a zároveň nejdůležitějším krokem. Při definování účelu je nutné si uvědomit, že veškeré další kroky se budou od tohoto kroku odvíjet (obr. 12). V tomto kroku je nutné si určit, jaké typy nehod (chybných akcí) se budeme snažit eliminovat nebo jim zabránit. Zároveň zda budeme soustředit STPA analýzu pouze na „klasické“ cíle jako u většiny analýz, jako je ztráta života či zranění, nebo se budeme soustředit na bezpečnost (safety + security), soukromí, výkonnost nebo další vlastnosti systému [13].



Obrázek 12: Části definování účelu analýzy (Zdroj: [14] Upraveno autorem)

Definování účelu analýzy má 4 části (obr.13):

1. Identifikace možných ztrát (Identify losses)
2. Identifikace nebezpečí na úrovni systému (Identify system-level hazards)
    a. Stanovení hranice systému
3. Identifikace omezení na úrovni systému (Identify system-level constraints)
4. Identifikace scénářů ztrát



Obrázek 13: Definování účelu analýzy [13], upraveno autorem

6.1.1 Identifikace možných ztrát

Identifikace možných ztrát je první částí tohoto kroku. Za ztrátu je možné považovat vše, co má pro zúčastněné strany nějakou hodnotu. Může zahrnovat lidský život, zranění člověka, poškození majetku, únik informací atd. Základním cílem STPA analýzy je vysvětlení, jak by mohlo dojít ke ztrátám. Před samotným začátkem analýzy je nutné si definovat, na které ztráty se musí analýza zaměřit. [14].

STPA lze použít pro identifikace jakékoliv možné ztráty, která je pro zúčastněné strany nepřijatelná. Za zúčastněné strany lze považovat téměř každého člověka v systému nebo i člověka mimo systém, kterého by se však případná nehoda v systému mohla dotknout. Ztráty budou v celé analýze označovány písmenem L z anglického loss. Příklady ztráty v systému:

- L-1: Úmrtí nebo zranění člověka
- L-2: Poškození budovy letiště

Ztráty, které je nutné vzít v úvahu, mohou být definovány nejen vedením, ale také operátory systému, zákony nebo zákazníky. V příručce pro STPA zmiňuje Levenson několik obecných přístupů k identifikaci ztrát:

- Určit všechny zúčastněné strany v systému (operátory, vedení, zákazníky apod.)
- Každá ze zúčastněných stran stanoví svůj podíl a cíle v systému. Pro bezpečnostní kontrolu například udržení sterility prostoru SRA.
- Převést každý identifikovaný cíl na možnou ztrátu.

6.1.2 Identifikace nebezpečí na úrovních systému

Definice nebezpečí: *nebezpečí je stav systému nebo sada podmínek, které spolu s konkrétní sadou v nejhorších podmínkách prostředí povedou ke ztrátě* [14].

Pro identifikování nebezpečí na úrovních systému je nutné nejdříve analyzovat hranice systému. Jinak řečeno je nutné určit, co je ještě součástí systému a co není. Hranice systému se nejlépe určují pomocí dosahu operátorů systému, tedy hranici systému lze definovat jako části systému, nad kterými má operátor určitou kontrolu, což je také hlavní rozlišovací důvod mezi nebezpečím a ztrátami – ztráty mohou zahrnovat vlivy prostředí, které může operátor jen málo nebo vůbec ovlivnit. Po identifikaci hranic systému je dalším krok definování nebezpečí v úrovních systému nebo podmínek v systému, které povedou ke ztrátě za nejhorších možných podmínek, jež mohou nastat [15,17].

STPA analýza počítá i s tím, že jedno nebezpečí může vést k více ztrátám. Každé nebezpečí může být sledováno k výsledné ztrátě. Výsledné ztráty z konkrétního nebezpečí jsou v STPA analýze zobrazeny v hranatých závorkách za daným nebezpečím [13]. Pro udržení přehlednosti i v dalších částech analýzy bude nebezpečí označováno H (anglicky hazard) a ztráta L (loss). Pro přehlednost uvedu příklad nebezpečí (H) vedoucího k více ztrátám (L).

H-1: Narušení sterility zabezpečeného prostoru SRA [L-1, L-2]

Tedy nebezpečí narušení sterility zabezpečeného prostoru SRA může vést jak k úmrtí nebo zranění člověka, tak k poškození budovy letiště. Díky tomuto kroku je velice jednoduché udržet si přehled během celé analýzy a v případě potřeby ji relativně rychle upravit, pokud by to bylo nutné.

Definovat nebezpečí na úrovni systému nemusí být vždy tak jednoduché, dle Dr. Levenson existují 3 základní kritéria pro definování nebezpečí na úrovni systému [14]:

- Nebezpečí jsou stavy nebo podmínky systému, nikoliv příčiny nebo stavy okolí
- Nebezpečí povede ke ztrátě za nejhorších možných podmínek prostředí
- Nebezpečí musí popisovat podmínky nebo stav, kterému je potřeba zabránit

K těmto třem krokům je nutné dodržet několik bodů ke správnému sestavení STPA analýzy a následného modelu.

K prvnímu bodu je potřeba si uvědomit, že není možné brát v potaz stavy nebo podmínky, které jsou mimo kontrolu návrháře nebo operátora. Zároveň není dobré

se při definici nebezpečí odkazovat na přesné části systému, neboť poté by to mohlo ovlivnit další kroky přílišným soustředěním se na zmíněnou věc v definici nebezpečí.
Druhé kritérium, které stanoví, že nebezpečí povede ke ztrátě za nejhorších možných podmínek, ale ne nutně každé nebezpečí musí vést vždy ke ztrátě, pokud nejsou splněny nejhorší možné podmínky [13]. Pokud bychom využili nebezpečí zmíněné výše (narušení sterility zabezpečeného prostoru), za určitých podmínek nemusí vždy dojít ke ztrátám (L-1, L-2). Za nejhorší možné podmínky v tomto případě můžeme považovat například nepřítomnost bezpečnostních složek na letišti, volný a jednoduchý přístup do letadla atd. Pokud by všechny podmínky nebyly splněny, nemusí nutně dojít ke zmiňovaným ztrátám.
K poslednímu bodu zmiňujícímu, že nebezpečí musí popisovat podmínky nebo stav, kterému je potřeba zabránit, je nutné říct, že za nebezpečí nemůžeme považovat přirozenou a nutnou součást systému [14]. Příkladem z bezpečnostní kontroly může být samotná bezpečnostní kontrola. Provádění bezpečnostní kontroly je stav, který je v systému a může kvůli němu dojít k nebezpečí. Zároveň to však není stav, kterému chceme zabránit, protože provádění bezpečnostní kontroly je samotnou podstatou systému. Jednoduše řečeno nebezpečí musí popisovat takový stav nebo podmínky, do kterých nechceme, aby se systém někdy dostal.

6.1.3 Identifikace omezení na úrovni systému

Definice omezení na úrovni systému: Omezení na úrovni systému specifikuje podmínky nebo chování, které musí být splněny, aby se zabránilo vzniku nebezpečí, tedy ztrátám [14].

Omezení na úrovni systému vychází z předchozího bodu identifikace nebezpečí na úrovni systému, tedy jedná se o omezení, která mají zbránit tomu, aby se systém dostal do nežádoucího stavu nebo podmínky. Omezení na úrovni systému, anglicky systém-level constraint, se v STPA analýze označuje „SC“. Omezení systému lze přiřadit jedno nebo více nebezpečí, kterému má zabránit. Při tvoření omezení systému se jednoduše předělá nebezpečí z předchozí části na podmínku.

Příklad:

H-1: Narušení sterility zabezpečeného prostoru SRA [L-1, L-2]

SC-1: Sterilita zabezpečeného prostoru STA nesmí být narušena. [H-1]

Omezení nemusí nutně definovat pouze jak zabránit nebezpečí, ale také mohou definovat, jak musí systém minimalizovat ztráty v případě nebezpečí [14]. Využiji opět příklad zmíněný výše – dojde-li k narušení sterility zabezpečeného prostoru, musí být toto narušení zjištěno a musí být podniknuty takové kroky, aby došlo k minimalizaci možných ztrát. Zbývající části STPA analýzy slouží k identifikaci všech scénářů, které mohou toto omezení porušit. Identifikací všech scénářů pak vznikají jednotlivá nebezpečí a potenciální ztráty.

6.1.4 Upřesnění nebezpečí

Tento krok STPA analýzy není naprosto nezbytný. Jedná se o krok, kterým je možné upřesnit nebezpečí v systému. Pomocí tohoto kroku dochází k vytvoření podmnožin jednoho nebezpečí na tzv. sub-nebezpečí. Při tomto kroku je nezbytné najít základní systémové procesy nebo činnosti, které je nutné řídit. Pro upřesnění využiji opět výše zmíněné nebezpečí [14].

H-1: Narušení sterility zabezpečeného prostoru SRA

Toto nebezpečí je možné rozložit na jednotlivé části, které se podílejí na sterilitě SRA. Pro udržení SRA například potřebujeme fyzické bariéry a kontrolu. Fyzické bariéry musí sloužit jako obrana proti násilnému nebo náhodnému vniknutí do SRA. Zatímco samotná kontrola před vstupem má sloužit pro udržení sterility i po vpuštění někoho dovnitř, standardně cestujícího nebo zaměstnance.

Fyzické bariéry:

H-1-1: Nedostatečná výška plotu

H-1-2: Možnost náhodného vniknutí do SRA

Kontrola před vstupem do SRA:

H-1.3: Bezpečnostní kontrola nedokáže zajistit sterilitu

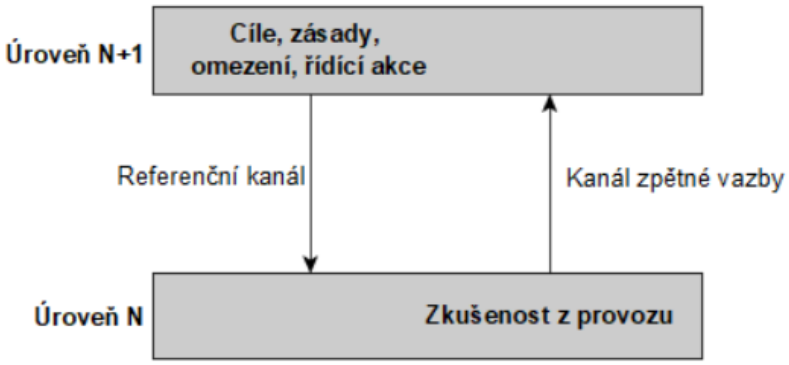
Tento čtvrtý krok STPA analýzy blíže specifikuje jednotlivá potenciální nebezpečí v systému, spolu s vytvořením upřesnění je možné vytvořit upřesnění omezení na úrovni systému (SC). Pro každé sub-nebezpečí je tedy následně možné vytvořit sub-omezení systému.

6.2 Modelace řídící struktury

Druhým krokem STPA analýzy je samotná modelace řídící struktury. Jedná se o hierarchickou strukturu řízení.

Definice:

Hierarchická řídící struktura je systémový model, který se skládá ze zpětnovazebných řídících smyček. Účinná řídící struktura bude prosazovat omezení chování celkového systému [14].

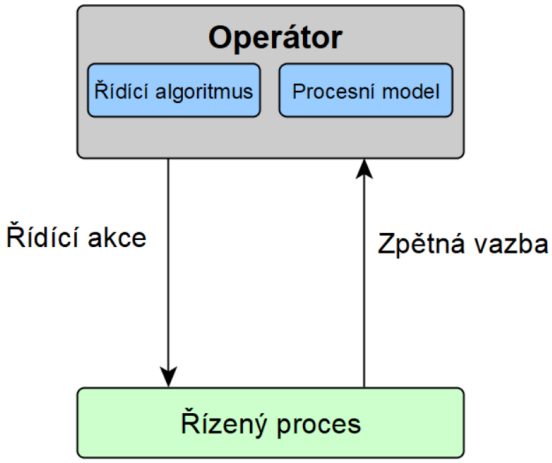


Obrázek 14: Základní model řídící smyčky [15]

Řídící struktura samozřejmě musí probíhat na všech úrovních systému (viz.obr.14.). Jak je možné vidět na modelu výše, probíhají zde 2 typy komunikací: vzestupná a sestupná. Sestupná komunikace slouží k předávání cílů, zásad, omezení a řídících akcí na nižší stupně systému. Vzestupná pak k předávání zpětné vazby na vyšší úrovně systému [15].

V STPA analýze je základní model ukázaný výše předělán a rozšířen o několik částí (viz. Obr 15). Pro vytvoření hierarchické řídící struktury dle STPA musí být v systému definováno alespoň 5 částí této řídící smyčky (viz. Obr 15):

- Operátor
- Řídící akce
- Zpětná vazba
- Ostatní vstupy a výstupy z/do jednotlivých součástí
- Řízený proces
- Procesní model



Obrázek 15: Řídící smyčka STPA analýzy (Zdroj: [14] Upraveno autorem)

V takovém modelu představuje řídící algoritmus rozhodovací procesy operátora, kterými určuje řídící akce, jež mají být poskytnuty. Operátor obsahuje i druhý prvek a tím je procesní model, jenž představuje vnitřní přesvědčení použité při rozhodování. Procesní model může být velice jednoduchý pouze s několika proměnnými, ale může být i velice složitý s velkým množstvím proměnných. Procesní model může být ovlivňován zpětnou vazbou, tedy informacemi získanými v řízeném procesu. Řídící algoritmus představuje například sadu podmínek, kterými se musí operátor řídit. Z toho následně vycházejí řídící akce, tedy akce ke správnému řízení kontrolovaného procesu. Řídící smyčka zobrazená výše může být využita pro jakýkoliv systém, včetně socio-technického systému, ve kterém se objeví největší výzva moderního inženýrství – interakce mezi softwarem a lidmi. Posledním prvkem STPA nemusí být nutně řízený proces. Poslední prvek může být například i člověk [14].

Problémy mohou nastat v jakékoliv části řídící smyčky. Procesní model se například může lišit od skutečnosti, to následně upraví řídící akce operátora a tím mohou vzniknout nebezpečné řídící akce. Stejně tak může vzniknout chyba na zpětné vazbě, kdy informace zpětné vazby nebude správná nebo může zpětná vazba naprosto chybět. Díky STPA je možné identifikovat všechny scénáře, které mohou vést ke ztrátě [15].

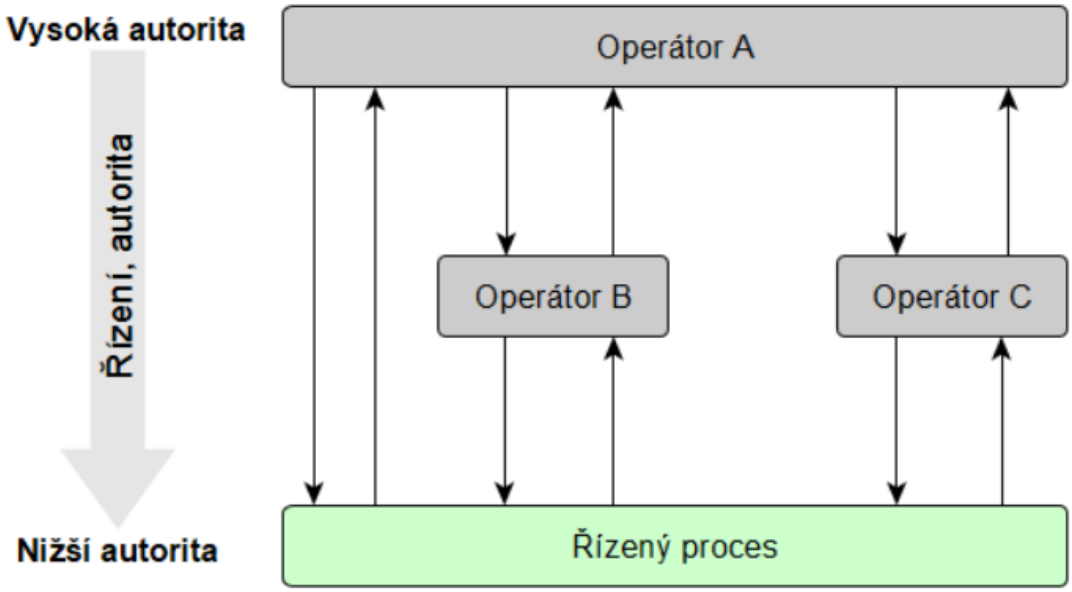
Pro sestrojení samotné řídící smyčky musí být splněny 4 podmínky. Jedná se o logické podmínky, které musí být splněny, abychom mohli vůbec mluvit o kontrolovaném procesu:

- Podmínka cíle – operátor musí mít cíl v systému.
- Podmínka akce – operátor musí být schopen ovlivnit stav / podmínky v systému.

- Podmínka modelu – operátor (člověk nebo stroj) musí mít model řízeného procesu, aby byl schopen ho efektivně kontrolovat. Účelem je určení správných řídících akcí založených na aktuálním stavu řízeného procesu v systému. Zároveň je operátor schopen odhadnout účinek svých řídících akcí na stav systému.
- Podmínka pozorovatelnosti – operátor musí být schopen zjistit stav systému. V případě STPA se jedná o prvek zpětné vazby (feedback) [15].

Ve složitých systémech samozřejmě nebude řídící smyčka tak jednoduchá, jako je na obrázku 15. Ve složitých systémech vznikne velice robustní model složený z mnoha řídících smyček. Tyto smyčky se budou navzájem propojovat a ovlivňovat, zároveň však vznikne hierarchická řídící struktura zmíněna výše. V jakékoliv hierarchické řídící struktuře ale budou platit určitá pravidla.

Vertikální osa řídící struktury určuje kontrolu a autoritu v systému. Vertikální umístění jednotlivých prvků (operátorů, řízeného procesu atd.) pak určuje jejich hierarchii od nejvyšší po nejnižší úroveň. Každý prvek má díky tomu kontrolu a oprávnění nad prvkem bezprostředně pod ním, z čehož vyplývá i opačná logika. Každý prvek je podřízený a podléhá kontrole prvku nad ním. Šipky směrem dolů, tedy řídící akce, pak znázorňují bezpečnostní omezení (constraints) z výše postaveného prvku. Šipky směrem nahoru pak znázorňují zpětnou vazbu v systému. V STAMP jsou podmínkou bezpečnostní omezení, která musí každý kontrolor prosazovat v hierarchické struktuře řízení bezpečnosti (viz obr.16.). Díky těmto nastaveným pravidlům předávání informací v řídící struktuře je pak mnohem jednodušší rozpoznat i předem nezpozorované chyby nebo nedostatky. Příkladem může být i samotná neexistence zpětné vazby, tedy operátor (řídící prvek) vydává své řídící akce na základě nedostatečných informací z ním řízených prvků nebo naopak, zpětná vazba je podávána dostatečně, ale je podávána prvkům, které nejsou schopny nijak ovlivnit proces pod nimi.



Obrázek 16: Složitější řídící model. (Zdroj: [1] Upraveno autorem)

Při modelování řídící struktury je nutné si uvědomit, že struktura STPA není fyzický model, ale pouze funkční model. Dále je nutné vědět, že řídící struktura není simulační model, spíše je tomu naopak. Řídící struktura STPA zahrnuje prvky, které nelze simulovat (lidi). STPA má spíše sloužit jako nástroj k nalezení všech nezbytných omezení ke správné kontrole systému. STPA však může sloužit také jako zdroj pro následnou simulaci, protože poskytuje všechny detaily o systému [14].

Řídící struktura sice obsahuje prvky řízení a zpětné vazby, ale to nutně neznamená, že každá řídící akce poslaná směrem k nižšímu prvku bude vykonána. Stejně tomu je pro zpětnou vazbu, kdy ne každá zpětná vazba má v praxi vliv na operátorovo řízení. V STPA analýze jsou řídící akce a zpětné vazby považovány spíše za tok informací, v praxi je hlavním cílem STPA analyzovat strukturu řízení a snaha o předvídání chování každého prvku a jak toto chování může být nebezpečné [14].

Během vytváření řídící struktury je možné každému řídícímu prvku (operátorovi) přiřadit odpovědnost (responsibility). Řídící akce mohou být definovány na základě těchto odpovědností. Dalším krokem při modelování řídící struktury je určení zpětných vazeb v systému pro úpravu řízení operátora [14].

6.3 Identifikace nebezpečných řídících akcí

Definice nebezpečné akce: *Nebezpečná řídící akce (Un-safe Control Action = UCA) je řídící akce, která v konkrétním kontextu a nejhorším prostředí povede k nebezpečí* [14].

Existují 4 důvody, kvůli kterým může být řídící akce považována za nebezpečnou [13]:

- Neposkytnutí řídící akce vede k nebezpečí
- Poskytnutí chybné řídící akce vede ke vzniku nebezpečí
- Poskytnutí potenciálně bezpečné řídící akce příliš brzy, pozdě nebo ve špatném pořadí
- Řídící akce trvá příliš dlouho nebo je zastavena příliš brzy (pouze pro v čase spojité řídící akce)

Při tvorbě STPA pak vzniká tabulka jednotlivých řídících akcí v systému, kde ve sloupci je vždy uveden jeden z důvodů vzniku nebezpečné řídící akce. V tabulce pak vznikají jednotlivé nebezpečné řídící akce vztažené k jedné řídící akci.

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon / Applied Too Long

Obrázek 17: Ukázka tabulky identifikace nebezpečných řídících akcí [13].

Každá nebezpečná řídící akce (UCA) musí specifikovat, během jakých podmínek je řídící akce nebezpečná. Poté je možné tyto podmínky v systému najít a odstranit nebo je alespoň zmírnit. UCA mohou být vztaženy k okolním podmínkám, řízenému procesu, stavu operátora atd. Při sestavování UCA může být velice užitečné využívat slova jako „během“, „když“ apod. [15]. Všechny výše zmíněné body k identifikaci nebezpečných řídících akcí lze využít nejen pro automatizované operátory, ale zároveň pro lidského operátora.

Součástí identifikace nebezpečných řídících akcí je nalezení omezení řídícího prvku (controler constraints – „C“). Omezení řídícího prvku vychází z identifikovaných nebezpečných řídících akcí. Pro každou identifikovanou nebezpečnou akci je potřeba stanovit omezení řídícího prvku, tedy pro každou UCA je potřeba stanovit C.

Příklad:

UCA-1: Neposkytnutí letového plánu

C: Letový plán musí být poskytnutý.

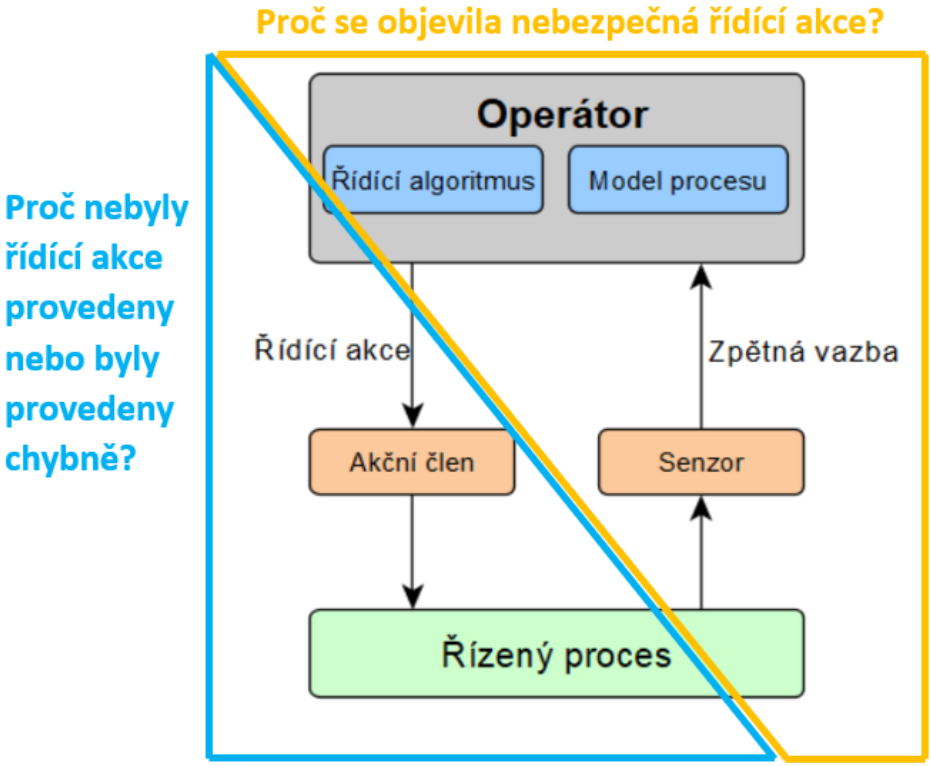
Nalezení všech omezení každého řídícího prvku zároveň může posloužit k nalezení chybějících nebo nedostatečných omezení na řídící prvek. Tyto nedostatky poté poslouží k další části analýzy, kde dojde k identifikaci scénářů ztrát.

6.4 Identifikace scénářů ztrát

Definice: Scénáře ztrát popisují kauzální faktory, které mohou vést k nebezpečné řídící akci nebo nebezpečí [14].

Existují 2 otázky při hledání scénářů (Obr.19)

1. Proč se objevila nebezpečná řídící akce?
2. Proč nebyly řídící akce provedeny nebo byly provedeny chybně?



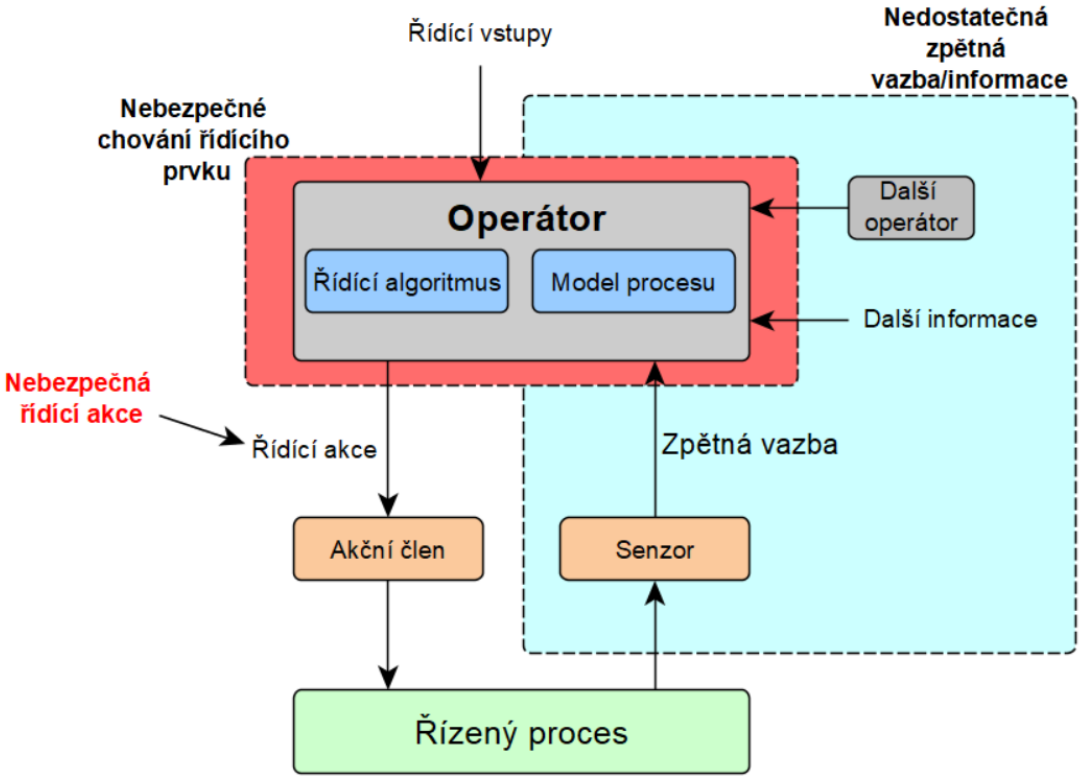
Obrázek 18: Rozšíření řídící smyčky. (Zdroj: [14] Upraveno autorem)

Obrázek 19 ukazuje rozšířenou řídící smyčku. Řídící smyčka byla rozšířena o akční člen a senzor. Do této části byly v řídící smyčce identifikovány řídící akce a zpětné vazby, avšak nebylo uvažováno, jak jsou řídící akce a zpětné vazby předávány. Řídící akce jsou předávány za pomocí akčního členu. Zpětná vazba je předávána pomocí senzorů [14].

6.4.1 Identifikace scénářů, které vedly k nebezpečné řídící akci

Při tomto hledání scénářů vezmeme v potaz danou UCA a postupujeme odzadu takovým způsobem, abychom nalezli důvod, proč řídící prvek předal nebezpečnou řídící akci dalším prvkům. Předání nebezpečné akce se může stát z mnoha důvodů, například fyzickou poruchou řídícího prvku, postupnou degradací řídícího algoritmu, přijetím nebezpečné řídící akce od vyššího prvku, nedostatečným procesním modelem samotného prvku (obr.18). Nebezpečné řídící akce mohou vznikat ze dvou důvodů [14]:

1) Nebezpečným chováním řídícího prvku
2) Nedostatečnou zpětnou vazbou a informací



Obrázek 19: Nebezpečné řídící akce mohou vznikat nebezpečným chováním řídícího prvku nebo nedostatečnou zpětnou vazbou a dalšími vlivy (Zdroj: [14] Upraveno autorem)

1) Nebezpečné chování řídícího prvku

Dr. Leveson udává 4 důvody, proč řídící prvek může vydat nebezpečnou řídící akci:

- Porucha samotného řídícího prvku
- Nedostatečný řídící algoritmus
- Přijetí nebezpečné řídící akce od jiného prvku

- Nedostatečný procesní model řídícího prvku

Nedostatečný řídící algoritmus udává, jak jsou řídícími prvky vybrány řídící akce založené na procesním modelu a jeho předchozích vstupech (obr.19). V našem modelu níže (obr. 20) jsou všechny řídící prvky lidé, řídící algoritmus tedy můžeme definovat jako rozhodovací proces. Rozhodovací proces může záviset na předchozích zkušenostech, tréninku a postupech.

UCA-2: Plánovač nepředá požadavek na maximální měsíční fond pracovníka BEK.

Scénář 1 pro UCA-2: Plánovač směn nepředá požadavek na maximální FPD, protože postupy pro plánovače tento krok neudávají. Nepředáním požadavků dojde k chybám při plánování pracovníků BEK.

Obecně lze říct, že chyby v řídícím algoritmu mohou pocházet z:

- Chybné implementace daného řídícího algoritmu
- Řídící algoritmus je chybný
- Řídící algoritmus se postupem času stane nedostatečným kvůli změnám nebo degradaci

Přijetím nebezpečné řídící akce může zkoumaný řídící prvek vydat následnou nebezpečnou řídící akci. Zkoumaný řídící prvek předpokládá, že řídící akce do něho vstupující byla správná a svou řídící akci tedy založí na chybě. Tento typ chybné řídící akce je především způsoben nedostatečnou nebo chybějící zpětnou vazbou.

Posledním důvodem vydání nebezpečné řídící akce je nedostatečný procesní model. Procesní model lze u člověka definovat jako jeho vnitřní přesvědčení / informace, které pak následně určují jeho řídící algoritmus. Chyby v modelu procesu se mohou vyskytnout z těchto důvodů:

- Řídící prvek dostane špatnou zpětnou vazbu / informaci
- Řídící prvek dostane správnou zpětnou vazbu / informaci, ale špatně si ji interpretuje nebo ji opomene
- Řídící prvek nedostane zpětnou vazbu / informaci, když ji potřebuje
- Nutná zpětná vazba / informace neexistuje

Všechny výše zmíněné problémy mohou vzniknout z mnoha důvodů. Při příjmu špatné zpětné vazby / informace může v řídícím prvku dojít ke konfliktu informací nebo konfliktu, který bude chybně vyřešen. Opomenutí zpětné vazby (informace) může nastat, pokud je řídící prvek zaměstnán jiným procesem nebo nemá možnost pomocí svého procesního modelu takovou situaci vyřešit. Neobdržení zpětné vazby může být

způsobeno, když procesní model prvku není pravidelně upravován vzhledem k systému. Pro náš systém by to bylo například zavedení nového systému úpravy směn pro pracovníky BEK, ale řídící prvek (operátor) v systému o tom nebyl informován. Zpoždění zpětné vazby je problematické především v dynamickém systému, kde dochází k vývoji. Pozdní obdržení zpětné vazby pak může mít za následek chybu v procesním modelu (řídící akci). Podobně tomu je u neexistence zpětné vazby, kde řídící prvek jednoduše neobdrží zpětnou vazbu na svou řídící akci a tím pádem nemůže upravit svůj procesní model (řídící algoritmus) vzhledem k situaci v systému [14].

2) Nedostatečná zpětná vazba a informace

Pokud v předchozím kroku STPA analýzy identifikujeme zpětnou vazbu nebo právě její neexistenci, která může vést k UCA, je potřeba zjistit, od jakého prvku tato vazba přichází a co mohlo způsobit tuto chybu ve zpětné vazbě [14].

7 STPA v procesech bezpečnostní kontroly

STPA analýza bude v tomto případě použita pro proces zabezpečení dostatečného počtu pracovníků BEK pro zajištění provozu. Se zajištěním provozu zároveň souvisí úroveň bezpečnosti, která je primárním úkolem a důvodem existence bezpečnostní kontroly samotné. Použití STPA je založeno na historických událostech, vnitřní znalosti celého systému a rozhovorech s jednotlivými účastníky v systému. Analýza bude postupovat přesně podle výše uvedených a popsaných kroků. Bude se zabývat pokrytím provozních potřeb na bezpečnostní kontrole, avšak nebude brát v potaz spokojenost pracovníků nebo cestujících. Budou podrobně popsány všechny vazby mezi jednotlivými prvky v modelu.

7.1 Definice účelu analýzy

Důvodem vzniku STPA analýzy v procesech bezpečnostní kontroly je ověření správnosti nastavených procesů pro zabezpečení dostatečného množství pracovníků pro provoz BEK.

7.1.1 Identifikace možných ztrát

Prvním krokem je identifikace možných ztrát (losses). Za ztrátu je možné považovat vše, co má pro zúčastněné strany nějakou hodnotu. Může zahrnovat lidský život, zranění člověka, poškození majetku, únik informací apod. Pro tuto STPA analýzu byly nalezeny 4 možné ztráty, které v systému hrozí [14].

- L-1: Finanční náklady
- L-2: Poškození nebo zničení majetku letiště
- L-3: Ztráta života, zranění
- L-4: Ztráta reputace

7.1.2 Identifikace nebezpečí na úrovních systému

Druhým krokem je identifikace nebezpečí na úrovni systému, kde dojde k nalezení možných nebezpečí a jejich následné spojení s možnými ztrátami z předchozího kroku. V tomto kroku došlo k nalezení 5 možných nebezpečí:

H-1: Bezpečnostní kontrola nepokryje provoz [L-1, L-2, L-4]

H-2: Bezpečnostní kontrola nezaručí dostatek pracovníků BEK [L-1, L-2, L-3, L-4]

H-3: Nedodržení pravidel pro plánování [L-1, L-4]

H-4: Při plánování dojde k překročení FPD (Fond pracovní doby) [L-1]

H-5: Nedostatečná bezpečnostní kontrola [L-1, L-2, L-3, L-4]

Hazard 1 – Za nepokrytí provozu lze považovat například neobsazení stanoviště bezpečnostní kontroly, zpoždění letadla nebo neobsazení požadovaných pozic v případě nouzové situace.

Hazard 2 – Nedostatek pracovníků znamená, že dispečer DEP má k dispozici menší počet pracovníků BEK, než je požadovaný počet na daný den.

Hazard 3 – Nedodržení pravidel plánování. Plánování směn je limitováno velkým množstvím pravidel, která jsou nastavena tak, aby byl vždy dodržen zákoník práce a kolektivní smlouva. Mezi tato pravidla lze zařadit maximální počet vložených směn, počet nočních směn jdoucích za sebou atd.

Hazard 4: Při plánování dojde k překročení FPD (Fond pracovní doby) [L-1]

Při plánování směn hrozí překročení fondu pracovní doby u jednotlivých pracovníků. Fond pracovní doby je maximální počet hodin, které může pracovník odpracovat během určitého období (měsíc/rok).

Hazard 5 – Nedostatečná bezpečnostní kontrola. Za nedostatečnou bezpečnostní kontrolu lze považovat neplnění legislativních požadavků, vpuštění nebezpečného předmětu na SRA, narušení security atd.

7.1.3 Identifikace omezení na úrovni systému v procesech bezpečnostní kontroly

Omezení na úrovni systému musí být nastavena takovým způsobem, aby předcházela výše definovaným nebezpečím. Pro přehlednost v tomto kroku využiji formátu nastaveném v STPA Handbook od prof.Levenson.

<System level-constraint > = <System> & <Condition to Enforce > & <Link to Hazards>

H-1: Bezpečnostní kontrola nepokryje provoz [L-1, L-2, L-4]

SC-1: Bezpečnostní kontrola musí zaručit pokrytí provozu [L-1, L-2, L-4]

H-2: Bezpečnostní kontrola nezaručí dostatek pracovníků BEK [L-1, L-2, L-3, L-4]

SC-2: Bezpečnostní kontrola musí zaručit dostatečné množství pracovníků BEK [L-1, L-2, L-3, L-4]

H-3: Nedodržení pravidel pro plánování

SC-3: Pravidla plánování musí být vždy dodržena [L-2, L-4]

H-4: Při plánování dojde k překročení FPD (Fond pracovní doby)

SC-4: Při plánování nesmí dojít k překročení fondu pracovní doby [L-1]

H-5: Nedostatečná bezpečnostní kontrola

SC-5: Bezpečnostní kontrola musí být prováděna dostatečně [L-1, L-2, L-3, L-4].

7.2 Modelace řídící struktury v procesech bezpečnostní kontroly

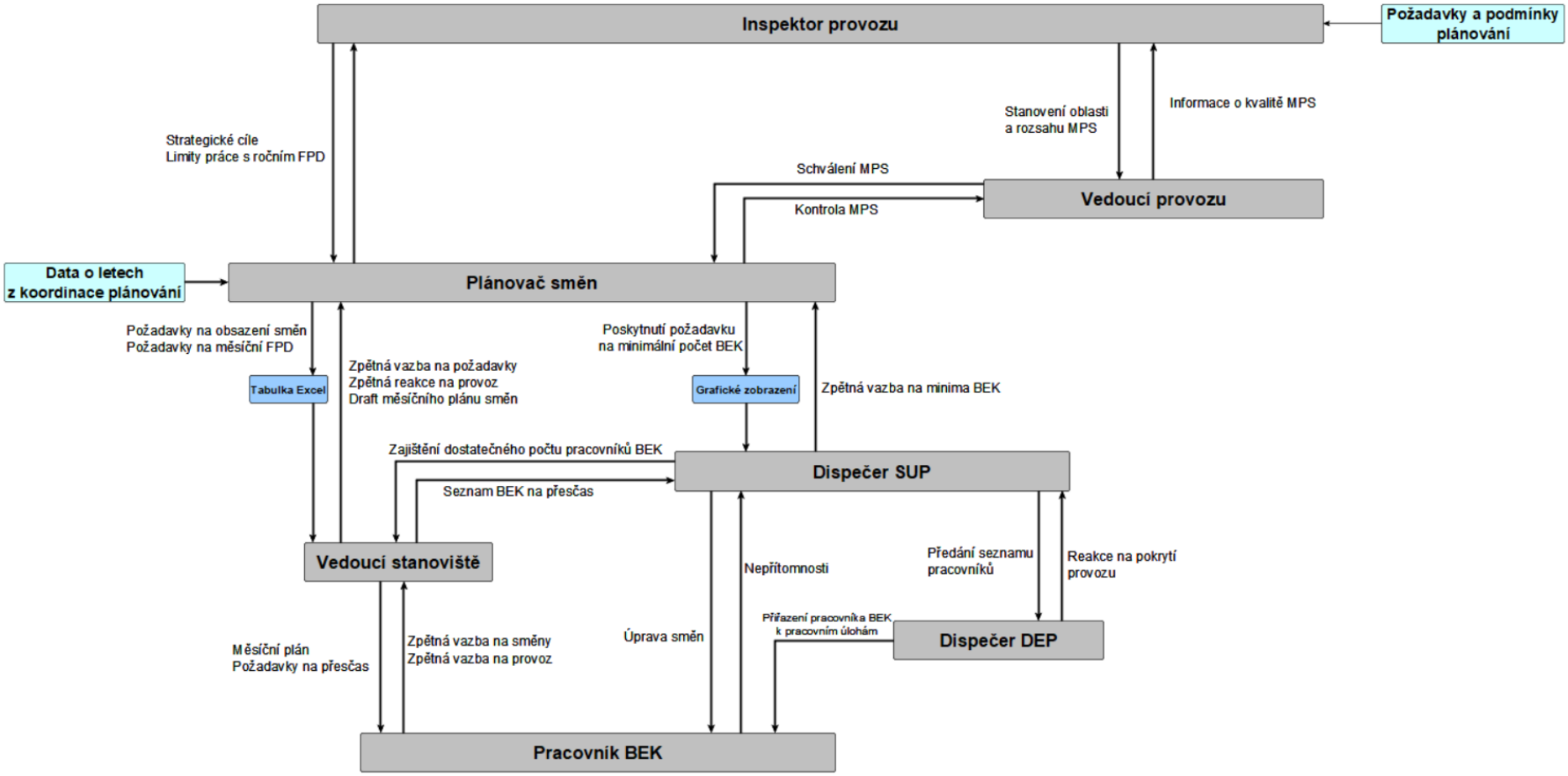
Při modelaci řídící struktury byl využit reálný příklad struktury bezpečnostní kontroly na Letišti Praha. Nejedná se o kompletní řídící strukturu, ale pouze o strukturu řízení, která ovlivňuje řešený proces – zabezpečení dostatečného počtu pracovníků BEK. Kompletní řídící struktura organizační jednotky BEK v tomto případě není potřebná. Ostatní prvky v organizační jednotce BEK nemají žádný vliv na pokrytí provozu pracovníky BEK. Při vytváření modelu bylo využito 8 řídících prvků (controler), které jsou vzájemně propojeny v hierarchické struktuře (obr. 21).

- Inspektor provozu
- Koordinace plánování letů
- Plánovač směn
- Vedoucí provozu
- Vedoucí stanoviště
- Dispečer SUP
- Dispečer DEP
- Pracovník BEK

Těchto 8 řídících prvků dohromady řídí proces zabezpečení dostatečného množství pracovníků BEK. Každý z řídících prvků má v hierarchické struktuře určitou odpovědnost podle vnitřních pravidel společnosti, autoritu nad prvky pod ním a zodpovídá se prvkům nad ním. Tyto 3 aspekty jsou uvedeny pod řídící strukturou pro lepší pochopení fungování celého systému spolu s popisem každého řídícího prvku.

Na obrázku 20 je vytvořena řídící struktura plánování směn k zabezpečení dostatečného počtu pracovníků BEK na pokrytí provozu. Směny jednotlivých pracovníků jsou naplánovány v měsíčním plánu směn (MPS).

:



Obrázek 20: Řídící struktura. (vytvořeno autorem)

7.2.1 Popis jednotlivých řídících prvků v řídící struktuře

Inspektor provozu

Inspektor provozu má nejvyšší pozici v řídící struktuře, tím pádem je přímo i nepřímo odpovědný za všechny řídící akce provedené v celém systému. Jedná se o řídící prvek, který udává základní pravidla pro zabezpečení procesu. Odpovídá za správných chod celého procesu bezpečnostní kontroly.

Plánovač směn

Pozice plánovače směn je klíčová pro celý proces. Plánovač směn udává požadavky na počty pracovníků BEK na celý následující měsíc. Plánování směn na následující měsíc probíhá vždy do 15. dne předchozího měsíce. Měsíční plán je tedy vydán vždy 15 dní před začátkem plánovaného měsíce. Důležitou součástí práce plánovače směn jsou zkušenosti a znalosti provozu. Musí být schopen spojit dohromady všechny informace (zpětné vazby), které dostává od ostatních prvků a na základě toho vytvořit co nejpřesnější předpoklad potřebného počtu BEK pro zabezpečení provozu a udržení bezpečnosti. Zároveň je zodpovědný za zpracování celého měsíčního plánu směn. Ten vzniká spojením naplánovaných směn jednotlivých posádek, které jsou plánovány přes vedoucího směny.

U plánovače směn je důležité zmínit fond pracovní doby (FPD) a jeho nastavování v průběhu roku. Roční práce s FPD patří mezi nejdůležitější aspekty při práci plánovače. Jedná se o informaci, jakým způsobem pracovat s fondem hodin pracovníka BEK. Každý pracovník BEK může dle zákoníku práce a kolektivní smlouvy odpracovat pouze určitý počet hodin za rok, konkrétně se jedná o 1955 hodin ročně. Fond pracovní doby je velice důležitým aspektem při plánování směn, především pro silně sezónní letiště, jakým je Letiště Václava Havla. Letiště má největší množství cestujících v době od května do září. V této době je potřeba více pracovníků BEK než mimo sezónu (viz. graf 1) [5].

Graf 1: Zobrazení průběhu počtu cestujících během roku [5].

Práce s fondem právě toto umožňuje. Samozřejmě nelze měnit počet pracovníků BEK v závislosti na sezóně, protože trénink a všechna školení pro vycvičení samostatného pracovníka jsou velice nákladná a zároveň trvají minimálně 2 měsíce. Tím pádem jediným řešením na pokrytí provozu s konstantním počtem pracovníků je správná práce s FPD.

Z grafu vyplývá, že pokud by pracovníci během celého roku chodili do práce ve stejném počtu, docházelo by k velkým ztrátám, nadbytku pracovníků mimo sezónu, a naopak k nedostatku pracovníků v sezóně. Řešením tohoto problému, je snaha o čerpání FPD takovým způsobem, aby co nejvíce odpovídal křivce cestujících v průběhu roku a toho je dosahováno za pomoci vypuštěných směn mimo hlavní měsíce. Vypuštěním směn dochází k šetření ročního FPD každého pracovníka a tyto ušetřené hodiny jsou poté využity ve formě vložených směn v měsících s velkým počtem cestujících. Rozvaha a čerpání ročního FPD během roku patří mezi nejdůležitější a nejsložitější práci plánovače směn. Počty PAX v průběhu roku neovlivňují pouze počet hodin pro každého pracovníka, ale zároveň typy směn, které jsou využívány. Mimo hlavní sezónu se využívá menšího množství směn, zatímco v sezóně se využívá většího množství typu směn vzhledem k většímu počtu letadel a jejich rozložení skrz den.

Zde je důležité zmínit, že celá práce, kterou plánovač směn vykonává, je silně závislá na datech o letech. Data o letech poskytuje koordinace plánování letů a v modelu jsou naznačeny jako externí vstup do plánovače směn. Bez těchto dat by veškerá práce byla pouhým odhadováním budoucího provozu.

Vedoucí provozu

Vedoucí provozu zastává v systému především funkci kontroly a zpětné vazby. V reálném systému je klíčovým prvkem pro spojení back-office a pracovníků provozu. Vedoucí provozu řeší s pracovníky BEK jejich různé náměty, problémy apod. Získává zpětnou vazbu od pracovníků BEK na měsíční plán směn a jednotlivé směny. Zároveň slouží jako poslední kontrola měsíčního plánu směn, u kterého má právě vedoucí schvalovací funkci. Vedoucí provozu musí schválit každý měsíční plán před vydáním.

Vedoucí stanoviště

Dalším velice důležitým řídícím prvkem je vedoucí stanoviště, který je v každodenním přímém kontaktu s pracovníky BEK. Vzhledem k pokrytí provozu je vedoucí stanoviště prvkem, který plánuje směny jednotlivým pracovníkům, a neboť plánování provádí právě tato pozice, mohou být už předem eliminovány některé problémy, které by mohly později vznikat. Každodenní kontakt s pracovníky BEK umožňuje vedoucímu stanoviště plánovat směny tak, aby co nejvíce odpovídaly požadavkům jeho posádky. Každý vedoucí plánuje směny pouze pro určité množství pracovníků.

Dispečer SUP

Dispečer SUP je řídící prvek zaručující především každodenní řízení provozu. Dispečer zabezpečuje pokrytí pracovníky BEK vždy pro následujících 5 dní. Práce dispečera spočívá v kontrole naplánovaných směn na daný den, eventuálně úpravu směn takovým způsobem, aby pokrývaly požadavky na potřebné počty BEK, které stanoví plánovač směn. Potřebné počty si lze představit jako křivku, která v čase stanovuje nutný počet pracovníků BEK v závislosti na letovém plánu a naplánovaných směnách. Dispečer SUP musí v závislosti na této křivce zajistit pracovníky BEK. Křivka (minima BEK) je v řídící struktuře pojmenována jako poskytnutí minimálních požadavků počtu BEK.

Dispečer DEP

Dispečer DEP je pozice zajišťující odlety (departures). Jedná se o pozici, která přiřazuje jednotlivým pracovníkům BEK jejich přesné pracovní pozice. Tato pozice řídí pracovníky BEK po celém letišti takovým způsobem, aby došlo k pokrytí celého

provozu. K řízení pracovníků si vytváří svůj rozpis pracovních pozic jednotlivých pracovníků pro daný den tak, aby je byl schopen efektivně řídit. Při přípravě tohoto rozpisu zároveň ověřuje dostatek pracovníků pro daný den. Je v přímém a neustálém spojením s dispečerem SUP. Podrobněji jejich vzájemnou vazbu popíšu v následující části.

Pracovník BEK

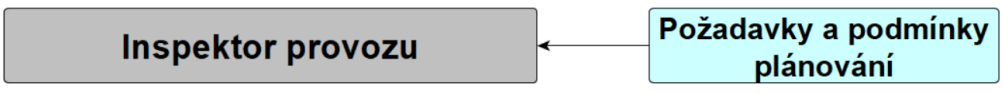
Pracovník BEK je prvkem zabezpečujícím samotné pokrytí provozu dle požadavků stanovených řídícími prvky nad ním. Úlohou pracovníka je samotná bezpečnostní kontrola cestujících a jejich zavazadel před nástupem do letadla. Bezpečnostní kontrola musí být provedena v souladu s nastavenými postupy a pravidly. Pracovník BEK pracuje na pozicích, které jsou určeny dispečerem DEP.

7.2.2 Popis řídících akcí a zpětných vazeb

V této části popíšu jednotlivé řídící akce a zpětné vazby mezi jednotlivými řídícími prvky v modelu. V modelu jsou naznačeny řídící akce a zpětné vazby, ale nelze do něj přesně popsat, co jaká řídící akce (zpětná vazba) znamená.

Požadavky a podmínky plánování – Inspektor provozu

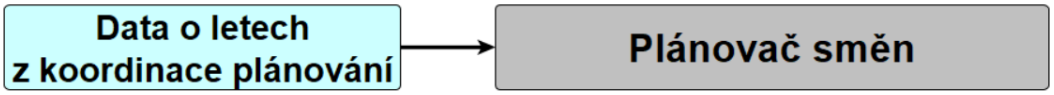
Z modelu je patrné, že vstupem do inspektora provozu jsou „požadavky a podmínky plánování“. Jedná se o externí vstup. Tento vstup nelze označit za řídící prvek, vstup označuje spíše zákonné a další podmínky pro celý proces. Mezi tyto požadavky a podmínky můžeme například zařadit zákoník práce, který přesně stanovuje pravidla ohledně limitů počtu odpracovaných hodin, nutných přestávek atd. Tyto podmínky jsou pak dále přenášeny jako součást řídících akcí vycházejících z inspektora provozu (obr.22).



Obrázek 21: Spojení inspektora provozu s požadavky

Data o letech z koordinace plánování – Plánovač směn

Tento prvek má stejnou funkci jako požadavky a podmínky plánování u inspektora provozu. Data o letech od koordinace plánování jsou spolu s podmínkami pro plánování naprosto nezbytná pro práci plánovače směn. Pod pojmem data o letech si lze představit letový plán, avšak upravený vzhledem k potřebám bezpečnostní kontroly (obr. 23).

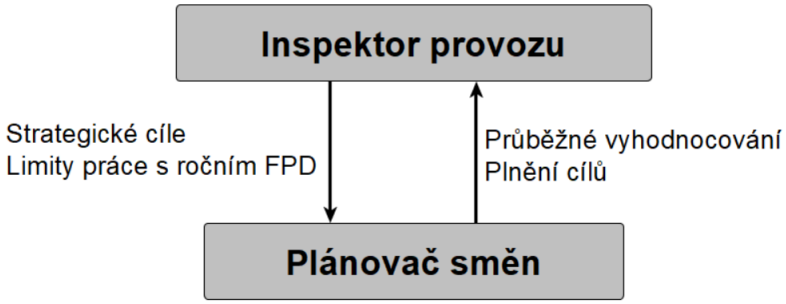


Obrázek 22: Vazba Koordinace plánování – Plánovač směn.

Informacemi, které potřebuje znát plánovač směn z této vazby, jsou, zda let směřuje do států schengenského prostoru či nikoliv. Stejně důležitým údajem jsou časy odletů jednotlivých letadel, dále pak plánované stojánky, destinace, typ letadla, respektive předpokládaný počet cestujících na daném letu. Všechny tyto informace jsou velmi podstatné pro procesní model plánovače směn. Například informace o destinaci se nemusí zdát příliš zásadní, ale je to právě naopak. Příkladem mohou být lety do Ameriky, kdy americké společnosti vyžadují nadstandardní postupy při bezpečnostní kontrole. Let do Ameriky je pak přibližně 5x náročnější na počet BEK hodin než standardní odlet. Data o letech poskytuje koordinace plánování letů. Bez těchto dat by veškerá práce byla pouhým odhadováním budoucího provozu.

Inspektor provozu – Plánovač směn

Vzájemná komunikace mezi těmito řídícími prvky je základem pro správné a efektivní pokrytí provozu. Inspektor provozu je od začátku ovlivněn požadavky a podmínkami pro plánování (zákoník práce, kolektivní smlouva atd.). Tyto požadavky poté předává dále do celého systému v rámci řídících akcí jednotlivých prvků.



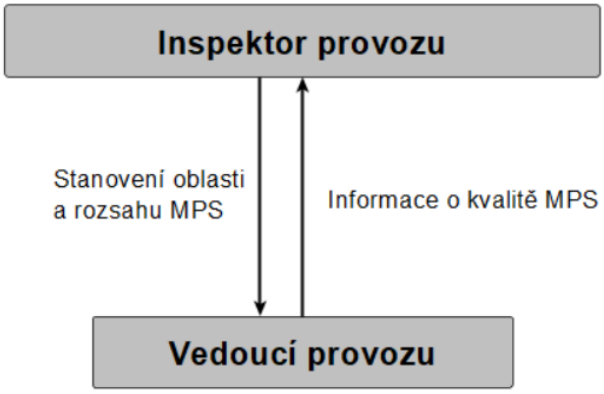
Obrázek 23: Vazba Inspektor provozu - Plánovač směn (vytvořeno autorem)

Jak je možné vidět na obrázku 23, inspektor provozu má dvě řídící akce směrem k plánovači směn, který je v tomto vztahu podřízen. Jedná se o předávání strategických cílů a limitů práce s ročním fondem pracovní doby tzv. FPD. Za strategické cíle můžeme považovat celkové směřování bezpečnostní kontroly samotné. Zároveň lze za strategické cíle označit školení, jež musí každý absolvovat. Druhou řídící akcí je práce s ročním FPD. Tato řídící akce je první akcí ovlivňující vnitřní proces plánovače směn.

Od plánovače k inspektorovi zde směřují dvě zpětné vazby. První z nich je průběžné vyhodnocení, za které lze považovat vyhodnocení práce s FPD. Jedná o informace o tom, jakým způsobem je reálně nakládáno s FPD. Druhou zpětnou vazbou je předání informací o plnění stanovených cílů.

Inspektor provozu – vedoucí provozu

Vazba mezi těmito řídícími prvky je především zaměřena na měsíční plán směn (MPS). Inspektor provozu na základě požadavků a podmínek stanovuje pravidla pro plánování a vydání měsíčního plánu směn. Vedoucí provozu zaručuje, že měsíční plán směn bude mít správnou formu a budou dodržena všechna pravidla. Jeho zpětnou vazbou je informace o kvalitě MPS.

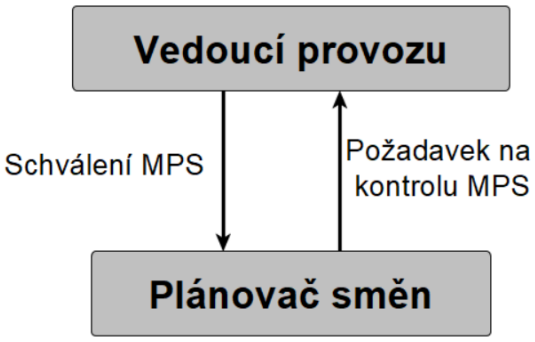


Obrázek 24: Vazba Inspektor provozu – Vedoucí provozu

Plánovač směn – Vedoucí provozu

Plánovač směn je podřízen vedoucímu provozu. Společně zabezpečují správné vydání měsíčního plánu směn. Zpětná vazba plánovače směn směrem k vedoucímu provozu je požadavek na kontrolu MPS. Tu vedoucí provozu provádí schválením především z hlediska pravidel nastavených inspektorem provozu. Řídící akcí je pak

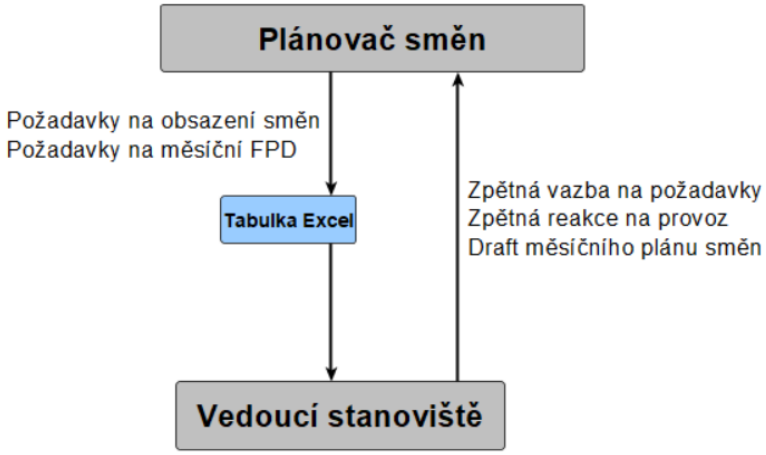
opravený měsíční plán směn, tím je myšlena jeho finální a schválená verze. Proces schválení MPS si lze představit jako kontrolu všech požadavků na daný MPS – dodržení pravidel plánování směn.



Obrázek 25: Vazba Plánovač směn – Vedoucí provozu

Plánovač směn – Vedoucí stanoviště

Spojení těchto dvou řídících prvků má nejvíce řídících akcí a zpětných vazeb. Plánovač směn má směrem k vedoucím dvě řídící akce – požadavky na obsazení směn a požadavky na měsíční fond pracovní doby (FPD). Kontrolní akce jsou předávány přes akční člen – tabulka excel. Vedoucí musí při plánování směn požadavky zadat do plánovacího nástroje, který slouží k plánování směn pracovníků.



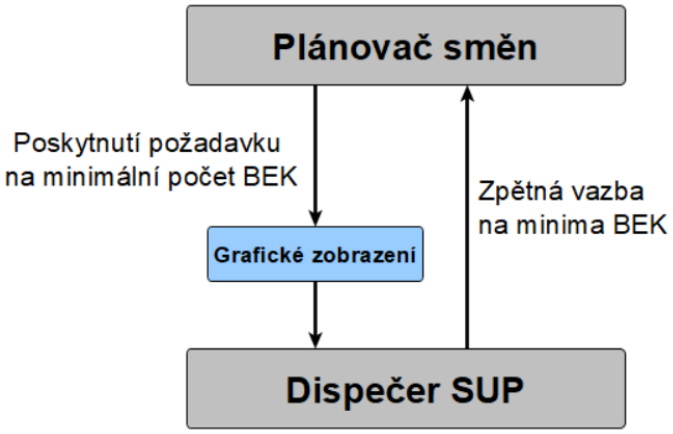
Obrázek 26: Vazba Plánovač směn – Vedoucí stanoviště

Zpětnou vazbou od vedoucího k plánovači je zpětná vazba na zadané požadavky a zpětná reakce na provoz samotný. Reakci na provoz lze chápat jako popis toho, jak naplánované směny pokrývají reálný provoz, eventuálně jestli by nebyla potřeba

nějaké úpravy směn. Zároveň vedoucí stanoviště předává plánovači směn draft měsíčního plánu směn.

Plánovač směn – Dispečer SUP

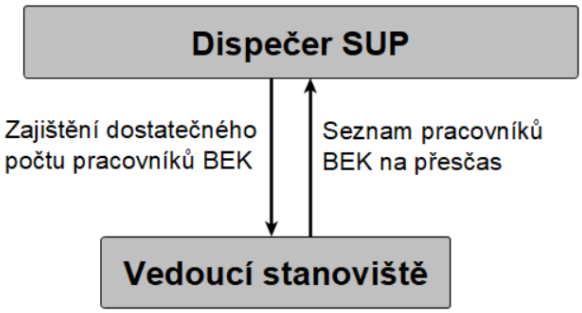
Plánovač směn a dispečer Sup mají vzájemně pouze jednu řídící akci a jednu zpětnou vazbu. Řídící akcí je zde poskytnutí minimálního počtu pracovníků BEK, tzv. minima BEK. Minima BEK stanoví přesný počet nutných BEK 5 dní před plánovaným dnem, například 10. den obdrží dispečer SUP od plánovače minima BEK na 15. den měsíce. Úkolem dispečera je pak zajištění požadovaného počtu BEK. Předání se uskutečňuje pomocí grafického zobrazení. Minima BEK si lze představit jako graf potřebných pracovníků BEK v čase. Minim BEK se týká i zpětná vazba na plánovače směn. Tato zpětná vazba má plánovači směn říct rozdíl mezi původním plánem a aktualizovaným plánem, tedy správnost plánování. Zpětná vazba zároveň udává, zda je například potřeba změna typu směn.



Obrázek 27: Vazba Plánovač směn – Dispečer SUP

Dispečer SUP – Vedoucí stanoviště

Ve vzájemné vazbě těchto dvou prvků se odehrává klíčová část pro zajištění bezproblémové provozu bezpečnostní kontroly. Řídící akcí od dispečera je zajištění dostatečného počtu pracovníků BEK. Zajištění dostatečného počtu pracovníků BEK je založeno na 2 faktorech – minima BEK a nepřítomnosti jednotlivých pracovníků. Tato řídící akce zahrnuje i požadavky na přesčasy na daný den. Dispečer SUP je zodpovědný za dostatečný počet pracovníků BEK pro pokrytí provozu. Zpětnou vazbou je seznam pracovníků BEK na přesčas.



Obrázek 28: Vazba Dispečer SUP – Vedoucí stanoviště

Vedoucí stanoviště – Pracovník BEK

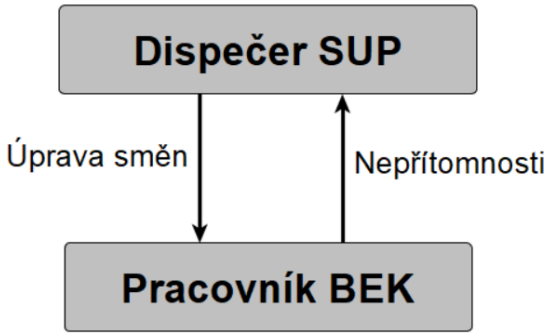
Při interakci těchto dvou prvků byly identifikovány 2 řídící akce a zároveň 2 zpětné vazby. První řídící akcí je předání měsíčního plánu směn, jedná se o měsíční plán směn, který je již finální verzí měsíčního plánu. Měsíční plán je tvořen směnami, které naplánoval právě vedoucí posádky tak, aby co nejvíce odpovídal požadavkům jeho posádky a vyhovoval požadavkům pracovníků BEK za dodržení požadavků a pravidel. Druhou řídící akcí jsou požadavky na přesčas, které jsou založeny na řídící akci od Dispečera SUP – zajištění dostatečného počtu pracovníků BEK. Při této akci musí vedoucí stanoviště sehnat mezi pracovníky někoho, kdo by mohl jít na přesčas. Požadavek na počet přesčasů může být samozřejmě i nulový.

Obrázek 29: Vazba Vedoucí stanoviště – Pracovník BEK

Existují 2 zpětné vazby od pracovníka, zpětná vazba na směny a na provoz. Zpětnou vazbu na směny lze chápat jako reakci na požadované směny do měsíčního plánu směn nebo úpravu směn od dispečera SUP. Zpětná vazba na provoz je reakcí na pokrytí provozu.

Dispečer SUP – Pracovník BEK

Dispečer SUP má směrem k pracovníkovi BEK jednu řídící akci – úprava směn. Úpravu směn provádí dispečer na základě minim BEK a nepřítomnosti pracovníků. Úpravy směn jsou potřebné především v případě posunu provozní špičky. Zpětnou vazbou v tomto spojení je nepřítomnost. Pracovníci BEK mají povinnost nahlásit předem nepřítomnost na plánované směně z důvodu nemoci, ošetřovného atd.

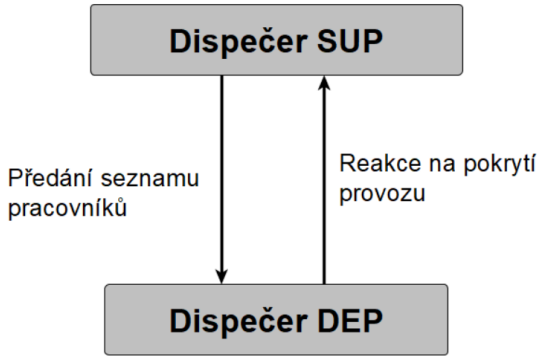


Obrázek 30: Vazba Dispečer SUP – Pracovník BEK

Dispečer SUP – Dispečer DEP

Dispečer SUP a dispečer DEP jsou v neustálém přímém kontaktu, oba mají na starost pokrytí provozu na denní bázi. Dispečer SUP dodá dispečerovi DEP seznam pracovníků BEK – jejich počty a směny. Seznam pracovníků je předán 5 dní před začátkem daného dne. Dispečer DEP pak přiřadí každému pracovníkovi pracovní pozici a řídí jejich pozice celý den. Seznam předaný 5 dní předem je neustále upravován až do dne, ke kterému se vztahuje. Upravuje se na základě nemocí, úpravy směn apod. Dispečer DEP v daný den přesouvá pracovníky v závislosti na provozu, tedy v závislosti na letovém plánu a přesných stojánkách (gate) tak, aby zabezpečil dostatečný počet BEK pro pokrytí všech nutných provozních úloh.

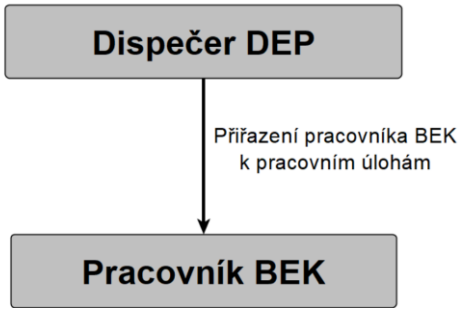
Zpětnou vazbou směrem k dispečerovi DEP je reakce na pokrytí provozu v závislosti na seznamu pracovníků. Zpětnou vazbu pak předá dispečerovi SUP. Při nedostatku pracovníků BEK na pokrytí všech potřebných provozních pozic předá dispečer DEP tuto informaci (zpětnou vazbu) dispečerovi SUP. Následně může dispečer SUP ještě upravit seznam pracovníků – upravit směny nebo zažádat o přesčas.



Obrázek 31: Vazba Dispečer SUP – Dispečer DEP

Dispečer DEP – Pracovník BEK

Dispečer DEP odpovídá za přiřazení pracovníků BEK k pracovním úlohám. Mezi pracovní úlohy lze zařadit obsazení stanoviště bezpečnostní kontroly před zahájením nástupu do letadla. Přiřazení k pracovním úlohám je jeho řídící akcí směrem k pracovníkovi. Pracovník nemá zpětnou vazbu na přirazení k pracovní úloze. Přiřazování je závislé na letovém plánu, respektive na potřebě obsazení jednotlivých stanovišť.



Obrázek 32: Vazba Dispečer DEP – Pracovník BEK

7.3 Identifikace nebezpečných řídících akcí v procesu bezpečnostní kontroly

Dalším krokem STPA je stanovení nebezpečných řídících akcí (Unsafe control actions = UCA), které se stanovují pro každou řídící akci zvlášť. Pro identifikaci nebezpečných akcí stanovuje STPA 4 důvody, proč může být akce považována za nebezpečnou [13]:

- Nepředání řídící akce vede k nebezpečí
- Předání řídící akce vede ke vzniku nebezpečí

- Poskytnutí potenciálně bezpečné řídící akce příliš brzy, pozdě nebo ve špatném pořadí vede k nebezpečí
- Řídící akce trvá příliš dlouho nebo je zastavena příliš brzy (pouze pro v čase spojité řídící akce)

Ke každé UCA je zároveň nutné uvést, které nebezpečí s sebou může nést. Na začátku STPA bylo stanoveno 5 nebezpečí (viz. kapitola 7.1.2.). V následující části uvedu pouze příklad pro tvoření UCA pro jednotlivé řídící akce. Celkový přehled všech UCA bude uveden v příloze (viz. příloha 1).

Řídící akce	**Nepředání řídící akce způsobuje nebezpečí**	**Předání řídící akce**	**Příliš brzy, pozdě nebo mimo pořadí**	**Trvá příliš dlouho nebo je zastavena příliš brzy**
Strategické cíle	UCA-1: Inspektor provozu neposkytne strategické cíle plánovači směn, během přípravy plánování [H-1, H-2, H-3, H-4]	UCA-2: Inspektor předá chybné strategické cíle [H-1, H-2, H-3, H-4]	UCA-3: Inspektor předá strategické cíle pozdě – až po začátku plánování MPS [H-1, H-2, H-3, H-4]	N/A

Tabulka 2: Příklad identifikovaných nebezpečných řídících akcí. Vytvořeno autorem

7.4 Omezení řídícího prvku

Omezení řídícího prvku vychází z identifikovaných nebezpečných řídících akcí. Pro každou identifikovanou nebezpečnou akci je potřeba stanovit omezení řídícího prvku, tedy pro každou UCA je potřeba stanovit „C“. Omezení řídícího prvku specifikuje chování řídícího prvku, které musí být dodrženo, aby nedošlo k nebezpečné řídící akci. Následující tabulka (tabulka 3) ukazuje omezení řídícího prvku vzhledem k řídící akci „Strategické cíle“ a možným nebezpečným řídícím akcím. Celý seznam jednotlivých omezení řídících prvků je uveden v příloze 2.

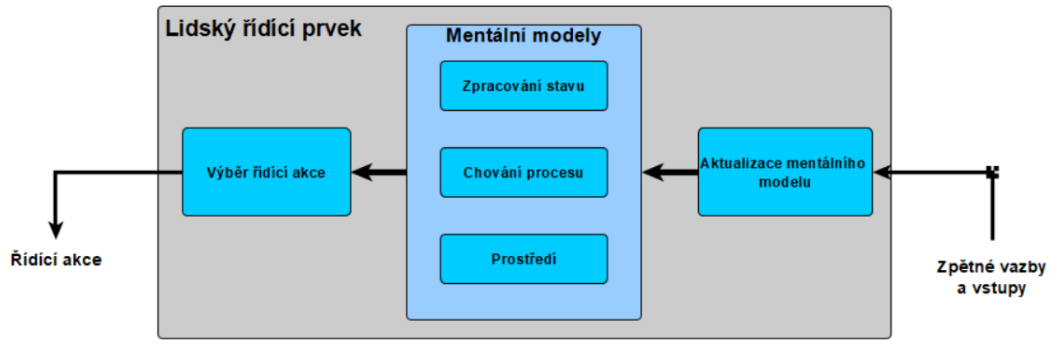
UCA-1: Inspektor provozu neposkytne strategické cíle plánovači směn během přípravy plánování [H-1, H-2, H-3, H-4]	C-1: Inspektor provozu musí poskytnout strategické cíle plánovači směn během příprav plánování
UCA-2: Inspektor předá chybné strategické cíle [H-1, H-2, H-3, H-4]	C-2: Inspektor musí předat správné strategické cíle

UCA-3: Inspektor předá strategické cíle pozdě – až po začátku plánování MPS [H-1, H-2, H-3, H-4]	C-3: Inspektor musí předat strategické cíle ještě před zahájením plánování

Tabulka 3: Identifikované omezení řídícího prvku. Vytvořeno autorem

7.5 STPA a lidský činitel

V této části práce je důležité zmínit nutné rozšíření modelu STPA, kterým je lidský činitel, tzv. STPA – Engineering for Humans [18]. Lidský činitel je velice široký vědní obor zabývající se především interakcí mezi člověkem a jeho okolím [17]. V tomto případě je to interakcí mezi lidmi jakožto řídícími prvky systému. Tato práce se nebude dopodrobna zabývat lidským činitelem, ale je nutné ho zmínit, protože většina řídících prvků v našem systému jsou lidé. Existuje mnoho modelů a teorií zabývajících se lidským myšlením a rozhodováním, ale STPA analýza se nezabývá tím, jak lidé myslí. STPA se spíše snaží vysvětlit, jak a proč řídící prvek překročil bezpečnostní omezení (safety constraints), zároveň se však nesnaží vysvětlit fungování lidské mysli, ale klade důraz na lidské interakce v systému vzhledem k řídícímu procesu. STPA – Engineering for humans je rozšíření, které přináší více možností při vytváření scénářů vedoucích k nebezpečí. Pro použití rozšíření je potřeba si mírně upravit vnitřní strukturu každého lidského řídící prvku (obr. 33) [18].



Obrázek 33: Vnitřní model lidského řídící prvku (Zdroj: [18] Upraveno autorem)

Výběr řídící akce je, jak naznačuje obrázek, závislý na kroku předchozím. Člověk se na rozdíl od stroje či počítače rozhoduje na základě mnoha podnětů. V závislosti na těchto podnětech může být rozhodnutí pokaždé jiné. Počítač naopak dělá „rozhodnutí“ na základě předem definovaného procesu. V našem systému jsou již řídící akce dány, avšak jejich konkrétní realizace může být jiná – závislá na kontextu [18]. Například vazba mezi plánovačem směn a vedoucím stanoviště, kde řídící akcí jsou „požadavky

na měsíční FPD“. Požadavky na měsíční FPD jsou v podstatě stanovením počtu hodin pro každého pracovníka. Tato hodnota může být rozdílná v závislosti na měsíci, počtu pracovních dní, předchozím měsíci atd.

Mentální modely (zpracování stavu, chování procesu, prostředí) v řídícím prvku (člověku) lze chápat jako jeho porozumění kontrolovanému procesu. Porozumění procesu je založeno na základě informací o systému – reprezentaci systému. Mentální modely jsou vždy pouze částečnou reprezentací systému, i když reprezentace obsahuje všechny informace pro konkrétní situaci, současně je potřeba vyloučit některé neužitečné informace, protože není možné současně pochopit všechny prvky reálného světa. Toto je důležitý faktor u rozšíření, protože je užitečné prozkoumat, kde v modelu mohou potřebné informace chybět nebo naopak přebývat zbytečné nebo chybné informace [18].

- Zpracování stavu (process state) lze jednoduše vyjádřit jako rozdíl mezi reálným stavem systému a přesvědčením řídícího prvku o stavu systému – nesoulad mezi reálným stavem a přesvědčením, co může být příčinou nehod [12].
- Chování procesu je další částí mentálního modelu. V této části se řeší chování modelu v závislosti na přesvědčení řídícího prvku, co systém udělá na základě jeho řídících akcí. Zde je potřeba zahrnout i zpracování stavu, kdy vždy existuje rozdíl mezi reálným stavem a stavem, ve kterém si řídící prvek myslí, že systém je [18].
- Poslední části je prostředí, ve kterém se řídící prvek nachází. Zde je potřeba uvažovat mnoho faktorů – zda se řídící prvek nachází ve známé nebo nové situaci, organizační strukturu, sociální vztahy apod.

Třetí součást vnitřního modelu řídícího prvku je aktualizace mentálního modelu. Aktualizaci lze chápat jako příjem informací z okolí operátora od jiných řídících prvků nebo externích vstupů, podle kterých následně dělá svá rozhodnutí. Jak ukazuje obrázek 33, v reálném modelu se jedná například o zpětné vazby a jiné vstupy. Na základě těchto vstupů následně operátor upravuje svoji znalost či přesvědčení o stavu systému [18].

Rozšíření o lidský činitel a rozhodování o přesných řídících akcích je potřebné, protože předpokládáme, že žádný řídící prvek v systému nebude záměrně vykonávat nebezpečné řídící akce. Příkladem může být „UCA-2: Inspektor provozu předá chybné

strategické cíle.“ Při této UCA se nepředpokládá, že inspektor provozu předal schválně chybné strategické cíle na základě správných požadavků a podmínek plánování. Výše zmíněné body lze využít v následujícím kroku STPA analýzy – identifikace scénářů vedoucích k nebezpečné řídící akci (UCA).

7.6 Identifikace scénářů vedoucích k nebezpečné řídící akci

Postup identifikace scénářů vedoucích k nebezpečné řídící akci je popsán v kapitole 6.4. Identifikace scénářů je založena na jednotlivých unsafe control actions (UCAs), kdy pro každou UCA je potřeba vytvořit scénář (Sc), při kterém by mohlo k dané UCA dojít. Je potřeba vzít v potaz 2 různé možné zdroje:

1) Nebezpečné chování řídícího prvku
2) Nedostatečná zpětná vazba a informace

V tabulce níže (tabulka 4) jsou uvedeny scénáře, při kterých může dojít k nebezpečné řídící akci. Scénáře jsou vytvořeny vzhledem k jednotlivým UCAs vytvořeným v předchozím kroku. Scénáře jsou opět vztaženy k řídící akci „Strategické cíle“, které předává inspektor provozu na plánovače směn. V tabulce je uvedeno celkově 8 scénářů ke třem UCAs. Všechny ostatní scénáře k jednotlivým UCAs jsou uvedeny v příloze 3.

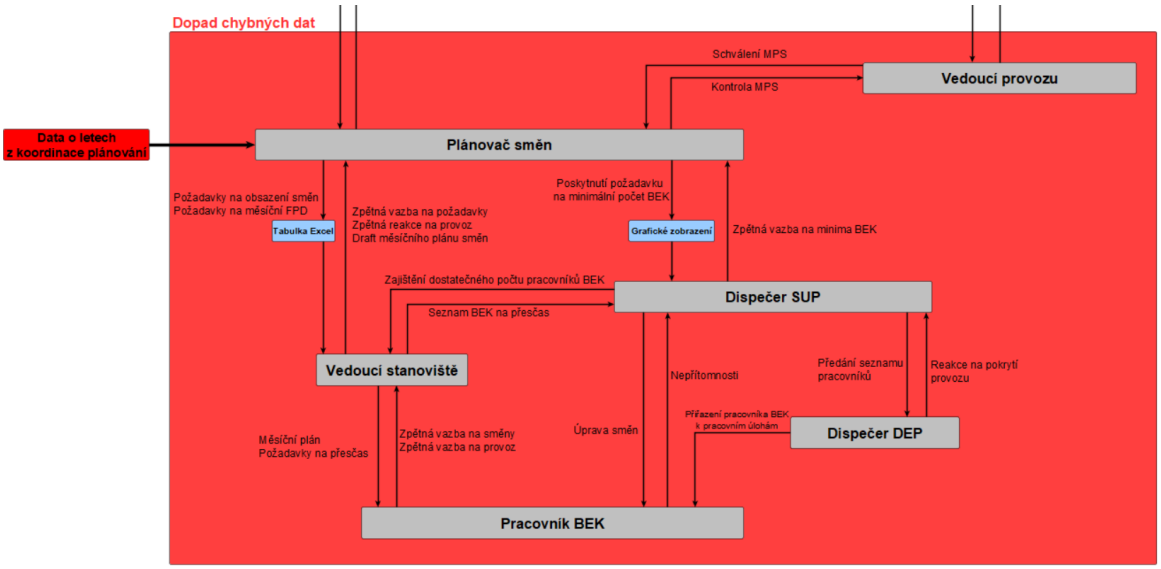
UCA-1: Inspektor provozu neposkytne strategické cíle plánovači směn během přípravy plánování [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-1: Inspektor neobdrží požadavky a podmínky plánování, protože nebyly stanoveny. Inspektor tedy nemůže aktualizovat svůj mentální proces na základě získaných informací, to následně vede k neposkytnutí strategických cílů plánovači směn.
	Sc-2 pro UCA-1: Inspektor získá všechny potřebné informace pro vydání strategických cílů, ty však neposkytne plánovači směn, protože je přesvědčen, že není nutné poskytnout nové strategické cíle. Nedostal totiž zpětnou vazbu o potřebné aktualizaci cílů během plánování od plánovače směn.

UCA-2: Inspektor předá chybné strategické cíle [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-2: Inspektor předá plánovači chybné strategické cíle, protože mu byly předány chybné požadavky a podmínky plánování. On si požadavky a podmínky neověřil a poslal je dále na plánovače směn.
	Sc-2 pro UCA-2: Inspektor předá plánovači chybné strategické cíle, protože chybně vyhodnotil požadavky a podmínky plánování. Došlo k chybné interpretaci poskytnutých informací. K tomuto může dojít, protože požadavky a podmínky se mohou měnit, a tedy vystaví inspektora nové neznámé situaci.
	Sc-3 pro UCA-2: Inspektor předá plánovači chybné strategické cíle kvůli nedostatečné zpětné vazbě ohledně stavu systému. Inspektorovo přesvědčení o stavu systému se liší od reálného stavu, k tomuto může dojít, protože není nastavena pravidelná aktualizace o stavu systému.
UCA-3: Inspektor předá strategické cíle pozdě – až po začátku plánování MPS [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-3: Inspektor předá strategické cíle pozdě, protože nebyl stanoven termín pro předání, k čemuž může dojít, pokud není termín nastaven v pravidlech pro plánování.
	Sc-2 pro UCA-3: Inspektor předá strategické cíle pozdě z důvodu pozdního obdržení požadavků a podmínek plánování.
	Sc-3 pro UCA-3: Inspektor předá strategické cíle pozdě, protože mu trvá příliš dlouho vyhodnocení podmínek. Tento scénář může nastat, pokud jsou podmínky a požadavky velice složité nebo naprosto rozdílné od předchozích – inspektor se nachází v nové/neznámé situaci a zpracování mu trvá dlouho.

Tabulka 4: Přehled scénářů k jednotlivým UCAs. Vytvořeno autorem

8 Diskuse

Během provádění analýzy v systému pro plánování směn byl identifikován jeden vážný systémový nedostatek, který může vést k velkému množství scénářů nebezpečných řídících akcí (viz.obr.34). Jedná o se příjem dat o letech z koordinace plánování. Plánovač směn přijímá data jako pevný fakt a nemá žádnou vazbu na koordinaci plánování. Data z koordinace plánování jsou v systému uvedena jako externí zdroj informace, ale mají velký vliv na celý systém. V systému se neuvažuje možnost předání chybných dat na plánovače směn, zároveň nemá plánovač směn možnost jakkoliv si správnost dat ověřit. Na základě těchto dat je plánován jak měsíční plán směn (MPS), tak i pokrytí každého dne včetně nutnosti pokrytí pracovních úloh. Jakmile jsou data od plánovače směn předána dále do systému, neexistuje zpětná vazba, která by ověřila správnost dat. Celkově je na těchto datech založeno 8 řídících akcí a tomu odpovídajících více než 30 nebezpečných řídích akcí (UCA). Celý systém by na základě těchto dat mohl překročit omezení na úrovni systému a vést ke ztrátám. Ztráty, které by vznikly na základě chybných dat, by mohly vést ke všem ztrátám, jež byly definovány na začátku analýzy (viz. kapitola 7.1.3.). Některé scénáře mohou vést „pouze“ k finančním nákladům, ztrátě reputace nebo poškození majetku. Jiné scénáře však mohou vést i k vážnějším ztrátám, jako je ztráta života z důvodu rizika nedostatečné bezpečnostní kontroly.



Obrázek 34: Identifikovaný systémový nedostatek. Vytvořeno autorem

Po identifikaci byl nedostatek prezentován nezávislému pracovníkovi bezpečnostní kontroly, ten identifikovaný nedostatek potvrdil. Po konzultaci s plánovačem směn bylo

rozhodnuto o provedení testu. Plánovač směn záměrně použil chybná data o letech pro své řídící akce. Chybné řídící akce předal jak na dispečera SUP, tak na vedoucí stanoviště. Ve zpětné vazbě od dispečera SUP a vedoucího stanoviště nebyla označena data za chybná. Test byl poté zastaven tak, aby nedošlo k reálnému ohrožení systému. Po rozhovorech s jednotlivými prvky systému však bylo zjištěno, že data nikdo neověřuje a nezkoumá. Na základě chybných dat by tak vedoucí stanoviště i dispečer SUP provedly svou aktualizaci mentálního modelu a postavili své řídící akce na těchto datech. Chyba v datech by se projevila ve všech řídících akcích spojených s těmito daty. Vedoucí stanoviště by chybně naplánoval měsíční plán směn, ten by byl následně schválen vedoucím provozu, protože vedoucí provozu provádí svou řídící akci na základě požadavku na kontrolu MPS od plánovače směn. Chyba v datech by se následně projevila i v ověření pokrytí na jednotlivé dny. Dispečer SUP by následně provedl úpravu směn jednotlivých pracovníků, stejně tak by předal chybný seznam pracovníků na dispečera DEP. Dispečer DEP by následně přiřadil pracovníka BEK k pracovní pozici na základě řídící akce od dispečera SUP. Dispečer SUP by vytvořil chybné požadavky na zajištění dostatečného počtu pracovníků BEK pro pokrytí provozu a předal by tuto řídící akci na vedoucího stanoviště. Vedoucí stanoviště by předal požadavky na přesčasy na pracovníky BEK. Všechny tyto řídící akce by následně mohly vést ke všem identifikovaným ztrátám v prvním kroku STPA analýzy. Zároveň byl během provádění analýzy a tvoření scénářů nalezen další problém tykající se více řídících akcí a možných nebezpečných řídících akcí. Nalezeným problémem je chybějící pevný termín předávání některých řídích akcí. Příklad je schválení MPS, které provádí vedoucí provozu. Není stanoven pevný termín schválení, ani doba potřebná pro schválení. V systému je nastaven pouze nejzazší termín předání MPS pracovníkům BEK. Obecně v systému neexistuje časová osa, která by stanovovala jednotlivé kroky před předáním MPS pracovníkovi BEK. Dalším přínosem práce bylo potvrzení nutnosti pevných zpětných vazeb v systému.

9 Závěr

Bezpečnostní kontrola je v dnešní době neodmyslitelnou součástí cestování letadlem, nejsou to pouze pravidla a omezení, nedílnou součástí jsou lidé, kteří kontrolu provádějí. V dnešní době kolísajícího provozu je správné plánování směn pracovníků důležité pro zabezpečení pokrytí provozu.

Práce je zaměřena na analýzu plánování směn pracovníků bezpečnostní kontroly a pokrytí provozu vzhledem k letovému plánu. Tento proces probíhá ve komplikovaném socio-technickém systému, kde pracují lidé s využitím techniky pro splnění společného úkolu. Cílem práce bylo ověření využití STAMP v procesech BEK. Pro svůj nezastupitelný význam a dosud chybějící zpracování této oblasti byla zvolena problematika zajištění směn a pokrytí provozních potřeb. Pro analýzu systému byl použit model STAMP (Systems-Theoretic Accident Model and Processes), přesněji byla využita STPA analýza (Systems-Theoretic Process Analysis). STPA analýza zapadá pro přístupu Safety III. Dle Safety III jsou nehody způsobeny nedostatečným řízením během nebezpečí. Lidský činitel Safety III je viděn jako další zdroj odolnosti systému z variability člověka zvládat nečekané události. Pro vytvoření analýzy posloužily historické události, vnitřní znalost systému a rozhovory s účastníky v systému. Analýza byla provedena na základě příručky vytvořené prof. Levenson, jež je autorkou STAMP. V práci došlo k identifikaci ztrát, které v systému hrozí, následně byla identifikována nebezpečí vedoucí k daným ztrátám. Dalším krokem STPA analýzy bylo vytvoření řídící struktury. V řídící struktuře jsou uvedeny jednotlivé řídící akce a zpětné vazby mezi prvky modelu. Třetím krokem STPA analýzy bylo nalezení nebezpečných řídích akcí. Nebezpečné řídící akce vznikají za nejhorších možných podmínek a v určitém kontextu z původních řídících akcí. Identifikované nebezpečné řídící akce byly využity ve čtvrtém kroku analýzy pro vytvoření scénářů, které mohou vést k těmto akcím.

STPA analýza nebyla provedena na celou řídící strukturu, která může mít vliv na plánování směn. Vyšší vedení společnosti a jeho možný vliv na celý analyzovaný proces byl uveden pouze v rámci externího vstupu do inspektora provozu. V analýze zároveň vůbec nebyla uvažována spokojenost pracovníků bezpečnostní kontroly s naplánovanými směnami. Při reálném procesu plánování je nutno brát spokojenost

pracovníků v úvahu. V rámci plánování je nutné nastavovat hranici mezi spokojeností pracovníků a efektivitou provozu.

Během analýzy byl objeven jeden vážný systémové nedostatek v plánování směn a pokrytí provozu. Jedná se o nedostatek ohledně ověření správnosti dat z koordinace plánování a chybějící vazby od plánovače směn ke koordinaci plánování. Dalším identifikovaným nedostatkem byla neexistence přesné časové osy, která by určovala termíny pro jednotlivé nutné kroky před vydáním MPS na pracovníky BEK. Současně analýza ukázala důležitost zpětné vazby vzhledem k množství nebezpečných scénářů založených na nedostatečné zpětné vazbě.

STAMP a STPA analýza by do budoucna mohly být využity na ostatní procesy probíhající na bezpečnostní kontrole, například v systému zajišťování příletů. Využitím v jiných procesech bezpečnostní kontroly by mohlo dojít k identifikaci dalších systémových nedostatků a snížení rizika chybné události.

Seznam příloh:

Příloha 1 – Identifikované nebezpečné řídící akce……73
Příloha 2 – Identifikované omezení řídícího prvku……74
Příloha 3 – Scénáře pro jednotlivé nebezpečné řídící akce……..77

Seznam tabulek:

Tabulka 1: Porovnání Safety I. a Safety II. a Safety III. (Zdroj [4] Upraveno autorem)……..…23
Tabulka 2: Příklad identifikovaných nebezpečných řídících akcí. Vytvořeno autorem……...59
Tabulka 3: Identifikované omezení řídícího prvku. Vytvořeno autorem……....59
Tabulka 4: Přehled scénářů k jednotlivým UCAs. Vytvořeno autorem……62

Seznam obrázků:

Obrázek 1: Zákon napnutého systému (Zdroj: [3] Upraveno autorem)……..……13
Obrázek 2 – : Princip přístupu Safety I [1]……...14
Obrázek 3 – Bimodální přístup Safety I (Zdroj: [14] Upraveno autorem)……16
Obrázek 4 – Princip Safety I (Zdroj: [14] Upraveno autorem)……17
Obrázek 5 – Přístup Safety II k výsledkům. (Zdroj: [1] Upraveno autorem)……18
Obrázek 6 – Přístup Safety II k nalezení chybné události (Zdroj: [1] Upraveno autorem)……..20
Obrázek 7 – Princip emergence (vzniku) Safety II [3]……21
Obrázek 8 – Princip emergence [14]……26
Obrázek 9 – Obecná řídící smyčka (Zdroj: [1] Upraveno autorem)……26
Obrázek 10 – Oblast zájmu STPA [14]……27
Obrázek 11 – 4 kroky STPA analýzy. Zdroj: [14]……29
Obrázek 12: Části definování účelu analýzy (Zdroj: [14] Upraveno autorem]……..…29
Obrázek 13 – Definování účelu analýzy (Zdroj: [13] Upraveno autorem)……..30
Obrázek 14 – Základní model řídící smyčky [15]……..34
Obrázek 15 – Řídící smyčka STPA analýzy (Zdroj: [14] Upraveno autorem)……..35
Obrázek 16 – Složitější řídící model (Zdroj: [1] Upraveno autorem)……37
Obrázek 17 – Ukázka tabulky identifikace nebezpečných řídících akcí [13]……38
Obrázek 18 – Rozšíření řídící smyčky (Zdroj:[14] Upraveno autorem)……..……39

Obrázek 19 – Nebezpečné řídící akce mohou vznikat nebezpečným chováním řídícího prvku nebo nedostatečnou zpětnou vazbou a dalšími vlivy (Zdroj: [14] Upraveno autorem).....40
Obrázek 20 – Řídící struktura (vytvořeno autorem)……..47
Obrázek 21 – Spojení inspektora provozu s požadavky……...51
Obrázek 22 – Vazba Koordinace plánování – Plánovač směn……52
Obrázek 23 – Vazba Inspektor provozu - Plánovač směn……52
Obrázek 24 – Vazba Inspektor provozu – Vedoucí provozu……53
Obrázek 25 – Vazba Plánovač směn – Vedoucí provozu……54
Obrázek 26 – Vazba Plánovač směn – Vedoucí stanoviště……54
Obrázek 27 – Vazba Plánovač směn – Dispečer SUP……..…55
Obrázek 28 – Vazba Dispečer SUP – Vedoucí stanoviště……56
Obrázek 29 – Vazba Vedoucí stanoviště – Pracovník BEK……..56
Obrázek 30 – Vazba Dispečer SUP – Pracovník BEK……..57
Obrázek 31 – Vazba Dispečer SUP – Dispečer DEP……58
Obrázek 32 – Vazba Dispečer DEP - Pracovník BEK……..58
Obrázek 33: Vnitřní model lidského řídící prvku (Zdroj: [18] Upraveno autorem)…...60
Obrázek 34: Identifikovaný systémový nedostatek. Vytvořeno autorem……..64

Seznam grafů:

Graf 1: Zobrazení průběhu počtu cestujících během roku [5]……..…49

Zdroje:

[1] prof. Hollnagel Erik, From Safety-I to Safety-II: A White Paper, 2015. [online]. Dostupné: https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf

[2] ICAO, Doc 9859 – Safety Management Manual, Fouth Edition, 2018. ISBN: 978-92-9258-552-5. [online]. Dostupné: https://skybrary.aero/sites/default/files/bookshelf/5863.pdf

[3] EUROCONTROL, From Safety-I to Safety-II: A White Paper, DNM Safety, 2013. [online]. Dostupné: https://www.skybrary.aero/bookshelf/books/2437.pdf

[4] prof. Levenson Nancy – Safety III: A systems Approach to Safety and Resilience. 2020. [online]. Dostupné: http://sunnyday.mit.edu/safety-3.pdf

[5] Tiskové zprávy | Letiště Václava Havla Praha, Ruzyně. Letiště Václava Havla Praha | Letiště Václava Havla Praha, Ruzyně [online]. Dostupné: https://www.prg.aero/tiskove-zpravy

[6] [KOVERDYNSKÝ, Bohdan. Letecká Security: historie, organizace, standardy a postupy. Cheb: Svět křídel, 2014.Svět křídel. ISBN 9788087567517]

[7] Characteristics of a Good Approach to Safety in the Workplace. EHS Software | EHS Insight [online]. Dostupné z: https://www.ehsinsight.com/blog/characteristics-of-a-good-approach-to-safety-in-the-workplace

[8] HOLLNAGEL, Erik. Safety-I and safety-II: the past and future of safety management. Burlington, VT, USA: Ashgate Publishing Company, [2014]. ISBN 9781472423061.

[9] Lidský faktor – Encyklopedie BOZP. [online]. Dostupné z: https://ebozp.vubp.cz/wiki/index.php/Lidsk%C3%BD_faktor

[10]]HOLLNAGEL, Erik. From Safety-I to Safety-II: A brief introduction to resilience engineering [online]. Dostupné: https://safetysynthesis.com/onewebmedia/Introduction%20to%20S-I%20and%20S-II.pdf

[11] Altabbakh Hanan. STAMP – Holistic system safety approach or just another risk model? [online]. Dostupné: https://www.sciencedirect.com/science/article/abs/pii/S0950423014001193

[12] Leveson, N.G. (2012). Engineering a Safer World: Systems Thinking Applied to Safety. [online]. Dostupné: https://library.oapen.org/bitstream/20.500.12657/26043/1/1004042.pdf

[13] Peper Nathaniel A. Systems Thinking Applied to Automation and Workplace Safety (2007). [online]. Dostupné: http://sunnyday.mit.edu/peper-thesis.pdf

[14] Leveson, N.G. , Thomas P. John. STPA Handbook, 2018. [online]. Dostupné: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[15] SONG Y. Applying System-Theoretic Accident Model and Processes (STAMP) to Hazard Analysis. 2012. [online]. Dostupné: https://macsphere.mcmaster.ca/bitstream/11375/11867/1/fulltext.pdf

[16] DSpace@MIT Home. Systems thinking for safety and security. [online]. Dostupné z: https://dspace.mit.edu/bitstream/handle/1721.1/96965/Leveson_Systems%20thinking.pdf?sequence=1&isAllowed=y

[17] Wickens, C. D., “Multiple resources and performance prediction,” Theoretical Issues in Ergonomics Science, vol. 3, 159-177, 2002. [online]. Dostupné: https://www.researchgate.net/publication/213798935_Multiple_resources_and_performance_prediction

[18] FRANCE MEGAN E. Engineering for Humas: A New Extension to STPA, 2017 [online]: https://dspace.mit.edu/bitstream/handle/1721.1/112357/1008570407-MIT.pdf?sequence=1&isAllowed=y

Příloha 1 – Identifikované nebezpečné řídící akce

Řídící akce	Nepředání řídící akce způsobuje nebezpečí	Předání řídící akce	Příliš brzy, pozdě nebo mimo pořadí	Trvá příliš dlouho nebo je zastavena příliš brzy
Strategické cíle	UCA-1: Inspektor provozu neposkytne strategické cíle plánovači směn během přípravy plánování [H-1, H-2, H-3, H-4]	UCA-2: Inspektor předá chybné strategické cíle [H-1, H-2, H-3, H-4]	UCA-3: Inspektor předá strategické cíle pozdě - až po začátku plánování MPS [H-1, H-2, H-3, H-4]	N/A
Limity práce s ročním FPD	UCA-4: Inspektor nepředá limity pro práci s ročním FPD během příprav na plánování [H-1, H-2, H-3, H-4]	UCA-5: Inspektor předá chybné limity pro práci s ročním FPD [H-1, H-2, H-3, H-4]	UCA-6: Limity pro práci s ročním FPD jsou předány pozdě - až po začátku plánování [H-1, H-2, H-3, H-4]	N/A
Stanovení oblasti a rozsahu MPS	UCA-7: Inspektor nepředá řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu během kontroly MPS [H-1, H-2, H-3, H-4]	UCA-8: Inspektor předá chybně řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu [H-2, H-3, H-4]	UCA-9: Řídící akce (stanovení oblasti a rozsahu MPS) je předána příliš pozdě - po vydání MPS [H-1, H-2, H-3, H-4, H-5]	N/A
Požadavky na obsazení směn	UCA-10: Plánovač směn nepředá požadavky na obsazení směn vedoucímu stanoviště během času na plánování [H-1, H-2, H-3, H-5]	UCA-11: Plánovač směn předá chybné požadavky na obsazení směn [H-1, H-2, H-3, H-4,H-5]	Uca-12: Plánovač směn předá požadavky na obsazení směn pozdě, až po stanoveném datu pro naplánování MPS [H-1, H-2, H-3, H-4,H-5] UCA-13: Plánovač směn předá požadavky na obsazení směn příliš brzy, v čase, kdy není ještě doba plánování [H-1, H-2, H-3]	N/A
Požadavky na měsíční FPD	UCA-14: Plánovač nepředá vedoucímu stanoviště požadavky na měsíční FPD v době pro plánování [H-1, H-2, H-3, H-5]	UCA-15: Plánovač předá chybné požadavky na měsíční FPD [H-1, H-3, H-4, H-5]	UCA-16: Požadavky na měsíční FPD jsou předány příliš pozdě - po začátku plánování [H-1, H-2, H-3, H-4, H-5] UCA-17: Požadavky jsou předány až po naplánování směn - mimo pořadí [H-1, H-2, H-3, H-4, H-5]	N/A
Schválení MPS	UCA-18: Schválení MPS ze strany VP není provedeno během doby na schválení MPS [H-1, H-2, H-3, H-4]	UCA-19: VP provede schválení MPS ve špatném formátu [H-1, H-2, H-3, H-4]	UCA-20: VP provede schválení MPS až po zákonem daném datu vydání [H-1, H-2, H-3, H-4] UCA-21: VP provede schválení MPS ještě před naplánováním všech směn [H-1, H-2, H-3, H-4]	UCA-22: VP zastaví schvalování MPS před dokončením kontroly celého MPS [H-1, H-2, H-3, H-4]
Poskytnutí požadavku na minimální počet BEK (Minima BEK)	UCA-23: Plánovač směn neposkytne dispečerovi SUP minima BEK, když plánuje pokrytí provozu [H-1, H-2, H-5]	UCA-24: Plánovač směn předá minima BEK chybně - ve špatném grafickém zobrazení [H-1, H-2, H-5]	UCA-25: Plánovač směn poskytne minima BEK brzy - více jak 5 dní před zahájením plánování pokrytí [H-1, H-2] UCA-26: Minima BEK jsou poskytnuta pozdě - méně než 5 dní před dnem, ke kterému se vztahují [H-1, H-2]	N/A
Měsíční plán	UCA-27: Vedoucí stanoviště nepředá MPS pracovníkům BEK během doby pro předání [H-1, H-2, H-5]	UCA-28: Měsíční plán je předán s chybami [H-1, H-2, H-3]	UCA-29: Měsíční plán směn je předán pozdě - po stanoveném datu předání [H-3] UCA-30: Měsíční plán je předán mimo pořadí, tedy před jeho schválením [H-1, H-2, H-3]	N/A
Zajištění dostatečného počtu pracovníků BEK	UCA-31: Dispečer SUP nezajistí dostatečný počet pracovníků BEK, když řeší pokrytí provozu [H-1, H-2, H-5]	UCA-32: Dispečer SUP zajistí chybný (na jiné směny nebo větší) počet pracovníků BEK [H-1, H-2, H-5] UCA-33: Dispečer SUP zajistí dostatečný počet pracovníků na jiný než plánovaný den [H-1, H-2, H-5]	UCA-34: Dispečer SUP zajistí dostatečný počet pracovníků BEK příliš pozdě - po začátku směn na plánovaný den [H-1, H-2, H-5]	UCA-35: Dispečer SUP zastaví zajišťování dostatečného počtu pracovníků BEK příliš brzy, ještě před zajištěním potřebného počtu. [H-1, H-2, H-5]
Požadavky na přesčas od VS	UCA-36: VS nepředá požadavky na přesčas mezi pracovníky BEK, když jsou přesčasy potřebné [H-1, H-2, H-5]	UCA-37: Požadavky na přesčas od VS jsou předány na pracovníky BEK chybně [H-1, H-2,H-5]	UCA-38: Požadavky na přesčas jsou předány pozdě na pracovníky - po odchodu pracovníka [H-1, H-2, H-5]	N/A
Úprava směn	UCA-39: Dispečer SUP neprovede úpravu směn, když plánuje pokrytí provozu na daný den [H-1, H-2]	UCA-40: Dispečer SUP udělá chybně úpravu směn [H-1, H-2]	UCA-41: Dispečer provede úpravu směn při plánování pokrytí příliš brzy [H-1, H-2]	UCA-42: Úprava směn je zastavena příliš brzy, ještě před úpravou všech potřebných směn [H-1, H-2]
Předání seznamu pracovníků	UCA-43: Dispečer SUP nepředá seznam pracovníků během plánování pokrytí [H-1, H-2]	UCA-44: Dispečer SUP předá chybný seznam pracovníků BEK [H-1, H-2]	UCA-45: Dispečer SUP předá seznam pracovníků BEK pozdě - po začátku daného dne [H-1, H-2] UCA-46: Dispečer SUP předá seznam brzy - před vytvořením kompletního seznamu [H-1, H-2]	N/A
Přiřazení pracovníka k pracovním úlohám	UCA-47: Dispečer DEP nepřiřadí pracovníka BEK k pracovní úloze, když je potřeba úlohy pokrýt [H-1, H-5]	UCA-48: Dispečer DEP přiřadí pracovníka k chybné pracovní úloze [H-1, H-5]	UCA-49: Dispečer DEP přiřadí pracovníka k úloze pozdě - po urgenci na obsazení úlohy [H-1, H-5] UCA-50: Dispečer přiřadí pracovníka příliš brzy, když nemá pozici obsadit [H-1, H-5]	N/A

Příloha 2 – Identifikované omezení řídícího prvku

Nebezpečné řídící akce	Omezení řídícího prvku
UCA-1: Inspektor provozu neposkytne strategické cíle plánovači směn během přípravy plánování [H-1, H-2, H-3, H-4]	C-1: Inspektor provozu musí poskytnout strategické cíle plánovači směn během příprav plánování
UCA-2: Inspektor předá chybné strategické cíle [H-1, H-2, H-3, H-4]	C-2: Inspektor musí předat správné strategické cíle
UCA-3: Inspektor předá strategické cíle pozdě – až po začátku plánování MPS [H-1, H-2, H-3, H-4]	C-3: Inspektor musí předat strategické cíle ještě před zahájením plánování
UCA-4: Inspektor nepředá limity pro práci s ročním FPD během příprav na plánování [H-1, H-2, H-3, H-4]	C-4: Inspektor musí předat limity pro práci s ročním FPD během příprav na plánování
UCA-5: Inspektor předá chybné limity pro práci s ročním FPD [H-1, H-2, H-3, H-4]	C-5: Inspektor musí předat správné limity pro práci s ročním FPD
UCA-6: Limity pro práci s ročním FPD jsou předány pozdě – až po začátku plánování [H-1, H-2, H-3, H-4]	C-6: Inspektor musí předat limity pro práci s ročním FPD před začátkem plánování
UCA-7: Inspektor nepředá řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu během kontroly MPS [H-1, H-2, H-3, H-4]	C-7: Inspektor musí předat řídící akci stanovení oblasti a rozsahu MPS před/během kontroly MPS
UCA-8: Inspektor předá chybně řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu [H-2, H-3, H-4]	C-8: Inspektor musí předat řídící akci stanovení oblasti a rozsahu MPS správně
UCA-9: Řídící akce (stanovení oblasti a rozsahu MPS) je předána příliš pozdě – po vydání MPS [H-1, H-2, H-3, H-4, H-5]	C-9: Inspektor je povinen předat řídící akci stanovení oblasti a rozsahu MPS před vydáním MPS
UCA-10: Plánovač směn nepředá požadavky na obsazení směn vedoucímu stanoviště během času na plánování [H-1, H-2, H-3, H-5]	C-10: Plánovač směn musí předat požadavky na obsazení směn před zahájením plánování ze strany VS
UCA-11: Plánovač směn předá chybné požadavky na obsazení směn [H-1, H-2, H-3, H-4,H-5]	C-11: Plánovač směn musí předat správné požadavky VS na obsazení směn
Uca-12: Plánovač směn předá požadavky na obsazení směn pozdě, až po stanoveném datu pro naplánování MPS [H-1, H-2, H-3, H-4,H-5]	C-12: Plánovač směn musí předat požadavky na obsazení směn před datem pro naplánování MPS
UCA-13: Plánovač směn předá požadavky na obsazení směn jsou příliš brzy, v čase, kdy není ještě doba plánování [H-1, H-2, H-3]	C-13: Plánovač směn musí předat požadavky na obsazení směn těsně před zahájením plánování
UCA-14: Plánovač nepředá vedoucímu stanoviště požadavky na měsíční FPD v době pro plánování [H-1, H-2, H-3, H-5]	C-14: Plánovač směn musí předat požadavky na měsíční FPD v době pro plánování
UCA-15: Plánovač předá chybné požadavky na měsíční FPD [H-1, H-3, H-4, H-5]	C-15: Plánovač směn musí předat správné požadavky na měsíční FPD
UCA-16: Plánovač směn předá požadavky na měsíční FPD příliš pozdě – po začátku plánování [H-1, H-2, H-3, H-4, H-5]	C-16: Plánovač směn musí předat požadavaky na měsíční FPD před zahájením plánování
UCA-17: Plánovač směn předá požadavky na měsíční FPD až po naplánování směn – mimo pořadí [H-1, H-2, H-3, H-4, H-5]	C-17: Plánovač směn musí předat požadavky na měsíční FPD před zahájením plánování směn

UCA-18: Schválení MPS ze strany VP není provedeno během doby na schválení MPS [H-1, H-2, H-3, H-4]	C-18: VP musí schválit MPS během doby pro schválení
UCA-19: VP provede schválení MPS ve špatném formátu [H-1, H-2, H-3, H-4]	C-19: VP musí schválit MPS ve správném formátu
UCA-20: VP provede schválení MPS až po daném datu vydání [H-1, H-2, H-3, H-4]	C-20: VP musí schválit MPS před daným datem vydání
UCA-21: VP provede schválení MPS ještě před naplánováním všech směn [H-1, H-2, H-3, H-4]	C-21: VP musí provést schválení MPS až po naplánování všech směn
UCA-22: VP zastaví schvalování MPS před dokončením kontroly celého MPS	C-22: VP musí projít celý MPS před jeho schválením
UCA-23: Plánovač směn neposkytne dispečerovi SUP minima BEK, když plánuje pokrytí provozu [H-1, H-2, H-5]	C-23: Plánovač směn musí poskytnout Dispečerovi SUP minima BEK během plánování pokrytí
UCA-24: Plánovač směn předá minima BEK chybně – ve špatném grafickém zobrazení [H-1, H-2, H-5]	C-24: Plánovač směn musí poskytnout minima BEK ve správném grafickém zobrazení
UCA-25: Plánovač směn poskytne minima BEK brzy – více jak 5 dní před zahájením plánování pokrytí [H-1, H-2]	C-25: Plánovač směn musí poskytnout minima BEK přesně 5 dní před zahájením plánování pokrytí
UCA-26: Minima BEK jsou poskytnuta pozdě – méně než 5 dní před dnem, ke kterému se vztahují [H-1, H-2]	C-26: Plánovač směn musí poskytnout minima BEK na požadovaný den 5 dní předem
UCA-27: Vedoucí stanoviště nepředá MPS pracovníkům BEK během doby pro předání [H-1, H-2, H-5]	C-27: Vedoucí stanoviště musí mít k dispozici MPS pro pracovníky BEK během doby pro předání.
UCA-28: Vedoucí stanoviště předá MPS s chybami [H-1, H-2, H-3]	C-28: Vedoucí stanoviště nesmí předat MPS s chybami
UCA-29: VS předá MPS pozdě – po stanoveném datu předání [H-3]	C-29: VS stanoviště musí předat MPS před stanoveným datem předání
UCA-30:VS předá MPS mimo pořadí, tedy před jeho schválením [H-1, H-2, H-3]	C-30: VS musí předat MPS až po schválení
UCA-31: Dispečer SUP nezajistí dostatečný počet pracovníků BEK, když řeší pokrytí provozu [H-1, H-2, H-5]	C-31: Dispečer SUP musí zajistit dostatečný počet pracovníků BEK při řešení pokrytí provozu
UCA-32: Dispečer SUP zajistí chybný (na jiné směny nebo větší) počet pracovníků BEK [H-1, H-2, H-5]	C-32: Dispečer SUP musí zajistit správný počet pracovníků BEK
UCA-33: Dispečer SUP zajistí dostatečný počet pracovníků na jiný než plánovaný den [H-1, H-2, H-5]	C-33: Dispečer SUP musí zajistit dostatečný počet pracovníků na plánovaný den
UCA-34: Dispečer SUP zajistí dostatečný počet pracovníků BEK příliš pozdě – po začátku směn na plánovaný den [H-1, H-2, H-5]	C-34: Dispečer SUP musí zajistit dostatečný počet pracovníků před zahájením směn na plánovaný den

UCA-35: Dispečer SUP zastaví zajišťování dostatečného počtu pracovníků BEK příliš brzy, ještě před zajištěním potřebného počtu. [H-1, H-2, H-5]	C-33/35: Dispečer SUP musí zajistit dostatečný počet pracovníků na plánovaný den
UCA-36: VS nepředá požadavky na přesčas mezi pracovníky BEK, když jsou přesčasy potřebné [H-1, H-2, H-5]	C-36: VS musí mít k dispozici požadavky na přesčasy
UCA-37: Požadavky na přesčas od VS jsou předány na pracovníky BEK chybně [H-1, H-2,H-5]	C-37: VS musí předat správné požadavky na přesčas na pracovníky BEK
UCA-38: Požadavky na přesčas jsou předány pozdě na pracovníky – po odchodu pracovníka [H-1, H-2, H-5]	C-37: VS musí předat požadavek na přesčas na pracovníka před jeho odchodem ze směny
UCA-39: Dispečer SUP neprovede úpravu směn, když plánuje pokrytí provozu na daný den [H-1, H-2]	C-39: Dispečer SUP musí provést úpravu směn při plánování pokrytí provozu
UCA-40: Dispečer SUP udělá chybně úpravu směn [H-1, H-2]	C-40: Dispečer SUP musí provést úpravu směn správně
UCA-41: Dispečer provede úpravu směn při plánování pokrytí příliš brzy [H-1, H-2]	C-41: Dispečer SUP musí provádět úpravu směn až po stanovení potřebných úprav
UCA-42: Úprava směn je zastavena příliš brzy, ještě před úpravou všech potřebných směn [H-1, H-2]	C-42: Dispečer SUP nesmí zastavit úpravu směn před úpravou všech směn
UCA-43: Dispečer SUP nepředá seznam pracovníků během plánování pokrytí [H-1, H-2]	C-43: Dispečer SUP musí předat seznam pracovníků během plánování pokrytí
UCA-44: Dispečer SUP předá chybný seznam pracovníků BEK [H-1, H-2]	C-44: Dispečer nesmí předat chybný seznam pracovníků
UCA-45: Dispečer SUP předá seznam pracovníků BEK pozdě – po začátku daného dne [H-1, H-2]	C-45: Dispečer SUP musí předat seznam pracovníků před začátkem daného dne
UCA-46: Dispečer SUP předá seznam brzy – před vytvořením kompletního seznamu [H-1, H-2]	C-46: Dispečer SUP je povinen předat kompletní seznam pracovníků
UCA-47: Dispečer DEP nepřiřadí pracovníka BEK k pracovní úloze, když je potřeba úlohy pokrýt [H-1, H-5]	C-47: Dispečer DEP musí vědět, kdy je potřeba úlohy pokrýt
UCA-48: Dispečer DEP přiřadí pracovníka k chybné pracovní úloze [H-1, H-5]	C-48: Dispečer musí přiřadit pracovníka ke správné pracovní úloze
UCA-49: Dispečer DEP přiřadí pracovníka k úloze pozdě – po urgenci na obsazení úlohy [H-1, H-5]	C-49: Dispečer DEP je povinen přiřadit pracovníka BEK k úloze včas – ihned po požadavku
UCA-50: Dispečer přiřadí pracovníka příliš brzy, když nemá pozici obsadit [H-1, H-5]	C-50: Dispečer musí mít k dispozici časový rozpis obsazení pozic

Příloha 3 – Scénáře pro jednotlivé nebezpečné řídící akce

Nebezpečné řídící akce	Scénáře pro jednotlivé nebezpečné řídící akce
UCA-1: Inspektor provozu neposkytne strategické cíle plánovači směn během přípravy plánování [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-1: Inspektor neobdrží požadavky a podmínky plánování, protože nebyly stanoveny. Inspektor tedy nemůže aktualizovat svůj mentální proces na základě získaných informací, to následně vede k neposkytnutí strategických cílů plánovači směn.
	Sc-2 pro UCA-1: Inspektor získá všechny potřebné informace pro vydání strategických cílů, ty však neposkytne plánovači směn, protože je přesvědčen, že není nutné poskytnout nové strategické cíle. Nedostal totiž zpětnou vazbu o potřebné aktualizaci cílů během plánování od plánovače směn.
UCA-2: Inspektor předá chybné strategické cíle [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-2: Inspektor předá plánovači chybné strategické cíle, protože mu byly předány chybné požadavky a podmínky plánování. On si požadavky a podmínky neověřil a poslal je dále na plánovače směn.
	Sc-2 pro UCA-2: Inspektor předá plánovači chybné strategické cíle, protože chybně vyhodnotil požadavky a podmínky plánování. Došlo k chybné interpretaci poskytnutých informací. K tomuto může dojít, protože požadavky a podmínky se mohou měnit, a tedy vystavit inspektora nové neznámé situaci.
	Sc-3 pro UCA-2: Inspektor předá plánovači chybné strategické cíle kvůli nedostatečné zpětné vazbě ohledně stavu systému. Inspektorovo přesvědčení o stavu systému se liší od reálného stavu, k tomuto může dojít, protože není nastavena pravidelná aktualizace o stavu systému.
UCA-3: Inspektor předá strategické cíle pozdě – až po začátku plánování MPS [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-3: Inspektor předá strategické cíle pozdě, protože nebyl stanoven termín pro předání, k čemuž může dojít, pokud není termín nastaven v pravidlech pro plánování.
	Sc-2 pro UCA-3: Inspektor předá strategické cíle pozdě z důvodu pozdního obdržení požadavků a podmínek plánování.
	Sc-3 pro UCA-3: Inspektor předá strategické cíle pozdě, protože mu trvá příliš dlouho vyhodnocení podmínek. Tento scénář může nastat, pokud jsou podmínky a požadavky velice složité nebo naprosto rozdílné od předchozích – inspektor se nachází v nové/neznámé situaci a zpracování mu trvá dlouho.
UCA-4: Inspektor nepředá limity pro práci s ročním FPD během příprav na plánování [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-4: Inspektor nepředá limity pro práci s ročním FPD, protože požadavky a podmínky plánování nebyly stanoveny. Inspektor tedy nemůže aktualizovat svůj mentální proces na základě získaných informací, není tedy schopen nastavit včas (v rámci příprav na plánování) pravidla pro práci s FPD.

	Sc-2 pro UCA-4: Inspektor nepředá limity pro práci s ročním FPD během příprav na plánování, protože nedostal zpětnou vazbu (průběžné vyhodnocování) od plánovače směn. Inspektor tedy nemá dostatečnou znalost o reálném stavu, nemá tak potřebu kontrolní akci vydat/upravit.
UCA-5: Inspektor předá chybné limity pro práci s ročním FPD [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-5: Inspektor nepředá limity pro práci s ročním FPD, protože věří, že je již předal. K tomuto může dojít kdykoliv v průběhu z důvodu možných častých změn ohledně ročního FPD.
	Sc-2 pro UCA-5: Inspektor nepředá limity pro práci s ročním FPD z důvodu nedostatečné zpětné vazby od plánovače směn. K tomuto může dojít, když plánovač věří, že zpětná vazba je dostatečná.
	Sc-3 pro UCA-5: Inspektor může neúmyslně předat chybné limity pro práci s FPD. Inspektor očekává určitou reakci systému na jeho kontrolní akci, reálná reakce systému je však jiná než očekávaná – chování procesu je jiné než očekávané. Toto může být způsobeno chybnou nebo nedostatečnou kvalitou zpětné od plánovače směn.
UCA-6: Limity pro práci s ročním FPD jsou předány pozdě – až po začátku plánování [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-6: Limity pro práci s ročním FPD jsou předány pozdě – po začátku plánování, kvůli pozdnímu obdržení informací ohledně požadavků a podmínek plánování. Tento scénář může nastat, pokud jsou podmínky a požadavky velice složité nebo naprosto rozdílné od předchozích – inspektor se nachází v nové/neznámé situaci a zpracování mu trvá dlouho.
UCA-7: Inspektor nepředá řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu během kontroly MPS [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-7: Inspektor nepředá řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu, protože inspektor není informován o probíhající kontrole MPS. Ke scénáři může dojít, protože kontrola MPS nemá stanovené přesné časové rozmezí.
UCA-8: Inspektor předá chybně řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu [H-2, H-3, H-4]	Sc-1 pro UCA-8: Inspektor předá chybně tuto řídící akci, protože zpětná vazba od VP není dostatečná. VP nerozporuje správnost řídící akce, inspektor tedy věří, že řídící akce je předána správně.
UCA-9: Řídící akce (stanovení oblasti a rozsahu MPS) je předána příliš pozdě – po vydání MPS [H-1, H-2, H-3, H-4, H-5]	Sc-1 pro UCA-9: Inspektor předá řídící akci stanovení oblasti a rozsahu MPS vedoucímu provozu pozdě, protože inspektor není informován o probíhající kontrole MPS. Ke scénáři může dojít, protože kontrola MPS nemá stanovené přesné časové rozmezí.

UCA-10: Plánovač směn nepředá požadavky na obsazení směn vedoucímu stanoviště během času na plánování [H-1, H-2, H-3, H-5]	Sc-1 pro UCA-10: Plánovač směn nepředá požadavky, protože neobdržel data o letech z koordinace plánování. Plánovač tedy neměl dostatek podkladů pro vytvoření požadavků.
	Sc-2 pro UCA-10: K nepředání požadavků ze strany plánovače může dojít z důvodu neobdržení řídící akce od inspektora provozu ohledně strategických cílů nebo limitů pro práci s FPD. Pro plánovače pak není možné stanovit požadavky na obsazení směn. K situaci může dojít, když inspektor není informován o potřebě jeho řídící akce.
	Sc-3 pro UCA-10: Plánovač směn nepředal požadavky na obsazení směn. K tomuto může dojít, protože nedostal zpětnou od vedoucího stanoviště o chybějících požadavcích – nebyl aktualizován jeho mentální model o tomto nedostatku.
UCA-11: Plánovač směn předá chybné požadavky na obsazení směn [H-1, H-2, H-3, H-4,H-5]	Sc-1 pro UCA-11: Plánovač předá chybné požadavky z důvodu chybné interpretace dat z koordinace plánování. Neexistuje možnost, jak by si mohl plánovač správnost dat o letech ověřit.
	Sc-2 pro UCA-11: Plánovač obdržel správná data o letech (od koordinace plánování), ale chybně je interpretoval. K chybné interpretaci může dojít k důvodu nedostatečného zácviku pro vytváření požadavků.
	Sc-3 pro UCA-11: Plánovač předá chybné požadavky, protože neprávně vyhodnotil data o letech v kombinaci s instrukcemi pro práci s ročním FPD. Kombinace těchto dvou požadavků je velice složitá a plánovač potřebuje dostatečný trénink – ke scénáři může dojít z důvodu nedostatečných instrukcích pro plánování.
Uca-12: Plánovač směn předá požadavky na obsazení směn pozdě, až po stanoveném datu pro naplánování MPS [H-1, H-2, H-3, H-4,H-5]	Sc-1 pro UCA-12: Plánovač směn předá požadavky na obsazení směn pozdě, až po stanoveném datu pro plánování MPS, protože obdržel pozdě data o letech. Ke scénáři může dojít, protože není nastaven pevný datum předání dat o letech.
	Sc-2 pro UCA-12: Plánovač předá požadavky na směny příliš pozdě, protože věří, že vedoucí stanoviště mají dostatek času na naplánování, k tomuto může dojít, jelikož není pevně stanoven minimální počet dní pro plánování.
UCA-13: Plánovač směn předá požadavky na obsazení směn příliš brzy, v čase, kdy není ještě doba plánování [H-1, H-2, H-3]	Sc-1 pro UCA-13: Plánovač předá požadavky příliš brzy před začátkem plánování, protože postupy nestanovují přesné maximální počet dní před začátkem plánování.
	Sc-2 pro UCA-13: Plánovač předá požadavky příliš brzy před začátkem plánování z důvodu brzkého obdržení dat o letech z koordinace plánování. Předání požadavků brzy může být způsobeno tlakem z okolí na stanovení požadavků.

UCA-14: Plánovač nepředá vedoucímu stanoviště požadavky na měsíční FPD v době pro plánování [H-1, H-2, H-3, H-5]	Sc-1 pro UCA-14: K nepředání požadavku ohledně měsíčního FPD může dojít, protože plánovač směn nemá k dispozici informace ohledně práce s ročním FPD od instruktora provozu. Plánovač tedy nemůže předat řídící akci, protože nemá dostatek informací pro její vytvoření.
	Sc-2 pro UCA-14: Plánovač nepředá požadavek na FPD, protože nemá data o letech – není nastaveno pevné datum předání. Není tedy schopen požadavky vytvořit.
	Sc-3 pro UCA-14: Plánovač nepředá požadavky, protože věří, že vedoucí stanoviště je schopen měsíční FPD stanovit na základě požadavků pro plánování. Scénář může nastat, pokud nemá plánovač dostatečnou zpětnou vazbu.
UCA-15: Plánovač předá chybné požadavky na měsíční FPD [H-1, H-3, H-4, H-5]	Sc-1 pro UCA-15: Plánovač předá chybný požadavek na měsíční FPD, protože nesprávně vyhodnotil data o letech v kombinaci s instrukcemi pro práci s ročním FPD, to může být způsobeno nedostatečným zacvičením.
	Sc-2 pro UCA-15: Plánovač předá chybný požadavek na měsíční FPD, protože je přesvědčen, že hodnoty FPD jsou pro daný měsíc dostatečné, tak aby byl zajištěn dostatečný počet BEK. Plánovač předpokládá, že jeho řídící akce je dostatečná v závislosti na dostupných informacích. Dostupné informace (zpětné vazby) jsou však nedostatečné nebo se liší od reálného stavu systému.
UCA-16: Plánovač směn předá požadavky na měsíční FPD příliš pozdě – po začátku plánování [H-1, H-2, H-3, H-4, H-5]	Sc-1 pro UCA-16: Požadavky na měsíční FPD jsou předány pozdě, protože potřebné informace (data o letech) obdržel příliš pozdě. Neexistuje možnost komunikace mezi koordinací plánování a plánovačem směn.
UCA-17: Plánovač směn předá požadavky na měsíční FPD až po naplánování směn – mimo pořadí [H-1, H-2, H-3, H-4, H-5]	Sc-1 pro UCA-17: Plánovač směn předá požadavky na měsíční FPD až po naplánování směn (mimo pořadí), protože nedostal zpětnou vazbu o chybějících požadavcích na měsíční FPD.
UCA-18: Schválení MPS ze strany VP není provedeno během doby na schválení MPS [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-18: VP neschválí MPS během doby na schválení, protože neobdržel řídící funkci, stanovení oblasti a rozsahu MPS od inspektora provozu.
	Sc-2 pro UCA-18: VP neschválí MPS během doby na schválení, protože neobdržel zpětnou vazbu od plánovače směn o potřebě schválení MPS. K tomuto může dojít, pokud plánovač směn nemá dostatek času, před datem vydání, čekat na schválení od VP – není stanoven pevný termín předání MPS na schválení

UCA-19: VP provede schválení MPS ve špatném formátu [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-19: VP provede schválení MPS ve špatném formátu, protože obdržel stanovení oblasti a rozsahu MPS chybně od inspektora provozu.
	Sc-2 pro UCA-19: VP provede schválení MPS ve špatném formátu, protože si chybně interpretoval stanovení oblasti a rozsahu MPS od inspektora provozu. Ke scénáři může dojít, pokud je stanovení oblasti a rozsahu MPS předáno v novém formátu a VP není s tím formátem seznámen.
UCA-20: VP provede schválení MPS až po daném datu vydání [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-20: VP schválí MPS až po datu vydání, protože není stanoven pevný termín předání MPS na schválení.
UCA-21: VP provede schválení MPS ještě před naplánováním všech směn [H-1, H-2, H-3, H-4]	Sc-1 pro UCA-21: VP schválí MPS před naplánováním všech směn, protože není stanoven pevný termín předání MPS na schválení.
	Sc-2 pro UCA-21: VP provede schválení MPS ještě před naplánování všech směn, protože nemá podrobnou znalost o všech typech a počtech směn, které je potřeba v MPS pokrýt. Ke scénáři dojde z důvodu nedostatečné zpětné vazby od plánovače směn – neposkytnutí všech detailů.
UCA-22: VP zastaví schvalování MPS před dokončením kontroly celého MPS	Sc-1 pro UCA-22: VP zastaví schvalování MPS před dokončením kontroly celého MPS, protože nemá dostatek času na kontrolu celého MPS. K situaci může dojít, pokud požadavek na schválení MPS přijde pozdě od plánovače směn – není stanoven pevný termín.
UCA-23: Plánovač směn neposkytne dispečerovi SUP minima BEK, když plánuje pokrytí provozu [H-1, H-2, H-5]	Sc-1 pro UCA-23: Plánovač směn neposkytne dispečerovi SUP minima BEK, protože nemá k dispozici data od koordinace plánování – neexistence zpětné vazby na koordinaci plánování.
UCA-24: Plánovač směn předá minima BEK chybně – ve špatném grafickém zobrazení [H-1, H-2, H-5]	Sc-1 pro UCA-24: Plánovač směn poskytne minima BEK ve špatném grafickém zobrazení, dispečer SUP pak není schopen plánovat pokrytí provozu. K situaci může dojít, pokud není nastaveno přesné grafické zobrazení minim BEK.
UCA-25: Plánovač směn poskytne minima BEK brzy – více jak 5 dní před zahájením plánování pokrytí [H-1, H-2]	Sc-1 pro UCA-25: Plánovač směn poskytne minima BEK dříve, než 5 dní před zahájením plánovaní pokrytí, když je plánovač směn přesvědčen, že dřívější poskytnutí minim BEK pomůže při plánování pokrytí. Přesvědčení plánovače je tedy jiné než realita systému.
	Sc-2 pro UCA-25: Plánovač smě poskytne minima BEK brzy, pokud obdrží data o letech dříve, než je plánováno – neexistuje pevné datum předání dat o letech od koordinace plánování.

UCA-26: Minima BEK jsou poskytnuta pozdě – méně než 5 dní před dnem, ke kterému se vztahují [H-1, H-2]	Sc-1 pro UCA-26: Plánovač směn poskytne minima BEK pozdě, pokud nedostal zpětnou vazbu od dispečera SUP o chybějících minimech BEK.
	Sc-2 pro UCA-26: Plánovač směn poskytne minima BEK pozdě, protože obdržel data o letech od koordinace plánování pozdě – neexistuje pevné datum předání dat o letech od koordinace plánování.
UCA-27: Vedoucí stanoviště nepředá MPS pracovníkům BEK během doby pro předání [H-1, H-2, H-5]	Sc-1 pro UCA-27: VS nepředá MPS pracovníkům BEK během doby pro předání pokud, nemá MPS k dispozici. K tomuto může dojít z důvodu opoždění při schvalování MPS.
UCA-28: Vedoucí stanoviště předá MPS s chybami [H-1, H-2, H-3]	Sc-1 pro UCA-28: VS předá MPS s chybami, protože MPS je založen na datech o letech z koordinace plánování a plánovač směn nemá žádnou možnost si ověřit správnost těchto dat.
	Sc-2 pro UCA-28: VS předá MPS s chybami, pokud kontrola MPS, ze strany VP, nebyla dostatečná.
UCA-29: VS předá MPS pozdě – po stanoveném datu předání [H-3]	Sc-1 pro UCA-29: VS předá MPS pozdě – po stanoveném datu. K situaci může dojít, pokud není dostatek času schválení MPS – není nastaveno pevné datum pro schválení.
	Sc-1 pro UCA-29: VS předá MPS pozdě – po stanoveném datu. K situaci může dojít, pokud byl proces plánování MPS zahájen pozdě ze strany plánovače směn.
UCA-30:VS předá MPS mimo pořadí, tedy před jeho schválením [H-1, H-2, H-3]	Sc-1 pro UCA-30: VS předá MPS mimo pořadí, tedy před jeho schválením, pokud plánovač směn nepředal požadavek na kontrolu MPS vedoucímu provozu.
UCA-31: Dispečer SUP nezajistí dostatečný počet pracovníků BEK, když řeší pokrytí provozu [H-1, H-2, H-5]	Sc-1 pro UCA-31: Dispečer SUP nezajistí správný počet pracovníků BEK, jestliže je počet pracovníků založen na chybných minimech BEK získaných od plánovače směn.
	Sc-2 pro UCA-31: Dispečer SUP nezajistí dostatečný počet pracovníků BEK, protože si nesprávně interpretoval grafické zobrazení minim BEK. Ke scénáři dojde, pokud nemá dispečer SUP dostatečnou znalost minim BEK – nedostatečný výcvik.
	Sc-3 pro UCA-31: Dispečer SUP nezajistí dostatečný počet pracovníků BEK, jestliže nedostal zpětnou vazbu (seznam BEK na přesčas) od vedoucího stanoviště. Ke scénáři dojde, jestliže VS nesehnal dostatečný počet pracovníků na přesčas.
	Sc-4 pro UCA-31: Dispečer SUP nezajistí dostatečný počet pracovníků BEK na plánovaný den, protože v minimech BEK nemá k dispozici možnost zobrazení počtu pracovníků v čase.

UCA-32: Dispečer SUP zajistí chybný (na jiné směny nebo větší) počet pracovníků BEK [H-1, H-2, H-5]	Sc-1 pro UCA-32: Dispečer SUP zajistí chybný počet pracovníků BEK, protože si nesprávně interpretoval grafické zobrazení minim BEK. Ke scénáři dojde, pokud nemá dispečer SUP dostatečnou znalost minim BEK – nedostatečný výcvik.
	Sc-2 pro UCA-32: Dispečer SUP zajistí chybný (na jiné směny nebo větší) počet pracovníků BEK, jestliže obdrží seznam BEK na přesčas od VS na jiný než požadovaný den. K tomuto může dojít, protože neexistuje kontrolní mechanismus. Chybějící řídící mechanismus způsobí, že VS věří, že předává požadavky na správný den, ale jeho řídící akce má jiný než požadovaný dopad. VS přiřadí pracovníky na základě jeho úsudku, dispečerovi pak předá jména, která se však liší od reálného stavu.
	Sc-3 pro UCA-32: Dispečer SUP nezajistí dostatečný počet pracovníků BEK na plánovaný den, protože v minimech BEK nemá k dispozici možnost zobrazení počtu pracovníků v čase.
	Sc-4 pro UCA-31: Dispečer SUP nezajistí správný počet pracovníků BEK, jestliže je počet pracovníků založen na chybných minimech BEK získaných od plánovače směn.
UCA-33: Dispečer SUP zajistí dostatečný počet pracovníků na jiný než plánovaný den [H-1, H-2, H-5]	Sc-1 pro UCA-33: Dispečer SUP zajistí dostatečný počet pracovníka na jiný než plánovaný den v případě, že si chybně interpretoval grafické zobrazení z minim BEK – nedostatečný výcvik.
UCA-34: Dispečer SUP zajistí dostatečný počet pracovníků BEK příliš pozdě – po začátku směn na plánovaný den [H-1, H-2, H-5]	SC-1 pro UCA-34: Dispečer SUP zajistí dostatečný počet pracovníků BEK pozdě, protože obdržel zpětnou vazbu od VS ohledně přesčasů příliš pozdě.
UCA-35: Dispečer SUP zastaví zajišťování dostatečného počtu pracovníků BEK příliš brzy, ještě před zajištěním potřebného počtu. [H-1, H-2, H-5]	Sc-1 pro UCA-35: Dispečer SUP zastaví zajišťování dostatečného počtu BEK ještě před zajištěním dostatečného počtu BEK, protože byl vyrušen jinými povinnostmi a následně se nevrátil k zajištění pracovníků. Neexistuje mechanismus, který by dispečerovi řekl, aby provedl kompletní pokrytí.
UCA-36: VS nepředá požadavky na přesčas mezi pracovníky BEK, když jsou přesčasy potřebné [H-1, H-2, H-5]	Sc-1 pro UCA-36: VS nepředá požadavky na přesčas, protože nezískal požadavky na přesčas od dispečera SUP. Dispečer SUP nemá požadavky, protože neobdržel minima BEK z důvodů uvedených výše v tabulce.
UCA-37: Požadavky na přesčas od VS jsou předány na pracovníky BEK chybně [H-1, H-2,H-5]	Sc-1 pro UCA-37: Požadavky na přesčas od VS jsou předány chybně, protože obdržel chybné požadavky od dispečera SUP a neexistuje možnost, jak by si mohl správnost požadavků ověřit.

	Sc-2 pro UCA-37: Vedoucí stanoviště předá požadavky na přesčas od dispečera chybně (na jiný než požadovaný den). Komunikace mezi VS a pracovníky BEK probíhá pouze ústně. Není nastaven žádný systém, ve kterém by mohli pracovníci BEK vidět požadované přesčasy na jednotlivé dny
UCA-38: Požadavky na přesčas jsou předány pozdě na pracovníky – po odchodu pracovníka [H-1, H-2, H-5]	Sc-1 pro UCA-38: Požadavky na přesčas jsou předány pozdě mezi pracovníky, jestliže VS obdržel požadavek na zajištění dostatečného počtu pracovníků pozdě od dispečera SUP.
UCA-39: Dispečer SUP neprovede úpravu směn, když plánuje pokrytí provozu na daný den [H-1, H-2]	Sc-1 pro UCA-39: Dispečer SUP neprovede úpravu směn, když plánuje pokrytí provozu na daný den, protože věří, že úprava směn není potřebná vzhledem k minimům BEK.
UCA-40: Dispečer SUP udělá chybně úpravu směn [H-1, H-2]	SC-1. pro UCA-40: Dispečer SUP udělá chybně úpravu směn, protože grafické zobrazení minim BEK není dostatečně srozumitelné.
	Sc-2 pro UCA-40: Dispečer SUP udělá chybně úpravu směn na základě správných minim bek, jestliže nedokáže správně interpretovat data z grafického zobrazení – nedostatečný výcvik.
UCA-41: Dispečer provede úpravu směn při plánování pokrytí příliš brzy [H-1, H-2]	Sc-1 pro UCA-41: Dispečer provede úpravu směn při plánování pokrytí příliš brzy – na základě dříve obdržených minim BEK od plánovače směn.
UCA-42: Úprava směn je zastavena příliš brzy, ještě před úpravou všech potřebných směn [H-1, H-2]	Sc-1 pro UCA-42: Úprava směn je zastavena příliš brzy, ještě před úpravou všech potřebných směn. K tomuto může dojít, protože dispečer SUP je vyrušen jinou prací a neexistuje mechanismus, který mu řekl, zda úpravu dokončil.
UCA-43: Dispečer SUP nepředá seznam pracovníků během plánování pokrytí [H-1, H-2]	Sc-1 pro UCA-43: Dispečer SUP nepředá seznam pracovníků během plánování pokrytí, jestliže neobdržel zpětnou vazbu od dispečera SUP o chybějícím seznamu pracovníků.
UCA-44: Dispečer SUP předá chybný seznam pracovníků BEK [H-1, H-2]	Sc-1 pro UCA-44: Dispečer SUP předá chybný seznam pracovníků BEK, protože obdržel chybný seznam pracovníků na přesčas od vedoucího stanoviště.
	Sc-2 pro UCA-44: Dispečer SUP předá chybný seznam pracovníků BEK, protože má k dispozici chybný (neschválený) MPS od plánovače směn.
UCA-45: Dispečer SUP předá seznam pracovníků BEK pozdě – po začátku daného dne [H-1, H-2]	Sc-1 pro UCA-45: Dispečer SUP předá seznam pracovníků pozdě, jestliže neobdržel zpětnou vazbu od dispečera SUP o chybějícím seznamu pracovníků.
UCA-46: Dispečer SUP předá seznam brzy – před vytvořením kompletního seznamu [H-1, H-2]	SC-1 pro UCA-46: Dispečer USP předá seznam brzy, protože věří, že seznam je kompletní. K tomuto může dojít, pokud je dispečer vyrušen a následně se k vytvoření seznamu nevrátí. Ke scénáři může dojít, protože neexistuje mechanismus, který by ověřil vytvoření kompletního seznamu.

UCA-47: Dispečer DEP nepřiřadí pracovníka BEK k pracovní úloze, když je potřeba úlohy pokrýt [H-1, H-5]	Sc-1 pro UCA-47: Dispečer DEP nepřiřadí pracovníka BEK k pracovní úloze, pokud nemá dostatek pracovníků k dispozici. Ke scénáři dojde, pokud dispečer DEP nepředal zpětnou vazbu na pokrytí provozu.
UCA-48: Dispečer DEP přiřadí pracovníka k chybné pracovní úloze [H-1, H-5]	Sc-1 pro UCA-48: Dispečer DEP přiřadí pracovníka k chybné pracovní úloze, protože neobdržel správný seznam pracovníků od dispečera SUP.
	Sc-2 pro UCA-48: Dispečer DEP přiřadí pracovníka k chybné pracovní úloze, protože neexistuje zpětná vazba.
UCA-49: Dispečer DEP přiřadí pracovníka k úloze pozdě – po urgenci na obsazení úlohy [H-1, H-5]	Sc-1 pro UCA-49: Dispečer DEP přiřadí pracovníka k úloze pozdě, protože nemá k dispozici dostatečný počet pracovníků. K tomuto může dojít, pokud nebylo zajištěno dostatečné množství pracovníků pro pokrytí provozu ze strany dispečera SUP.
	Sc-2 pro UCA-49: Dispečer DEP přiřadí pracovníka na pozici pozdě, protože věří, že pozici obsadil. Dispečer nemá zpětnou vazbu od pracovníka ohledně obsazení pracovních pozic.
UCA-50: Dispečer přiřadí pracovníka příliš brzy, když nemá pozici obsadit [H-1, H-5]	Sc-1 pro UCA-50: Dispečer přiřadí pracovníka na pozici brzy, protože věří, že je potřeba pozici obsadit. Ke scénáři může dojít, protože pracovník BEK nemá zpětnou vazbu na dispečera DEP ohledně obsazení pozic.