



CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

Department of Air Transport

STAMP-based Safety Data Collection and Processing in Civil Aviation Authority

Master's Thesis

Bc. Kateřina Grötschelová

Thesis Advisor: Ing. Andrej Lališ, Ph.D.

Prague 2020



K621**Ústav letecké dopravy**

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

Jméno a příjmení studenta (včetně titulů):

Bc. Kateřina Grötschelová

Kód studijního programu a studijní obor studenta:

N 3710 – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Sběr a zpracování dat o bezpečnosti dle modelu
STAMP v dozorových orgánech**

Název tématu (anglicky): **STAMP-based Safety Data Collection and Processing in
Civil Aviation Authority**

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cíl práce: Návrh sběru a zpracování dat o bezpečnosti dle teorie STAMP pro dozorové orgány v letecké dopravě
- Analýza provozní dokumentace a dat o bezpečnosti leteckých dozorových orgánů
- Analýza systémového modelu bezpečnosti STAMP a metodik CAST/STPA
- Návrh a tvorba vybraných částí provozní dokumentace dle teorie STAMP
- Návrh postupu pro sběr a zpracování dat o bezpečnosti dle teorie STAMP v kontextu navržené provozní dokumentace leteckých dozorových orgánů
- Vyhodnocení navrženého řešení



- 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.
Allweyer, T. BPMN 2.0: Introduction to the Standard for Business Process Modeling. 2nd Ed, Books on Demand 2016.

Vedoucí diplomové práce: **Ing. Andrej Lališ, Ph.D.**

Datum zadání diplomové práce: **17. července 2019**
(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: **18. května 2020**
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

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



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

Potvrzuji převzetí zadání diplomové práce.

.....
Bc. Kateřina Grötschelová
jméno a podpis studenta

V Praze dne..... 17. července 2019

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

Dean's office

Konviktská 20, 110 00 Prague 1, Czech Republic



K621 Department of Air Transport

MASTER'S THESIS ASSIGNMENT

(PROJECT, WORK OF ART)

Student's name and surname (including degrees):

Bc. Kateřina Grötschelová

Code of study programme code and study field of the student:

N 3710 – PL – Air Traffic Control and Management

Theme title (in Czech): **Sběr a zpracování dat o bezpečnosti dle modelu
STAMP v dozorových orgánech**

Theme title (in English): **STAMP-based Safety Data Collection and Processing in
Civil Aviation Authority**

Guides for elaboration

During the elaboration of the master's thesis follow the outline below:

- Thesis goal: Proposal of safety data collection and processing based on STAMP for civil aviation authorities
- Process documentation and safety data analysis of civil aviation authorities
- Analysis of STAMP systemic model of safety and CAST/STPA methodologies
- Proposal and creation of selected parts of process documentation according to the theory of STAMP
- Proposal of safety data collection and processing procedure based on STAMP in the context of the proposed process documentation of civil aviation authorities
- Evaluation and summary

Graphical work range: according to the instructions of thesis supervisor

Accompanying report length: minimum of 55 text pages (including figures, graphs and sheets which are part of the main text)

Bibliography: Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
Leveson, N., Thomas, J. STPA Handbook, 2018.
Allweyer, T. BPMN 2.0: Introduction to the Standard for Business Process Modeling. 2nd Ed, Books on Demand 2016.

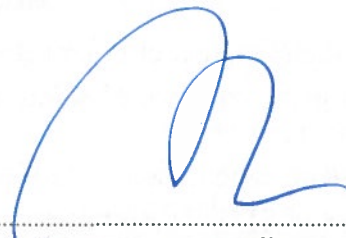
Master's thesis supervisor: **Ing. Andrej Lališ, Ph.D.**

Date of master's thesis assignment: **July 17, 2019**
(date of the first assignment of this work, that has be minimum of 10 months before the deadline of the theses submission based on the standard duration of the study)

Date of master's thesis submission: **May 18, 2020**
a) date of first anticipated submission of the thesis based on the standard study duration and the recommended study time schedule
b) in case of postponing the submission of the thesis, next submission date results from the recommended time schedule



doc. Ing. Jakub Kraus, Ph.D.
head of the Department
of Air Transport



doc. Ing. Pavel Hrubeš, Ph.D.
dean of the faculty

I confirm assumption of master's thesis assignment.

.....
Bc. Kateřina Grötschelová
Student's name and signature

Prague July 17, 2019

Declaration

I hereby declare, that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

I have no serious motives against using this educational work according to the § 60 of Act of the Czech Republic No. 121/2000, on Copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act.).

In Prague, May 2020

A handwritten signature in blue ink, appearing to read 'K. Grötschelová', is written over a horizontal dotted line.

Bc. Kateřina Grötschelová

Acknowledgements

I would like to express gratitude to my supervisor Ing. Andrej Lališ, Ph.D. for his help, support and valuable advice provided during the writing of this thesis. I would also like to thank the employees of the Civil Aviation Authority Czech Republic for sharing their valuable expert knowledge with me and providing consultations to improve my work. Finally, I would want to thank my family and friends for their continuous support thorough my studies and for always believing in me.

Abstrakt

Cílem mé diplomové práce je navrhnout postup sběru a zpracování dat o bezpečnosti dle teorie STAMP pro dozorové orgány v letecké dopravě. První část práce obsahuje popis současného stavu sběru a zpracování dat o bezpečnosti u dozorového orgánu, vysvětlení, co je model STAMP a jak ho lze použít a popis základů BPMN. Na tomto základě je pak v druhé části popsán postup, jak vytvářet procesní modely podle STAMP za použití BPMN modelovacího nástroje. Návrh postupu sběru a zpracování dat o bezpečnosti je popsán a vyobrazen za pomoci vytvořených procesních modelů podle STAMP. Procesní modely i celý návrh postupu jsou v závěru práce validovány a mohou tak poskytovat základ pro modelování dalších procesů a vytváření softwaru pro sběr a zpracování dat o bezpečnosti pro dozorové orgány v letecké dopravě.

Klíčová slova: sběr a zpracování dat o bezpečnosti, dozorový orgán v letecké dopravě, STAMP, STPA, CAST, řídicí smyčka, BPMN modelovací nástroj, bezpečnost, událost v letectví

Abstract

The objective of the master's thesis is to propose safety data collection and processing procedure according to the theory of STAMP for civil aviation authorities. The first part of the thesis contains a description of the current state of safety data collection and processing at the authority, an explanation, what STAMP is and how it can be used, and a description of the fundamentals of BPMN. Based on this, the procedure how to create process models according to STAMP using BPMN modeling tool is described in the second part. The proposal of the safety data collection and processing procedure is described and depicted with created process models according to STAMP. The process models and the entire proposal of the procedure are validated at the end of the thesis and can thus provide a fundamental for modeling other processes and creating software for safety data collection and processing for civil aviation authorities.

Keywords: safety data collection and processing, civil aviation authority, STAMP, STPA, CAST, control loop, BPMN modeling tool, safety, occurrence

Table of Contents

Introduction.....	1
1 Czech system of civil aviation regulation	3
1.1 Civil Aviation Authority – safety oversight.....	4
1.1.1 Certification	5
1.1.2 Safety oversight of aviation services and aviation products.....	5
1.1.3 CAA internal oversight.....	6
1.1.4 External oversight of CAA activities	6
1.2 Safety data collection and work.....	7
1.2.1 Mandatory reporting system.....	8
1.2.2 Voluntary reporting system.....	8
1.3 Internal organizational structure of the CAA and its safety management.....	9
1.3.1 External oversight of organizations.....	10
1.3.2 Internal audits and compliance monitoring system of CAA	10
1.3.3 CAA safety management – Safety Action Group	12
1.4 Process documentation and work with data	13
2 STAMP.....	15
2.1 STPA.....	18
2.2 CAST.....	20
3 BPMN	22
3.1 Flow objects.....	23
3.2 Connecting objects.....	23
3.3 Swimlanes	23
3.4 Atrifacts	24
4 Methodology.....	25
5 Modeling of CAA process documentation	27
5.1 Requirements for the selection of the modeling tool.....	27
5.2 Comparison of modeling tools	29

5.2.1	Bonitasoft.....	32
5.3	Selection of CAA process documentation.....	35
5.4	CAA process models.....	36
5.4.1	CAA Directive – 331: Safety information processing.....	37
5.4.2	Chapter 4, Inspecting staff manual: Procedures for continued oversight of AOC holders.....	44
5.4.3	Work with selected documents and advantages of process models.....	51
6	STAMP-based safety data collection and processing with process models	52
7	Validation.....	58
7.1	Validation using Bonita Studio	58
7.2	Validation by consultations with CAA CR.....	59
7.3	Validaton based on the use of real data.....	59
8	Discussion.....	63
	Conclusion.....	67

List of Figures

Figure 1: Civil aviation administration in the Czech Republic [3].....	3
Figure 2: ICAO audit in the Czech Republic in 2005 [8].....	7
Figure 3: Standard control loop [17]	16
Figure 4: Process model contained in the controller [19]	18
Figure 5: Basic parts of STPA analysis [18]	19
Figure 6: Basic parts of CAST analysis [20]	20
Figure 7: BPMN core objects of BPD [23].....	22
Figure 8: Layout of panels and windows in Bonita Studio	32
Figure 9: Palette of BPMN graphic objects.....	33
Figure 10: Part of the process model of CAA Directive – 331	40
Figure 11: Process to call – subprocess.....	41
Figure 12: Actors – controller.....	41
Figure 13: Local variables – deviations.....	42
Figure 14: Part of the process model of Chapter 4, Inspecting staff manual.....	49
Figure 15: STAMP-based proposal of SDCPS	55
Figure 16: Validation status in Bonita Studio.....	59
Figure 17: Validation based on real occurrence	61

List of Tables

Table 1: Result of comparison of BPMN modeling tools.....	31
Table 2: BPMN object functions [26].....	34
Table 3: Actors and deviations of individual activities from Figure 10.....	43
Table 4: Actors and deviations of individual activities from Figure 11	50
Table 5: Comparison of current and proposed SDCPS	62

Abbreviations

AAII	Air Accidents Investigation Institute
ADREP	Accident/Incident Data Reporting Programme
ANS	Air Navigation Services
AOC	Air Operator Certificate
ARMS – ERC	Aviation Risk Management Solutions – Event Risk Classification
ASM	Airspace Management
ATFM	Air Traffic Flow Management
BPD	Business Process Diagram
BPMN	Business Process Modeling Notation
CAA	Civil Aviation Authority
CAST	Causal Analysis based on STAMP
CMT	Compliance Monitoring Team
CR	Czech Republic
EASA	European Union Aviation Safety Agency
ECCAIRS	European Co-ordination Centre for Accident and Incident Reporting Systems
EU	European Union
EUROCONTROL	European Organisation for the Safety of Air Navigation
ICAO	International Civil Aviation Organization
ISM	Inspecting Staff Manual
LAA	Light Aircraft Association
MoT	Ministry of Transport
RIT	Reduced Interface Taxonomy
SAFA	Safety Assessment of Foreign Aircraft
SAG	Safety Action Group
SDCPS	Safety Data Collection and Processing System

SISel	Safety Intelligence System
SMS	Safety Management System
SSP	State Safety Programme
STAMP	System-Theoretic Accident Model and Process
STPA	System-Theoretic Process Analysis
USOAP	Universal Safety Oversight Audit Programme
XML	Extensible Markup Language

Introduction

Air transport is nowadays a very widespread and often used type of transport. There are many aspects that contribute to the popularity of this type of transport. These aspects are, for example, speed, comfort, economic availability, but also safety. In order to meet all these aspects in the best possible way, aviation must be subject to compliance with many set requirements and to follow relatively strict rules.

Safety is one of the most important aspects of aviation. If aviation safety is not ensured, then the economy of the entire aviation, for example, will be significantly affected. It is therefore highly desirable to constantly improve safety and to use the latest possible procedures to maintain safe aviation.

Every mistake that happens is the first step to learning and improving safety. During the development of the aviation industry, many mistakes occurred, which even many times caused an accident with catastrophic consequences, but this mistake has always provided space for improved safety. It is necessary to learn from past mistakes and not repeat them. With regard to the idea, we should treat all mistakes with respect, deal with them in detail and keep them in mind. It happens in the same way in aviation. Every aviation safety occurrence that happens is examined in detail, processed and stored in a database. It is possible to subsequently perform further analyses from the processed occurrence data, from which various safety recommendations follow, and these recommendations should prevent further similar mistakes and occurrences.

A common problem, however, is that the core of an occurrence is not just one root cause. An occurrence is often the result of several deficiencies in the system that, when met at a given time, can cause an accident. Therefore, during the accident investigation, it is necessary to examine the system as a whole and not be satisfied only with the root cause found. It is clear, that the systemic approach is much more demanding and therefore needs to be simplified and speeded up in some way for investigation and analysis.

There is opportunity to access the occurrence using a systemic approach and simultaneously not complicate the work with safety data. One such option is to improve the Safety Data Collection and Processing System (SDCPS). This system is very important for all aviation organizations, but especially the civil aviation authority, because it is an institution at the state level which oversees the whole aviation. In order to be able to oversee organizations and have an overview of all developments in aviation at the state level, the authority is forced to collect and process safety data.

The aim of this thesis is to propose a procedure for the safety data collection and processing at civil aviation authorities using a new approach to safety. This new approach is based on the theory of the System-Theoretic Accident Model and Process (STAMP), which brings a systemic approach to solving the problem. Based on this approach, it is possible to propose a better procedure for the safety data collection and processing system. However, it is necessary to find a way to apply STAMP to this type of issue and to further deal with how to combine data with a systemic approach so that the proposal can be applied in practice. Given that it is not possible to change the entire environment and conditions for all work with safety data at once, it is also necessary to consider the compatibility of the proposed procedure with the currently used system. The whole proposal of the procedure with its systemic approach should contribute to the improvement of aviation safety and simultaneously be able to fit into the existing system.

1 Czech system of civil aviation regulation

Member states of the International Civil Aviation Organization (ICAO) must meet certain standards in order to maintain an acceptable level of safety. Therefore, each such state must have administrative authorities to ensure the functionality of the civil aviation system. The Czech Republic is part of the European Union Aviation Safety Agency (EASA) system, which promotes the highest social standards of civil aviation safety and environmental protection within the European Union (EU). Synergy is achieved with European Organisation for the Safety of Air Navigation (EUROCONTROL), which provides expert support to EASA. Within the EU, the regulatory framework is addressed mainly at EASA level, which is entrusted by the European Commission to carry out a number of activities related to civil aviation safety. [1][2]

The state (here Czech Republic) is responsible for ensuring safety in the area of civil aviation and, therefore, must actively supervise that all aviation activities are carried out as safely as possible. As a result, the state operates in the area of civil aviation through state administration (Figure 1). The state administration consists of the Ministry of Transport (MoT) and its subordinate, the Civil Aviation Authority of the Czech Republic (CAA). The responsibilities of MoT and CAA are described in Act No. 49/1997 Coll., on Civil Aviation, as amended. [1]

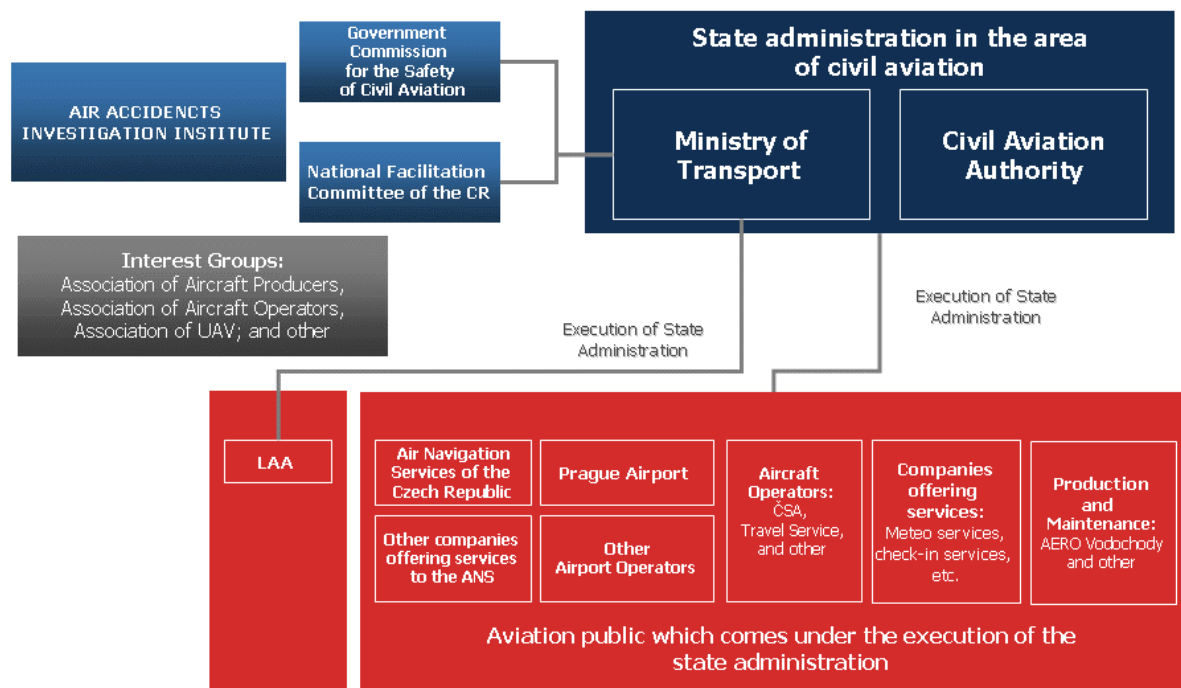


Figure 1: Civil aviation administration in the Czech Republic [3]

The specialised Air Accidents Investigation Institute (AAIL) has been entrusted with the activities of identifying the causes of air accidents and incidents. The state administration of sports flying equipment activities is provided by the Light Aircraft Association of the Czech Republic (LAA). Air traffic services in airspace on the territory of the Czech Republic and at selected airports are provided by Air Navigation Services of the Czech Republic (ANS CR). Under the Civil Aviation Act, CAA may also entrust another legal entity or natural person with providing air traffic services (e. g. Vodochody Airport, Kunovice Airport, Hradec Králové Airport, etc.). [1]

The Ministry of Transport is the main (central) legislative body of the state administration responsible for the development of state transport policy, also in the area of civil aviation. MoT prepares amendments to the laws and, at the same time, publishes implementing legislation. The aim of the MoT is to promote measures for the development of civil aviation and, at the same time, increase its level of safety and efficiency. MoT is an institution that officially communicates with ICAO on behalf of the Czech Republic. [1]

The Civil Aviation Authority is the main executive body of the civil aviation state administration, which is entrusted with this activity by the Ministry of Transport. Its powers extend to the oversight and regulation of civil aviation activities. The CAA acts as a national oversight authority which oversees the performance of the obligations of organizations operating in the area of civil aviation. It also issues various permits, consents and certificates. The CAA is also an institution that officially communicates with EASA on behalf of the Czech Republic. [1][2]

1.1 Civil Aviation Authority – safety oversight

Safety oversight in the Czech Republic is carried out by the Civil Aviation Authority within the scope of the State Safety Programme (SSP). The MoT has the role of an appellate authority as well as an authority responsible for national legislation and the overall concept of air transport at the national level. [1]

CAA issues initial authorizations and permits together with the necessary specifications of operating conditions and subsequently oversees their performance by operators. The main oversight mechanisms include inspections and audits. Other oversight activities are also research to ensure effective implementation of the applicable requirements.

Safety management in the Czech Republic includes processes such as hazard identification and risk management. The oversight system, therefore, also deals with the implementation of these processes by individual operators. Then the oversight system should confirm and ensure that the processes have been implemented efficiently and that they meet the required effect on safety risks. Safety of civil aviation is subject to a number of audits and the implementation of certain standards by ICAO, the European Commission and EASA. The CAA and the MoT strive to ensure that the implementation of standards is as effective as possible in order to meet the appropriate level of oversight of its safety risks. [1]

The Civil Aviation Authority oversees many civil aviation activities. These activities can be divided as follows. The CAA deals with the initial authorization process, oversight of the safety of aeronautical products and air services provided, internal investigation of its own efficiency and quality assurance, and this is related to an external review of effectiveness of the implementation of standards by EASA and ICAO.

1.1.1 Certification

The approval by the state includes the process of certifying organizations, licensing aviation personnel, certifying aerodromes or any other organizations providing civil aviation activities. The exception is aeronautical products certification. The type certificates issuance is the responsibility of EASA, and CAA only performs the assigned certification tasks specified in the contract concluded between EASA and CAA. [1]

All approval processes are described in the applicable directives and manuals of individual CAA units. These process descriptions contain both administrative procedures and technical approval procedures. All CAA procedures must meet all the requirements of ICAO, the EU regulatory framework, but also national legislation. Organizations or individuals can find the procedures and advisory material on the CAA website. [1][4]

1.1.2 Safety oversight of aviation services and aviation products

The certification activity is continuously followed by the activity of ensuring continued oversight of organizations or individuals. Continued oversight has always aimed to ensure that organizations and individuals fulfill their obligations. If, under the continued oversight, it is found that an organization or an individual performs a function contrary

to the regulatory requirements, then the state may use a series of enforcement measures. [1]

Continued safety oversight is carried out in organizations through a system of planned and unplanned inspections and audits. Inspections and audits should help to ensure an acceptable level of safety while verifying that all activities of the organization are operated safely. That means that the activities are carried out in accordance with the regulatory framework. Inspections and audits performed by CAA also often focus on Safety Management System (SMS) procedures and verification of its performance and effectiveness. [1][5][6]

A Safety Assessment of Foreign Aircraft (SAFA) programme has been introduced in the EU as part of safety oversight. This programme allows the ramp inspection of aircraft used by third country operators. Inspections are regulated by strict rules that are the same for all EU countries. The outputs of all SAFA inspections are then stored in a unified format in a common database. [1][5]

1.1.3 CAA internal oversight

As the CAA is the authority responsible for the state oversight of civil aviation safety, it is necessary that inspections and audits are also carried out regarding the CAA's actual operation. For this reason, CAA has implemented a compliance monitoring system in its own management system, which is supported by an internal audit function. The internal audit shall verify the fulfillment of the specified goals and ensure that all requirements for the civil aviation safety oversight system are met. The internal audit also includes the check of SSP compliance. CAA appoints certain natural persons, such as a quality manager or a group of internal auditors, to perform internal oversight activities. [7]

1.1.4 External oversight of CAA activities

The regular external oversight of the CAA is performed by EASA, which is authorized to perform regular standardization inspections and audits in all areas competent within the territory of the EU member states. Goal of these regular inspections and audits is to ensure a unified implementation of requirements and to verify that the implementation of requirements is effective thus fulfilling their purpose. Inspections and audits are performed according to a published procedure. [1]

Other external oversight in the form of audits is conducted by ICAO as part of its Universal Safety Oversight Audit Programme (USOAP). Audits are carried out in ICAO member states in cycles. ICAO's comprehensive standardization audit was carried out in the Czech Republic in 2005. Its results are shown in Figure 2, where the purple bars show the implementation efficiency in individual civil aviation areas, and the blue line shows the global average of audit results from ICAO member states. [8]

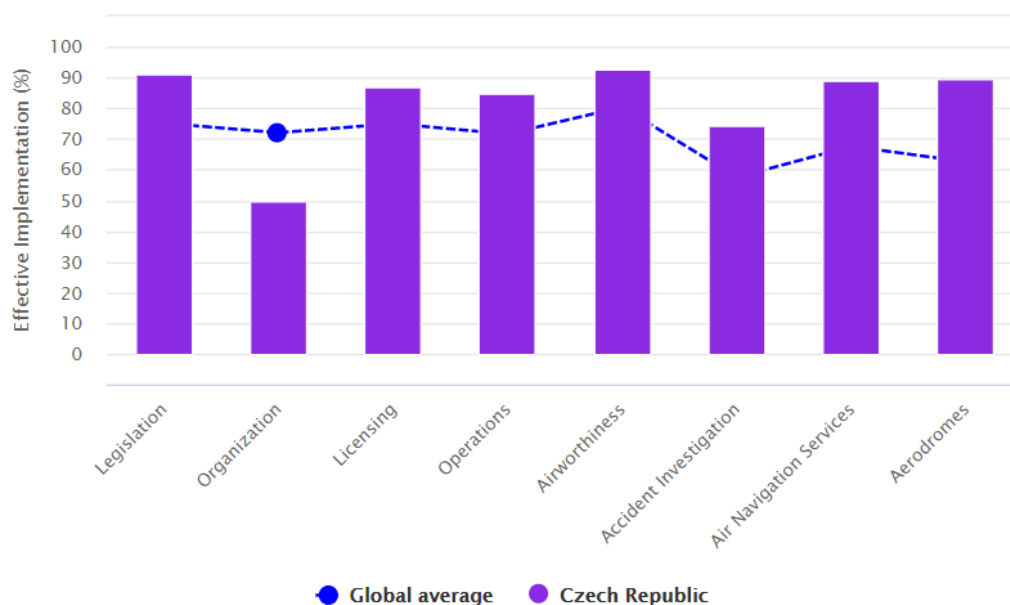


Figure 2: ICAO audit in the Czech Republic in 2005 [8]

1.2 Safety data collection and work

As mentioned in the previous subchapters, the CAA collects external data using various types of inspections or audits performed at individual organizations. But there is another source of civil aviation data. This source is an established aviation safety reporting system. The aviation safety reporting system is one of the main sources of civil aviation safety information. The aviation safety reporting system is divided into a mandatory reporting system and a voluntary reporting system. Regulation (EU) No 376/2014 of the European Parliament and of the Council with Commission Implementing Regulation (EU) 2015/1018 specify the aviation safety reporting system. Regulation (EU) No 376/2014 provides protection to persons who report an occurrence and determines how the state can handle sensitive information. [9][10]

1.2.1 Mandatory reporting system

The AAll was chosen by the competent authority for the basic administration of the mandatory safety reporting system in the Czech Republic. The responsibility of AAll is to implement an effective mechanism for collection, evaluation and storage of civil aviation occurrence reports and to maintain this system in operation. The competent authority designated in a number of implementing regulations is the Civil Aviation Authority. [11]

AAll manages the system of mandatory reporting on its website. All information obtained from individual reports is stored to the database European Co-ordination Centre for Accident and Incident Reporting System (ECCAIRS). This database is also used to store information obtained during the investigation of the reported occurrence. This is information gathered by the AAll, but also information gathered by organizations themselves. [1][11]

CAA has ensured access to aviation occurrences data in the ECCAIRS database. The CAA uses the data stored in the database with its own system for the safety information management in civil aviation.

1.2.2 Voluntary reporting system

A voluntary safety reporting system is established to capture occurrences that the mandatory reporting system might not capture. Any person involved in air traffic may report to the voluntary reporting system. Therefore, the person reporting the voluntary report need not be among the specified persons who fall under the mandatory reporting system. [9][10]

Aviation professionals are supported to report the voluntary occurrence reports. A person who decides to submit a voluntary report may use the voluntary reporting system on the AAll website or on the CAA website. The voluntary reporting system on the CAA website is considered as an additional system, serving as an alternative way of submitting voluntary reports. The reporting form on the AAll website is considered as the main voluntary reporting system. This standard AAll form is followed with other procedures and processes set up by AAll. [11]

1.3 Internal organizational structure of the CAA and its safety management

The Civil Aviation Authority has its own structure, which is given by the Organizational Code of the CAA. The whole CAA is headed by the director. There are several positions under the direct supervision of the CAA director. These include the position of management system manager, quality auditor, safety inspector, spokesperson of the CAA, security director and internal quality control. Furthermore, CAA in the Czech Republic is divided into four divisions, namely the Internal Services and Security Division, Flight Division, Technical Division and Aeronautical Operations Division. Each division, headed by the division director, is further divided into individual departments. The individual departments are managed by the department director. Departments may be further divided into sections headed by a section head. [12][13]

Each division is responsible for certain part of the CAA's activities. The Internal Services and Security Division is responsible for the logistics of the CAA's operations and partially participates in the performance of state oversight in terms of reliability verification processes, the performance of state administration in the area of civil aviation security and legal services of the CAA. The Flight Division carries out oversight activities in the form of continued oversight of Czech commercial air transport operators, non-commercial and specialised operations. The aim of the Flight Division is to ensure the safe operation of aircraft of Czech air transport operators. This division also addresses the issue of the competence of aviation personnel and conducts ramp inspections. The Technical Division deals with the performance of state oversight over the area of airworthiness certificate and continuing airworthiness of aircraft, engines, propellers and other aircraft parts. Another activity that falls within the competence of the Technical Division approval of organizations that design, develop, produce, test, manage continuing airworthiness, maintain, repair, modify and design changes to aircraft, engines, propellers and other aircraft components. The last Aeronautical Operational Division fulfills the task of the national oversight authority under the aeronautical operational safety oversight in the area of air navigation services (ANS), air traffic flow management (ATFM) and airspace management (ASM). Another important scope of this section is the airport oversight and, last but not least, the section is concerned with the issue of unmanned aerial systems. [14]

1.3.1 External oversight of organizations

Each section is responsible for certain part of the external oversight of organizations involved in civil aviation. External oversight can be divided into certification and change management, which can be considered the first part of the safety oversight of organizations. The following safety oversight is called continued safety oversight. Continued oversight includes inspections and audits. The performance of external continued safety oversight covers all four sections. It is the Internal Services and Security Division, Flight Division, Technical Division and Aeronautical Operations Division. Each of these sections has its own procedures for the performance of continued safety oversight in the organizations. However, these procedures of the individual sections are very similar, they differ only in some parts. [5][6]

Sections always determine the cycle of oversight activity for each organization. The base cycle may be shortened or extended with respect to previous inspection and audit results. Furthermore, the cycle may be adapted also with regard to whether or not the organization proves the ability to effectively manage safety risks thus ensures the safe functioning of the whole organization, with an overlap with safe functioning of the whole air transport. Following the identification of the cycle, oversight plans are prepared and inspections or audits are carried out in each organization according to the plans. Each audit or inspection process then has a similar procedure. First, an inspector or group of inspectors shall be appointed to carry out the audit or inspection. Subsequently, the organization that will be inspected must be informed about inspection or audit. After an audit or inspection has been carried out, the inspector must prepare a final report within a specified period. In the final report, the inspector shall indicate all findings (level 1 finding or level 2 finding). On the basis of this final report, the organization shall prepare a plan of corrective actions for each finding. The inspector then approves the corrective action plan or notes any shortage and subsequently oversees for a specified period whether the organization has followed the plan and fulfilled the set objectives. All CAA control activities are in accordance with the Inspection Code of the Czech Republic. [5][6]

1.3.2 Internal audits and compliance monitoring system of CAA

The Civil Aviation Authority has established a system of compliance monitoring and internal audits. Internal audits of the management system are the basic means for verifying that the system (at the CAA) is functioning as a whole. It also verifies the effectiveness of the functioning, fulfillment of requirements, objectives and set goals

within the CAA management system. The aim of internal audits is to identify problem areas in the processes that take place every day at the CAA. Specific problem areas are identified as non-compliance and then corrective actions are established. The corrective action should then resolve the cause of the non-compliance and regulate the problem area. The whole issue of the compliance monitoring system and internal audits should help to identify timely the situation when the CAA is unable to fulfill its responsibilities and tasks. [7]

The Management System Manager is in charge of the system of internal audits at the CAA, who is also the head of the compliance monitoring system according to EU regulations. Other activities such as implementation and administration of the compliance monitoring system are provided by the Quality Auditor. The Management System Manager and the Quality Auditor form together the Compliance Monitoring Team (CMT). The Compliance Monitoring Team then performs internal audits. However, there is a list of suitable and responsible CAA employees who, under certain conditions, form a team of internal auditors. Therefore, the Compliance Monitoring Team can also invite internal audit team members to perform internal audits. [7]

Internal audits are carried out at regular intervals to identify any deviations from the defined requirements in time. Internal audits are, therefore, planned in advance. The CAA's internal audits can be distinguished into two types: a comprehensive audit and a follow-up audit. The comprehensive audit is first announced in advance. The audit itself is carried out by auditors according to the procedures. During this audit all processes of the audited area are verified. Compliances or non-compliances are recorded, which are then described in detail in the Internal Audit Report. Possible non-compliances are divided into two levels, namely level 1 non-compliance and level 2 non-compliance. Level 1 non-compliance usually has direct effect on the CAA process output and the level 2 non-compliance is not reflected in the quality of the CAA output. The Internal Audit Report must be delivered to the audited party in a certain time and then the audited party analyzes the root causes of non-compliance. If the cause can be resolved by corrective action within the audited area, the audited area shall perform it. If a broader corrective action is needed, then the corrective action is taken with the director of the relevant division or with the director of the CAA. A follow-up audit may be carried out after some time after a comprehensive audit has been carried out. The aim of the follow-up audit is to verify the state of implementation of corrective actions for previously identified non-compliances. [7]

1.3.3 CAA safety management – Safety Action Group

Within the CAA, a group for dealing with safety issues was established. This group is called the Safety Action Group (SAG). The SAG regularly deals with specific issues of implementation of the safety management principle and submits proposals for measures to improve safety to the director of the CAA and the management board. SAG therefore deals with the assessment of safety risks, their classification, preparation of proposals for related measures and subsequent monitoring of their effectiveness. Consequently, the SAG is dedicated to the processing of outputs including the analysis of civil aviation safety performance. These outputs are then used to inform the director of the CAA and management board about the situation. In addition, SAG also identifies safety issues, proposes measures to address them and tools to monitor the effectiveness of these measures. [15]

The SAG consists of the head of the group and other members. SAG members cover the area of the Flight Division, the Aeronautical Operations Division and the Technical Division. SAG organizes meetings every month. Meetings can be organized even in extraordinary dates when a response to a safety issue is required. Before each regular SAG meeting, the agenda is determined in advance and distributed to all members of the SAG. Each member of the SAG has the right to supplement the agenda or comment in any way. After the meeting itself, minutes of the meeting are prepared and sent to SAG members who comment the document. Comments are included in the final version of the minutes and the minutes, together with all attachments, are submitted to the director of the CAA for approval. [15]

The sources for SAG activities are mainly mandatory and voluntary safety reporting systems, CAA oversight activities and other information channels. Initial mandatory and voluntary reports come into the AAll system. Based on the concluded agreement, AAll shares all these reports with CAA, together with the final reports of AAll investigation and safety recommendations resulting from them. Another source is the voluntary safety reporting system operated by the CAA, which can be found on the the CAA website. Important inputs are suggestions from any SAG member, CAA leadership, but also other CAA employees. [15]

1.4 Process documentation and work with data

The Civil Aviation Authority has its processes described in detail in directives and manuals. The directives and manuals contain all administrative processes, technical requirements and various procedures for all activities for which the CAA is responsible, and which performs. CAA also publishes procedures and advisory materials that are available to the public on CAA websites. All CAA process documentation must always comply with the requirements of ICAO or, where applicable, with the EU regulatory framework, including applicable national legislation.

However, CAA must also ensure data collection, their analysis and further dissemination. CAA may receive various data from different sources, and it is necessary to work with this data and store it. CAA must then analyze all stored data and share the obtained information with individual organizations, aviation industry areas and the state as a whole. The data is further used in a number of preventive safety measures, for example through the results of statistics or other possible analyzes.

As a standard, keeping data records at CAA is performed in such a way that all obtained data are stored in individual files. These files are either in paper or electronic form. The responsible person therefore puts all the documents obtained into specific files related to certain issue. In addition to record keeping, the responsible person must also keep documentation on the circulation and sharing of specific documents within CAA.

CAA currently utilizes Safety Intelligence System (SISel) in trial operation. SISel is now used to record and protect the received initial safety reports. SISel is used as a support system for the SAG processes. SISel also currently offers the possibility of some evaluation and, based on it, monitoring of trends and other statistics. SISel is able to receive and register all mandatory and voluntary safety reports pursuant to Regulation (EU) No 376/2014 of the European Parliament and of the Council, in an ECCAIRS-compatible format. Reports in a different format must be entered manually into the system. In addition to the recorded occurrence, the responsible person will always add other necessary information such as available documents or the occurrence factors. Available documents are complemented by the cloud system of the CAA (InterCloud). The factors that the responsible person enters to the occurrence are based on the ICAO Accident/Incident Data Reporting Programme (ADREP) taxonomy. The information obtained by the occurrence investigation are progressively added to the SISel system. SISel has implemented the Aviation Risk Management Solutions – Event Risk Classification (ARMS – ERC) methodology, which enables a general evaluation of the

occurrence without knowledge of the occurrence details. The output of the evaluation of the ARMS – ERC methodology are four risk levels, into which the individual evaluated occurrences are categorized. The results of the SISEI evaluation are used in some cases by the SAG to identify further procedures or measures in response to the reported occurrence. [15]

2 STAMP

The System-Theoretic Accident Model and Process (STAMP) is one of the new systemic safety models that carries some of the ideas of Safety-II. The Safety-II approach differs from older Safety-I in that it assumes system variability. Each system operates under certain conditions and these conditions may change. Thus, it is necessary to consider the variability of systems that is capable of responding to changing conditions. Modern systems often include a human who is a part of systems in Safety-II that can be flexible and resilient and that can respond to various impulses. The main idea of Safety-II is to understand how a complex system operates. Safety-II tries to ensure that as many things as possible work in the system properly. Just like Safety-I, it tries to assess risks, manage safety efficiently and also investigate accidents or incidents that have already occurred. But the aim of Safety-II is first to identify how the system normally operates, to explain how it sometimes fails. This leads to better understanding of the conditions under which system performance may be endangered or wrongly monitored and controlled, and to better prevention of incidents or accidents. Because the complexity of our modern systems continues to increase, the approach of how safety is managed also needs to be adapted. Complex systems must be able to maintain their adaptive ability to respond effectively to unavoidable and unexpected situations. [16]

Given the Safety-II approach, it is clear, that it is always necessary to get to know the system in detail, which we want to examine further from the point of safety. That is the reason why STAMP builds on the main idea of systems engineering. Systems engineering was created naturally with the development of new technologies. Every new technology usually brings more complexity to the system, but it is necessary to design and use the system with the highest efficiency and low error and accident rate. Also, new technologies usually bring more frequent interactions between human and machine (computer), so it is necessary to look at the system as a socio-technical whole. [16][17]

Systems engineering is based on systems theory, which forms the theoretical basis. Systems theory tries to perceive individual parts of the system as components that are integrated into one whole. If we deal with safety, we will find that safety of the whole system is always the most important to us. If one of the system components does not perform safely, then this is somehow translated into the whole system performance. It is necessary to connect individual subsystems and monitor the processes of the system as a whole to understand the translation. Systems theory looks at the whole issue in two

ways. The first is the emergence and hierarchy of the systems and the second is the communication and control. [17]

The issue of the system emergence and hierarchy explains each system as a structure that is organized into levels. Each level then carries a specific type of behavior, language and properties. The main concept of emergence and hierarchy is to identify differences between levels of the system and understand their complexity. The result of the levels study should be an explanation of the relationships between the levels. Specifically, to find out how levels arise, what generates them, what separates them, and what emergent properties each level contains and why. The second approach from the perspective of communication and control loosely follows the idea of the emergence and hierarchy. A system, which is divided into individual levels, is characterized by control processes that take place at the interface between system levels. The system control is therefore associated with establishment of safety constraints. The reason for creating constraints is to prevent dangerous events and conditions that could put the system in a hazardous state. Most systems have some input and output, whether within their own structure or through interaction between systems. This suggests that communication is an integral part of systems. Systems that have input and output, or open systems, can be considered components that are interconnected. Due to mutual cooperation, these systems operate on the principle of dynamic balance. In this balance, the system can be maintained using feedback control loops. [17]

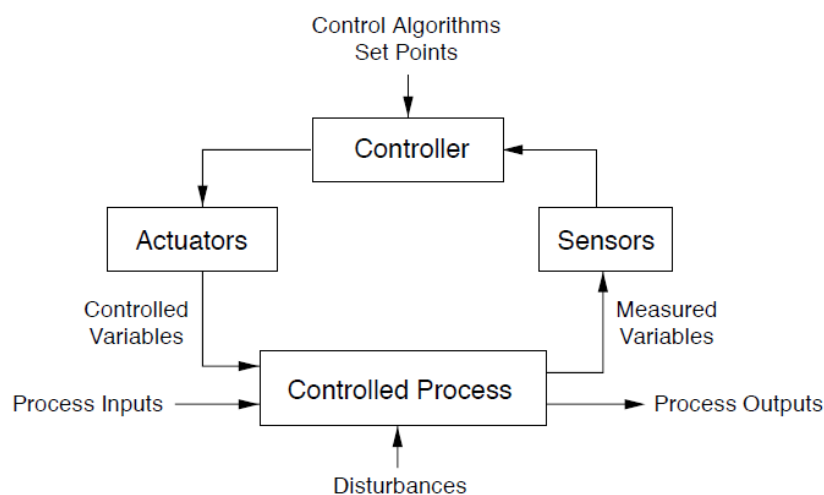


Figure 3: Standard control loop [17]

One of the typical feedback loops is the standard control loop, which we can see in Figure 3. This control loop consists of four main elements: Controlled Process, Sensors,

Controller and Actuators. Each process is controlled by an element called Controller. Controller, whether human or computer, must have some process model and control algorithm to effectively control the process. The Controller uses Sensors to get up-to-date information about the Controlled Process. The Sensors record the measured variables, which describe the current state of the process to the Controller. After the Controller evaluates the current state and decides for control action, then come the Actuators to start the newly chosen way of the process control. If we focus on the Controlled Process, we can see that its integral part is input and output. However, one should not forget the important component that often enters the process, namely noise. Noise is a component that can significantly affect the process. Therefore, in order to obtain the desired goal of the process operating within predetermined limits, we need to use feedback control loops. [17][18]

As discussed in the previous paragraphs, STAMP is an extended causal safety model based on system theory. It can be described and explained in more detail using three basic terms. These are safety constraints, hierarchical safety control structure and process model. STAMP cannot be simply graphically represented like some other models. All three terms need to be properly assembled and interconnected to explain the essence of STAMP. These three terms have already been partially approached above, but here it is appropriate to explain their interconnection and relation in more detail. [17]

Safety constraint describes limitations on the controller's behavior to achieve the required goal and is the basis of STAMP. Its new approach to safety requires the control of socio-technical systems and enforcement of safety constraints. The control can be divided into two types, namely passive and active control. Passive control is based on physical laws and limits of materials used. These limits bring natural constraints. Examples are system components that maintain a safe environment by their presence or ensure the safe system state through physical laws. Unlike passive control, active control requires additional activities to help identify safety constraints. These activities include monitoring, measurement of some variables, diagnostics of measured outputs and setup of corrective procedures. Therefore, safety constraints in the system must be identified, enforced and subsequently effective controls implemented. In addition to safety constraints, responsibility needs to be defined for their enforcement. [17]

In order to define safety constraints in the system as accurately as possible, the system must be logically divided. It is obvious from systems theory that STAMP takes a view of the system as hierarchical structure. Each level of the hierarchical system imposes safety

constraints on activities performed by the lower level. Thus, the lower level behavior can define an area with a missing constraint. Between levels, there operate control processes that control the lower level but carry feedback to the higher level. Control processes, therefore, need to have safety constraints identified. If the control processes have no defined safety constraints, then the responsibility in the system would be lost. [17]

The third important part of STAMP is the process model. The process model is embedded in each system level. Specifically, we can say that the process model is included in the automated controller's control logic or in the mental model maintained by the human controller (Figure 4). The process model is used to maintain the required state of variables and to monitor the current state of the system. The model is regularly updated with feedback that transmits information and helps determine what control actions must be performed. Process models are used both to understand why accidents occur and why people provide inadequate control over system safety, and to design safer systems. STAMP is trying to analyze why accidents occur in today's complex socio-technical systems with tools such as Systems-Theoretic Process Analysis (STPA) and Causal Analysis based on STAMP (CAST). For both analyses, STAMP is the theoretical basis. [17]

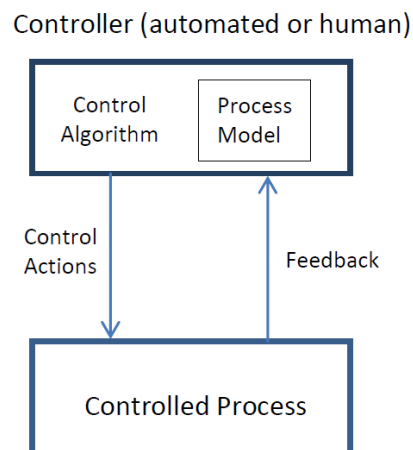


Figure 4: Process model contained in the controller [19]

2.1 STPA

System-Theoretic Process Analysis (STPA) is a hazard analysis method based on control and systems theory. In contrast to other hazard analyzes, STPA does not look at the reliability of individual components, but rather deals with the issue of component interaction. Thus, in STPA is difficult to generate any probability or stochastic value,

because important causal factors would have to be omitted and such a value could be distorted and misleading. However, STPA can better analyze hazards in emerging systems that we have no historical data from to proceed. Furthermore, STPA supports much better systems where software and human behavior occur together. As mentioned, the application of STPA is already possible during the design of the system, which allows the creation of requirements and constraints at an early phase of system development. STPA can also be used for a functional system, both for technical and for organizational. [19]

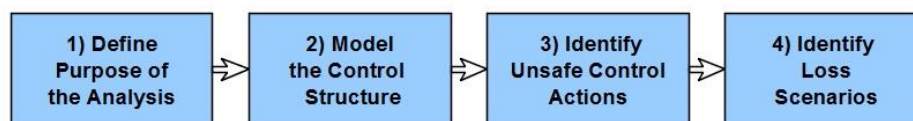


Figure 5: Basic parts of STPA analysis [18]

Figure 5 shows how to perform STPA on the systems studied. STPA considers steps 3) and 4) as the core parts of the analysis, where unsafe control actions and their causes are identified. Steps 1) and 2) are considered complementary but necessary to initiate the main analysis steps 3) and 4). An explanation of the steps is provided in the STPA Handbook (Nancy G. Leveson and John P. Thomas; 2018) [18]:

- 1) The first step ensures definition of the purpose of the analysis. First, we define the area that will be subject to the analysis and determine the goal that we want to achieve by the analysis. Next, we proceed according to the specified parts of the analysis: identify losses, identify system-level hazards, identify system-level safety constraints and specify the hazards.
- 2) In the second step we should model the control structure of the system using feedback control loops.
- 3) The third step identifies unsafe control actions that could lead to a hazardous state of the system. Such states can arise from inadequate control or enforcement of safety constraints. Such a situation can occur due to:
 - control action not provided,
 - control action provided hazardously (incorrectly),
 - control action performed too early, too late, or in the wrong order,
 - control action lasting too long or is stopped too soon.

- 4) The last fourth step of the analysis says that we must identify the loss scenarios. The task is to find out how these scenarios can occur and identify their causal factors. Specifically, we execute the following points:
- We identify all unsafe control actions and examine the functionality of the control loops. We then examine the existing measures of the system and, if they do not exist, we create them.
 - If we propose any new measures, we must consider how these measures could degrade over time. For this reason, protection needs to be ensured in advance through management of change procedures, performance audits and accident and incident analyzes.

2.2 CAST

Causal Analysis based on STAMP (CAST) is an accident analysis method that is based on systems theory. If we look at an accident report, we usually find accident description from the event point of view. Often these events are taken as root causes, and the entire analysis ends at the point where the person who is to blame for the event is found. If we look at such an accident report from the perspective of STAMP, we can come up with a very different view of the accident with many other questions that are not answered in the report. The aim of CAST analysis is to examine the whole design of the socio-technical system, understand its operation, identify its flaws and subsequently to propose changes that would potentially eliminate other possibilities of accidents. It is therefore necessary to focus on the reason why, for example, the person behaved at a given time and with the information, so that this behavior caused an accident. However, we can also perform CAST in cases where there is no accident or (safety or security) incident. CAST can be used to explain any unwanted events in order to prevent future losses (financial loss, loss of life, environmental pollution or damage to company reputation). [17][20]

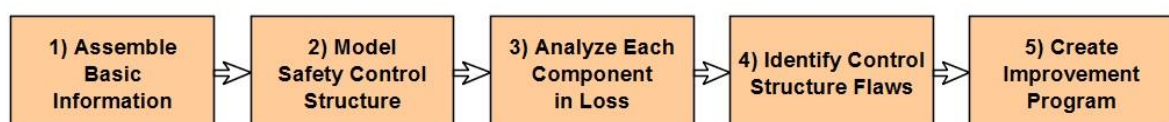


Figure 6: Basic parts of CAST analysis [20]

Figure 6 shows how to perform CAST on the systems studied. CAST says that accident investigations do not necessarily follow a straight line of the process. However, it is

practical to start with steps 1) and 2), because they provide basic information for later activities. The following steps 3), 4) and 5) then deal with the analysis itself, where questions are generated that lead us to the goal of the investigation. Detailed explanation of the steps is in the CAST Handbook (Nancy G. Leveson; 2019) [20]:

- 1) The first step ensures the collection of basic information to perform the whole analysis. This step can be divided into the following five points:
 - Define the system involved and the scope of the analysis.
 - Describe the losses and the hazardous state that led to the losses.
 - Identify the system-level safety constraints that are needed to prevent hazards.
 - Describe what happened without conclusion or blame and generate questions that need to be answered to explain events.
 - Analyze the physical losses in terms of the equipment and controls.
- 2) In the second step, we model the existing safety control structure for this type of hazard using feedback control loops.
- 3) In the third step, it is necessary to find out why the losses were not prevented. The task is to go through all levels of the control structure and focus on individual roles (automated or human). We need to find out why the roles did what they did and why they thought it was right at the time.
- 4) The fourth step identifies flaws in the control structure as a whole (general systemic factors), which may have contributed to the losses.
- 5) The last fifth step of the analysis says that it is necessary to create recommendations for changes in the control structure. These changes should prevent further similar losses in the future. If appropriate, it is also possible to design a continuous improvement program for the hazard as part of the risk management program.

3 BPMN

Business Process Modeling Notation (BPMN) is a modern notation created in accordance with current trends in the world of business systems. BPMN version 1.0 was created in 2004, but nowadays a newer version of BPMN (BPMN 2.0) is used. The goal of BPMN is to standardize the description of processes throughout their life cycle, or workflow. BPMN therefore provides a notation that meets several required conditions at the same time. BPMN is easy to understand for business analysts and project managers who monitor, manage and control processes, but also fulfills a form of technical process notation that is readable for analysts and developers who implement solutions to further support the processes. With this approach, BPMN has become the standard for business process modeling. [21][22]

The description of BPMN processes is defined by the Business Process Diagram (BPD). BPD is based on flowchart elements and is modified to create visual process models. BPD consists of a network of graphic objects, especially activities and flows, which define the activities order in which they are performed. The aim of BPMN is to create well arranged diagrams, so BPDs use graphical objects that are well distinguishable. Their mutual difference lies in the shape of individual objects. For even better distinguishing, it is also possible to highlight these objects with different colours. However, colours are not precisely defined, so each BPMN software can use them arbitrarily. But in the currently used BPMN softwares, it is possible to see that the basic use of colours for certain objects does not vary significantly. BPD contains four fundamental categories of graphic objects, which can be further divided into subtypes. These four fundamental categories are flow objects, connecting objects, swimlanes and artifacts (Figure 7). [21][22]

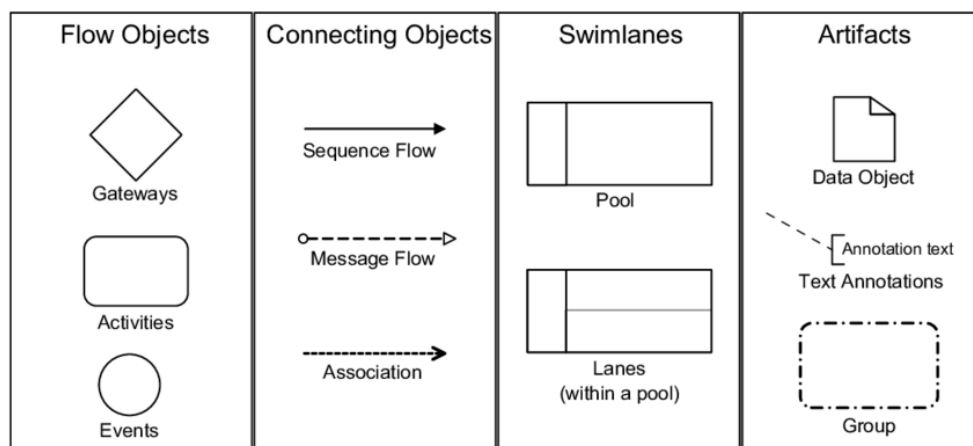


Figure 7: BPMN core objects of BPD [23]

3.1 Flow objects

Flow objects are objects that are related to the flow of information in the process. This category contains three fundamental objects: event, activity, and gateway. The event is represented by a circle. It is something that directly affects the process flow. Events are used at the start and end of the process, but there are other types of events which can be used during the process. The activity is represented by a rectangle with rounded corners. It is a general term for the work or tasks that a company performs. The activity is divided into atomic and compound. An atomic activity is called a task, whereas compound activity contains another separate process (subprocess), so this type of activity is called a subprocess. The gateway is represented by a diamond. It is used to represent decision-making or dividing and connecting flows. [21][22]

3.2 Connecting objects

Connecting objects are objects that are used to connect flow objects to each other or to artifacts. Together they form the fundamental structure of the process diagram. Connecting objects are divided into sequence flow, message flow and association. The sequence flow is represented by a solid line with a solid arrow and determines the order of activities performed in the process. The message flow is represented by a dashed line with an empty circle and an empty arrow. This object shows the flow of messages between two process participants (business roles/entities) who send and receive them. The association is represented by a dashed or dotted line with a simple arrow, which allows to associate flow objects with some additional information such as data, text and other artifacts. [21][22]

3.3 Swimlanes

Swimlanes are used to separate activities in order to differentiate the responsibilities of process participants for individual activities. There are two types of swimlanes: pool and lane. The pool bounds the process and its title is placed in its heading. It represents the participant in the process. In one pool there is just one process and the communication between these pools takes place using message flow. Lane is a part within the pool and is used to organize and further categorize activities. It can indicate the roles, departments, or functions of an organization. Communication between lanes takes place using sequence flow. [21][22]

3.4 Artifacts

Artifacts increase the flexibility of the modeling tool, extend and specify information for the process which does not affect process flow. The fundamental artifacts include data object, group and text annotation. This object is represented by a rectangle with a folded corner, or sheet of paper. The data object refers to data that is required or produced by the activity. Data objects are associated with specific activities using associations. The group is represented by a rectangle, which is drawn by a dashed line. Grouping of activities can be used for documentation or analytical purposes, but it has no effect on the flow sequence. The text annotation is represented by text that is associated using the association with another graphic object. It provides only additional text information in the process diagram. This information can make it easier to read and understand the process diagram. [21][22]

4 Methodology

The goal of the master's thesis is to create a proposal of safety data collection and processing according to the theory of STAMP for civil aviation authorities. It follows from this goal that it is first necessary to perform an analysis of the current state of safety data collection and processing at the authority and then analyze the STAMP systemic model of safety, including STPA and CAST methodologies. To create the whole proposal, it is necessary to make a model to show how the STAMP approach can be used in civil aviation authority. For the creation of such a model, it is required to provide process documentation that describes the processes taking place at the CAA. Considering that the process documentation of CAA is normally in the form of a text description of processes, it is necessary to find a way to create a graphical algorithmic representation of processes to which STAMP is better applied. In this case, the use of BPMN is a possible solution, which allows to represent processes in graphical algorithmic form. Both STAMP and BPMN approach each organization as a hierarchical control structure. This structure can be found in the current process documentation of CAA, but it is necessary to make an algorithmic representation of it, which will allow the collection of process data of CAA. BPMN modeling tools allow this representation, so it is appropriate to use them. However, BPMN is not fully compatible with the theory of STAMP, so it is required to find a way how BPMN software can be used to store information needed for STAMP. In the selection of software, it is therefore advisable to consider whether it is open source software, where source code is open, because if so, then it is possible to extend the software with additional features. It is also necessary that the appropriate BPMN software meets other requirements that are placed in terms of further use of this proposal in practice. For example, in order to be able to work with the model in practice, it is convenient to find software that is freeware, so that anyone can work with it and is powerful and stable even after entering more data than this work requires. Detailed requirement list follows in the next chapters.

To create a proposal, it is necessary to model the process documentation of CAA. Due to the validation cooperation with CAA CR, its process documentation was used, but the proposal is created for all CAAs. However, the CAA documentation is very extensive, and at the same time, there is no graphical algorithmic representation of it, which makes it harder to understand and prepare for further use. Due to the extent of process documentation and the complexity of its modeling, it is appropriate to select only a part of it and process it for the needs of this work. In this work, the selection of part of the

CAA's process documentation was made based on the relevance of the processes to safety and safety data, not by random selection. In this case, it is necessary that the processes regard the issue of safety data and thus be one of the fundamental pillars for the safety data collection and processing.

5 Modeling of CAA process documentation

This chapter builds on the previous chapter, where the methodology of this work was described. The following subchapters progressively describe the individual solutions of specific parts, which were presented in the Methodology chapter. The solution of individual steps connected with the issue of modeling brings us to the modeling of the process documentation of CAA and the description of the resulting process models.

5.1 Requirements for the selection of the modeling tool

BPMN modeling tools are software that allows to appropriately process existing theoretical information into process models. The goal of these modeling tools is to facilitate the creation of models and enable further work with information. The main contribution of BPMN software is the visualization and the possibility of interconnection of models into more comprehensive units. These tools are often used as a foundation for the subsequent mediation of software development. This opportunity is used mainly in large organizations, which require somehow to capture the reality of the operation in the organization using the process model.

There are many BPMN softwares, so it is necessary to focus on selection of the one suitable for this work. Each BPMN software operates a bit differently and also enables diverse work with information. It all brings the necessity of requirements determination for the selection of a BPMN modeling tool. It is necessary to determine in advance as accurately as possible what our goal is and what we expect from the software. Furthermore, determine the detail level of information and data that the models should contain, define the information and data that need to be modeled and, last but not least, test and compare selected software whether they operate according to user ideas and whether they can handle the required amount of data. Nowadays, it is also important to consider that some BPMN software only operates as an online application, which can create problems when modeling organization's internal protected information and data.

Comparative criteria of BPMN modeling tools for the needs of this thesis were considered from several perspectives, mainly because the goal of modeling in this thesis is not only to create a classic BPMN process model, but a STAMP-compatible representation. Given that BPMN software was selected as the most suitable tool for creating extended process models based on STAMP, it is subordinate to additional requirements than when creating

classic BPMN models. The individual perspectives describing the criteria for the selection of BPMN software are divided for clarity and orientation as follows:

- **Functional perspective**

The functional perspective provides criteria in terms of efficiency and the possibility of creating models. It can be said that it determines whether the software is user-friendly and whether it contains all the necessary objects for creating process models. Furthermore, the functional perspective brings requirements for the environment where the models will be created. More specifically, whether it is an online or desktop application. Due to the type of the information and data obtained from the CAA, desktop application is strongly preferred, because an online application would not meet the CAA requirements for data protection. From the functional perspective, separate issue was whether the software is freeware or payware, strongly preferring freeware solutions due to limited resources for this work.

- **Process perspective**

The process perspective is to determine whether the creation of processes and subprocesses is possible. It then studies whether it is possible to interconnect or follow up processes and whether the creation of processes in the software is suitable for the needs of the organization, in this case for the CAA. Specifically, it was necessary to test whether the software allows the creation of multiple levels of subprocesses.

- **Organizational perspective**

The organizational perspective brings criteria in terms of roles, which are responsible for individual activities throughout the process. It is therefore necessary to be able to assign the role well to the activity. Based on STAMP, together with the requirements of the CAA, it was also necessary to ensure that the software allowed the creation of a certain role library. The library brings better orientation in roles as well as facilitates work with them.

- **Data perspective**

The data perspective in this case brings criteria especially from the point of view of the STAMP. It is necessary to input data into the BPMN software. These data are based on the standard control loop, but also, for example, information about

control actions or added information about roles. Apart from these data, it is necessary to consider other types of information that would come from the CAA, such as references to documents.

- **Performance perspective**

The performance perspective creates requirements for a certain level of BPMN software interoperability. In this case, it was important to pay attention to the format in which the software allows the import and export of data, because to further work with data from models, it is necessary to have the models in a certain language, such as Extensible Markup Language (XML). In this regard, it can also be mentioned that in this case it is advantageous to use open source software, because using STAMP with a tool that was not originally designed for the purpose may lead to the need of the tool extension or at least a non-standard way of using it. An important requirement is also that BPMN software must be stable and exhibit good performance even with larger amount of data. Its performance and stability should not decline.

5.2 Comparison of modeling tools

In the previous chapter, the issue of requirements for the selection of a suitable BPMN modeling tool for the needs of this thesis was described in detail. After defining these requirements, it was necessary to search for existing BPMN software and select some convenient ones for further research. The software was searched through various websites, where existing BPMN software was listed with a short description of its features. Based on these descriptions, some softwares were selected and further studied. The selected BPMN softwares specified in Table 1, were installed on an ordinary user computer and a new project was created. A test part of the documentation was modeled in each BPMN software. During the modeling of the test part of the documentation, the capabilities of each BPMN software were verified and then these capabilities were compared with predetermined criteria using the table. After testing all selected BPMN modeling tools, an overall software comparison was performed. The comparison result of the studied BPMN software was the selection of the suitable tool for modeling the processes of a selected part of the process documentation of the CAA according to STAMP, to work within the further development phases. This selected modeling tool was Bonitasoft.

Table 1 contains eight selected BPMN softwares (Modelio, Bizagi, Bonitasoft, Camunda, Adonis:CE, Cubetto, ARIS Express, BeePMN). These softwares have been studied based on the previously mentioned requirements. The requirements are summarized in the table into the main points, which are: Free Software, Downloadable, Export XML, Subprocesses, Role Library, Other Descriptions and Stability. Thus, the requirements determine whether the software is suitable or unsuitable. The last point is Decision. It shows the final decision for the most suitable software (Bonitasoft). Positive results are checked in the table cells with a green tick and negative results with a red cross. For software that did not meet some of the first requirements, no further requirements were studied, so some cells in the table are empty.

Table 1: Result of comparison of BPMN modeling tools

BPMN Software / Requirements	Free Software	Downloadable	Export XML	Subprocesses	Role Library	Other Descriptions	Stability	Decision
 Modelio the open source modeling environment	✓	✓	✓	✓	✗	✓		✗
 Bizagi	✓	✓	✓	✓	✓	✓	✗	✗
 Bonitasoft	✓	✓	✓	✓	✓	✓	✓	✓
 Camunda	✓	✓	✓	✓	✗	✓		✗
 ADONIS:CE Your free BPM Tool	✓	✗						✗
 Cubetto	✗	✓	✓	✗				✗
 ARIS Express	✓	✓	✗					✗
 BEEP M N	✗	✗						✗

5.2.1 Bonitasoft

Bonitasoft is a company from France, which has been focusing on building the BPMN application platform since 2009. Their tool has recently a very good position, thanks to high-quality and rapid development and a relatively simple approach to modeling processes. The Bonitasoft platform has open source code and consists of several components. The basic component is a BPMN modeling tool called Bonita Studio. Bonita Studio is a downloadable software that allows the user to graphically display and subsequently edit processes according to BPMN. [24][25]

After Bonita Studio is downloaded and installed, it is possible to open this BPMN modeling tool and start creating a new process model. After opening this tool and selecting to create a new diagram, we can see the layout of panels and windows on our computer screen, which is shown in Figure 8.

Figure 8 shows a basic view of Bonita Studio when creating process models. At the top there are two basic toolbars. Below are several panels or windows, which are marked with a red border and numbered from 1 to 4.

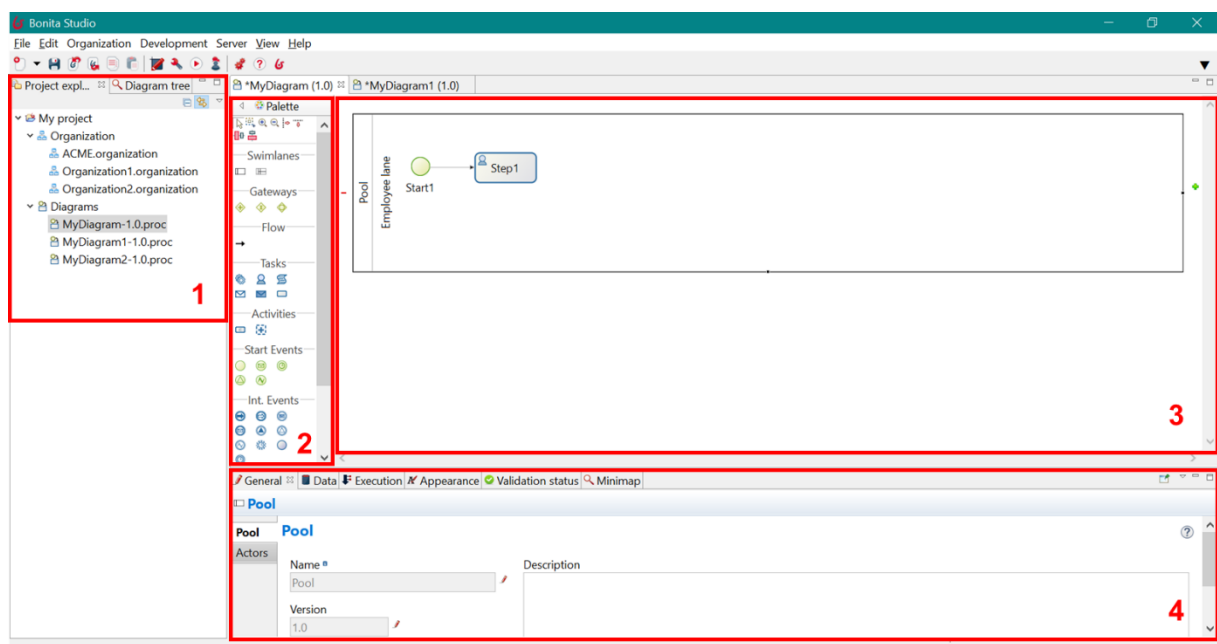


Figure 8: Layout of panels and windows in Bonita Studio

In panel number 1 there is the Project explorer, where all created projects are listed, whether they are diagrams, organizations or other created projects. In this panel we can also switch to the Diagram tree, where all pools with other objects from the selected

open diagram are listed. Panel number 2 is a Palette with graphic objects that are used during BPD creation. In window number 3 there is a workspace where process models are created and are arranged in individual pools. Panel number 4 allows work with individual objects that are in the diagram. If any graphic object from the diagram is marked, then the General, Data, Execution and Appearance tabs show all details of the selected object, which can be further edited. The other two tabs in this panel are Validation status and Minimap. Validation status checks the syntax validity of the proposed process model and Minimap displays a miniature of the model, in which it is possible to locate a specific part of the model using a magnifying glass. This part is then seen in detail in window 3.

The Palette in Bonita Studio contains graphic objects, which are shown in Figure 9. Those circled in red are objects needed for modeling processes according to STAMP, so it is advisable to mention what their functions are and when it is appropriate to use them.

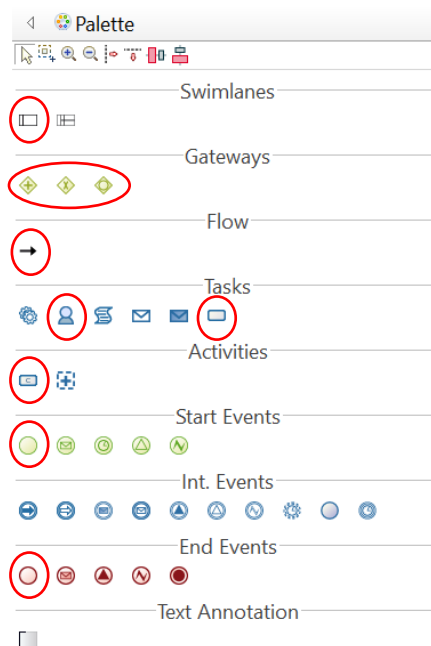





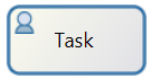
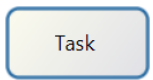
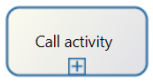




Figure 9: Palette of BPMN graphic objects

Table 2 describes the functions and uses of the circled BPMN objects from Figure 9. The table consists of four columns. The first indicates the category to which the object belongs. The second column shows the graphic sign of the object, and the third column shows the name of the graphic object. The last fourth column describes the functions of each object.

Table 2: BPMN object functions [26]

Category	Object sign	Object type	Function
Swimlanes		Pool	A pool bounds a process and forms a container for the individual processes in a diagram.
Gateways		Parallel gateway (AND)	In this gateway, all inputs must be received before a process can continue, and all outputs will be triggered simultaneously.
		Exclusive gateway (XOR)	This gateway must ensure that only one input will reach the gateway and only one output will be triggered. This gateway requires to determine a condition if it has several outputs.
		Inclusive gateway (OR)	This gateway waits for an input from all active path, and than activates an outgoing transition. If there are several outgoing transitions, it is necessary to determine a condition.
Flow		Transition	It represents sequence flow and transitions arrows are used to connect all graphic object in a diagram.
Tasks		Human task	A human task is an activity in a process and has an assigned actor who performs the activity.
		Abstract task	An abstract task is an activity, which is used as a placeholder for more specific type of task.
Activities		Call activity	It calls a subprocess, a process flow passes from the call activity to the subprocess and when the subprocess is complete, the flow returns back to the call activity.
Start Event		Start	It indicates the start of a process.
End Event		End	It indicates the end of a flow in a process.

5.3 Selection of CAA process documentation

The CAA's process documentation describes the processes that take place within the activities of CAA. These processes are described in directives and manuals, which together form the process documentation. The documentation, therefore, includes various types of processes from administrative to technical. The entire CAA documentation is in the form of a text description of the processes, so it was necessary to create the whole process model in the BPMN modeling tool and apply STAMP to it. Since the process documentation of CAA is not processed into any graphical algorithmic form, the creation of process models is more demanding, because text documents do not always provide clear views of the situation.

The process documentation of CAA is very extensive and includes many processes. For the needs of this work, it was necessary to model the process documentation, but due to its current extent and processing, it was not possible to process it into models in its entirety. A suitable solution was to select only a part of it and model it to show the next steps of the purposal of safety data collection and processing based on the theory of STAMP for civil aviation authorities.

It should be added that due to the validation cooperation with CAA of the Czech Republic, it was appropriate to select the processes of CAA CR, but the proposal for the safety data collection and processing is intended for all civil aviation authorities.

The work deals with the topic of collection and processing of safety data, so it was appropriate to select directives that include the processes dealing with this topic. Thus, two documents were selected for the modeling, namely CAA Directive – 331: Safety information processing (Směrnice ÚCL – 331: Zpracování informací o bezpečnosti) [15] and Chapter 4, Inspecting staff manual: Procedures for continued oversight of AOC holders (Hlava 4, Příručka inspektora: Postupy pro průběžný dozor nad držiteli AOC) [5].

CAA Directive – 331: Safety information processing describes the processes related to the processing of safety data. In particular, this directive deals with the activities of SAG, as well as the processing of initial reports within the SAG processes and the responses to received occurrence reports.

Chapter 4, Inspecting staff manual: Procedures for continued oversight of AOC holders describes the processes that deal with the continued oversight of Air Operator Certificate (AOC) holders. Specifically, it deals with responsibility for continued oversight, oversight

program, oversight planning cycle, procedures for conduct of audits and inspections, and evaluation of operational safety risk management process of an operator.

Both documents are, therefore, related to the topic of the thesis. The first informs about the safety information processing at the civil aviation authority and the second deals with the continued oversight of AOC holders, from which the authority collects data and further processes and subsequently analyzes them.

5.4 CAA process models

This chapter details process models proposed according to the theory of STAMP. The models are based on the selected parts of CAA's process documentation, which are CAA Directive – 331 and Inspecting staff manual, as already mentioned in the previous chapter. Both the directive and the manual provide the reader with a description of the process, along with other necessary information. Based on these two selected text documents, two relatively extensive process models were created in Bonita Studio. Given the fact that CAA Directive – 331 and the Inspecting staff manual are internal confidential documents, the thesis contains only a part of each process model, where all performed operations are described and explained. Together with these analyzed parts of the models, the following subchapters also show the extracted text parts from both documents, which relate to selected analyzed parts of the process models. The text document is presented here to compare and explain the problematic moments that may occur during modeling, but also in order to indicate the advantages the process model brings.

Parts of the process models and documents were chosen so to not be too complex to understand and not too bounded by the context of the whole document. Without this choice of process parts, it could lead to limited understanding of other operations. The second aspect was to choose such parts of the models that can help explain the future use of the whole proposal of this thesis.

Analyzed part of the directive's model was chosen because it shows the usual administrative activity, which is very common at the authority. Simultaneously, this part of the model is not difficult to understand. And analyzed part of the manual's model was selected because it shows the interaction between CAA and the organizations. It is therefore possible to see that the processes, which are mapped in the CAA

documentation, also include some activities for which other organizations are responsible.

5.4.1 CAA Directive – 331: Safety information processing

The selected part of the directive (Example 1) deals with SAG meetings. This is one complete article from the directive; the article, which specifically refers to activities that can be seen in the analyzed part of the process model in Figure 10. Given that the complete process model was created according to the entire directive, the selected part of the directive used in this section as example contains not all information, which is in the presented analyzed part of the process model, and vice versa. Thus, analyzed part of the model and selected part of the directive are not exactly the same, but missing information is contained in another part of either the model or the directive. The process model in some aspects provides more information than the directive, because querying the experts was used during the modeling.

Example 1 – part of CAA Directive – 331:

“Article 9 – SAG meeting

(Článek 9 – Jednání SAG)

1. The group meets when necessary, usually once per calendar month at a pre-scheduled date. If an immediate response to a safety issue is required, it is summoned by SAG manager without delay. An extraordinary meeting can be initiated by the CAA director.

(Skupina se schází na jednání dle potřeby, obvykle jedenkrát za kalendářní měsíc v předem známém termínu. V případě nutnosti okamžité reakce na bezpečnostní problém je neprodleně svolána vedoucím SAG. Mimořádné jednání může iniciovat i Ř/ÚCL¹.)

2. There is no minimum participation required. However, in case of repeated unexcused absences, the SAG manager may initiate negotiations and require redemption measures from division director responsible for the group to be suitably and effectively staffed.

(Minimální účast není stanovena. Na základě opakované neomluvené nepřítomnosti však může vedoucí SAG iniciovat jednání a nápravu u ředitele dané

¹ CAA Director (ředitel ÚCL)

sekce, který je odpovědný za to, že je skupina pro jím řízené oblasti vhodně a efektivně obsazena.)

3. As first agenda point there shall be appointed the program approval with each member or participant having the opportunity to express disagreement, request addition or cancellation of an agenda point.

(Prvním bodem jednání je schválení programu, každý člen nebo účastník má v tuto chvíli možnost vyjádřit nesouhlas, doplnit nebo požádat o zrušení některého z bodu jednání.)

4. Each agenda point addressing a specific issue shall have an official conclusion. Or, alternatively, the agenda point can lead to a task with specified responsibility and deadline.

(Každý bod jednání, který řeší konkrétní problém, musí mít oficiální závěr. Případně z takového bodu jednání může vzejít úkol s danou odpovědností a určeným termínem splnění.)

- a. Such tasks are obligatory for the SAG members and are limited to operation of Group's processes. Conceptual tasks reaching beyond this Group as well as recommendation of next steps in order to address a potential safety issue are presented by SAG manager to the management meeting. The management meeting decides on further procedure and its form. SAG is informed by the Group manager.

(Tyto úkoly jsou závazné v rámci členů SAG a jsou omezené jen pro účely fungování procesů skupiny. Konceptní úkoly nad rámec skupiny předkládá vedoucí SAG vhodnou formou poradě vedení, jakožto doporučení dalšího postupu pro řešení možného bezpečnostního problému. Porada vedení rozhodne o dalším postupu a jeho formě. SAG je následně informován prostřednictvím vedoucího skupiny.)

- b. Tasks are formally assigned by CAA director signing the approved meeting minutes.

(Úkoly jsou formálně zadány až s podpisem schváleného zápisu z jednání ze strany Ř/ÚCL.)

- c. SAG manager keeps record of tasks from Group meetings. Report on status of open tasks is part of every Group meeting.

(Evidenci úkolů z jednání skupiny vede vedoucí SAG. Zpráva o stavu otevřených úkolů je součástí každého jednání skupiny.)

5. The meeting minutes are recorded by the minute clerk assigned by SAG manager. Draft of the meeting minutes is shared with meeting members without any delay, if possible within 5 working days after the meeting.
(Zápis z jednání vyhotovuje zapisovatel, který je určen vedoucím SAG. Návrh zápisu je sdílen se členy a dalšími účastníky jednání v nejkratším možném čase, ideálně do 5 pracovních dnů po skončení jednání.)
6. Any comments on the draft shall be consulted by the minute clerk with SAG manager. If comments cannot be accepted, the submitting party shall be informed about reasons of their rejection.
(Případné připomínky k zápisu konzultuje zapisovatel s vedoucím SAG, pokud není možné připomínce vyhovět, je navrhovatel srozuměn s odůvodněním.)
7. After comments are incorporated, the meeting minutes is submitted to CAA director for approval. SAG members and participants are informed of its approval.
(Po zapracování všech připomínek je zápis s i přílohami předložen řediteli ÚCL ke schválení. O jeho schválení jsou členové SAG a účastníci jednání informováni.)" [15]

Analyzed part of the model in Figure 10 consists of two pools. The first pool, entitled *Procedure of SAG meeting*, is part of the general level of the whole process. This entire level consists of Call activity objects marked with the (+) sign, which means that each of these activities hides a subprocess underneath it. One such subprocess is shown in the second pool, which has the same name as the third activity in the general level part, namely *Taking the minutes of SAG meeting*. In the second pool are the Human task objects, which are the final activities that have defined responsibility or role. However, if required, it is possible to create another subprocess in the subprocess to avoid unnecessarily complex activity maps. In the second pool, there are also Gateways, which are used to split or merge the flow or to direct it according to the specified condition. Events Start and End are typically used to start and end the process.

As written above, the whole process model of the directive consists of several pools, which mostly represent subprocesses of Call activity objects. In Bonita Studio, after selecting a certain Call activity, the Process to call option appears in the General tab of the fourth panel, as described in the Bonitasoft chapter, and here it is possible to find the name of the pool that represents the subprocess of the selected Call activity (Figure 11). After selecting it, the objects are connected.

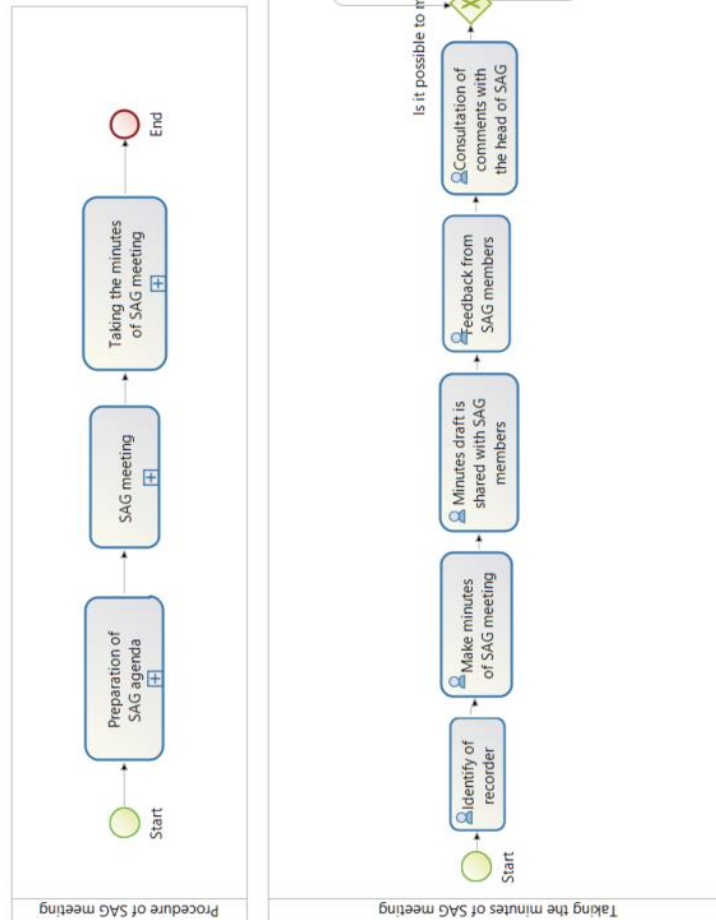


Figure 10: Part of the process model of CAA Directive – 331

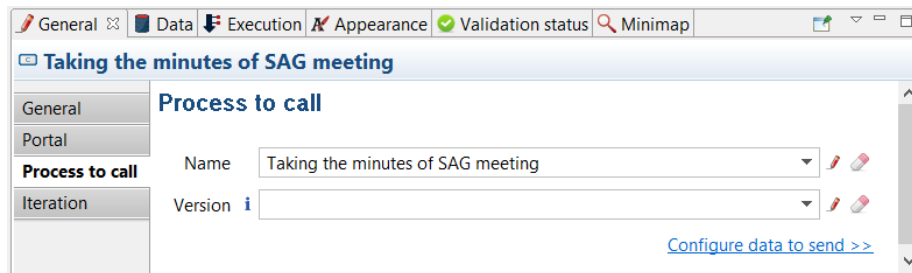


Figure 11: Process to call – subprocess

The process model of the directive is modeled according to the approach of STAMP, specifically from the point of view of STPA analysis. This means that control structure of the system processes from the directive was modeled using feedback control loops. These loops are not directly graphically represented in Bonita Studio, but the data that the loop contains is saved and linked by means of other BPMN software functions. Each final activity or Human task represents a Controlled Process in the control loop. Its Controller is then added as an Actor in Bonita Studio. Actor is added to a specific highlighted task by selecting Actors option in the lower panel number 4 in the General tab (Figure 12), as described in the Bonitasoft chapter.

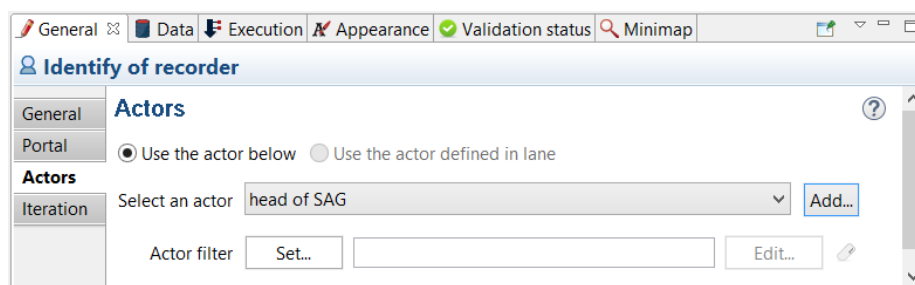


Figure 12: Actors – controller

The next step during creating the model was to define unsafe control actions according to STPA. Unsafe control action can be understood as dangerous deviations from the correct control of individual activities so, for the sake of practicality in this thesis, unsafe control action is called deviation. It can be seen from the STPA chapter that there are four types of deviations, namely:

- Deviation 1 = control action not provided,
- Deviation 2 = control action provided hazardously (incorrectly),
- Deviation 3 = control action performer too early, too late, or in the wrong order,
- Deviation 4 = control action lasting too long or is stopped too soon.

Deviations were recorded in Bonita Studio as follows. After selecting and highlighting a task and moving again to the lower panel number 4, where it is possible to select the Local variables option in the Data tab, we can add and write deviations to the highlighted activity (Figure 13). Local variables allow to write the deviation using a maximum of 50 characters, and underscore characters must be used instead of spaces. However, 50 characters ensures that deviations are not too long and complicated. It is necessary to write the deviation to well understand and explain the problem.

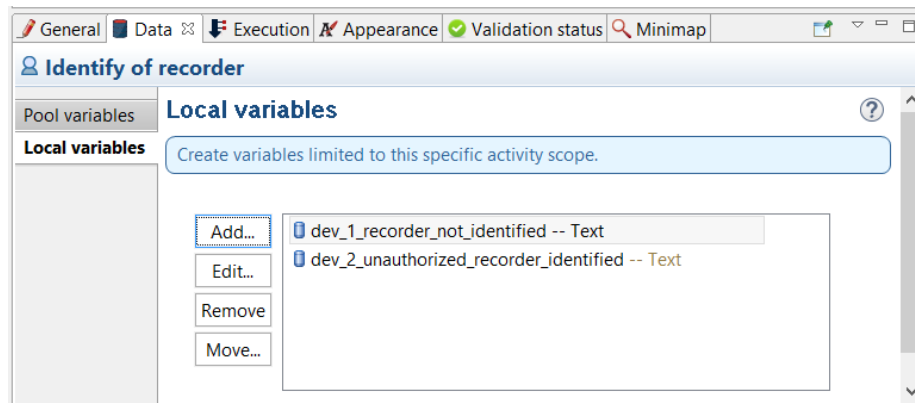


Figure 13: Local variables – deviations

Because both the controllers and the deviations, which are recorded directly in Bonita Studio, are difficult to illustrate here, a table has been created for the selected part of the process model in Figure 10 to provide this information. Table 3 lists all the final activities (Human task) from Figure 10 and each has assigned the controller (Actor) which, based on system knowledge and feedback from previous activities, controls the controlled process to achieve the required state. Sensors and Actuators, which are also part of the control loop, are not mentioned in the process models of this work, because it is not necessary to propose the model to such a level of detail. It would involve a more extensive analysis of the system, where it would be necessary to get acquainted in detail with individual activities. The next four columns of the table describe possible existing deviations for each of the activities. Not every controlled process must meet all conditions for all four types of deviations to occur. For some activities, some types of deviation would not make sense and would therefore have no effect. In such cases, a dash is written in the table instead of deviation.

Table 3: Actors and deviations of individual activities from Figure 10

Taking the minutes of SAG meeting					
Task (Activity)	Actor	Deviation 1	Deviation 2	Deviation 3	Deviation 4
Identify of recorder	Head of SAG	Recorder not identified	Unauthorized recorder identified	-	-
Make minutes of SAG meeting	Recorder	Minutes of SAG meeting not made	Minutes of SAG meeting made incorrectly	-	-
Minutes draft is shared with SAG members	Recorder	Minutes draft not shared with SAG members	Minutes draft is shared with unauthorized persons	Minutes draft is shared late	-
Feedback from SAG members	SAG member	No feedback from SAG member	Incorrect feedback	-	Feedback lasting long
Consultation of comments with the head of SAG	Recorder	Non-consultation of comments with the head of SAG	Consultation incorrectly	-	-
Processing of comments	Recorder	Non-processing of comments	Processing comments incorrectly	-	Processing of comments lasting long
Proposer is informed about reasons	Head of SAG	Proposer not informed about reasons	Proposer informed incorrectly	-	-
Submission of minutes to the director of CAA	Head of SAG	Non-submission of minutes to CAA director	-	Minutes submitted late	-
Approval of minutes	CAA Director	Disapproval of minutes	Minutes incorrectly approved	-	-
Informing SAG members about minutes approval	Head of SAG	SAG members not informed about minutes approval	Informing SAG members about minutes approval incorrectly	-	-

5.4.2 Chapter 4, Inspecting staff manual: Procedures for continued oversight of AOC holders

The selected part of the manual (Example 2) deals with findings and corrective actions. The whole chapter in the manual is quite extensive, so there is only the part that specifically relates to activities that can be seen in the analyzed part of the process model in Figure 14. Given that the complete process model was created according to the entire manual, it is possible that the selected part of the manual used as example in this chapter will not contain all information, which is in the analyzed part of the process model and vice versa. Thus, analyzed part of the model and selected part of the manual may not be exactly the same, and the missing information may be contained in another part of either the model or the manual. The process model can also provide in some aspects more information than the directive, because querying the experts was used during the modeling.

Example 2 – part of Inspecting staff manual:

"Findings and corrective action – Procedures for treatment of findings discovered by the CAA CR within the continued oversight of AOC holders
(Nálezy a nápravná činnost – postupy pro práci se zjištěnými nálezy v rámci průběžného dozoru)

Operator shall implement corrective action for discovered findings of Level 2 according to below mentioned point (b) within a period not exceeding 3 calendar months. This period begins on the day of acquaintance with the protocol (signature of protocol or postal return receipt). Operator may raise written objections to the findings within 15 days from the date of report delivery, and this appeal does not affect extension of deadline for implementation of corrective action.

(Provozovatel musí provést realizaci nápravné činnosti zjištěných nálezů úrovně 2 dle níže uvedeného bodu (b) ve lhůtě, nepřesahující 3 kalendářní měsíce. Lhůta začíná dnem seznámení se s protokolem (podpis protokolu, nebo poštovní vratka o doručení). Provozovatel může proti nálezům podat písemné námitky do 15ti dní ode dne doručení protokolu, toto odvolání ale nemá vliv na prodloužení lhůty pro realizaci nápravné činnosti.)

Inspectors of OOLD/SL² follow the below stated system for Level 1 and Level 2 findings analysis in terms of its safety. Findings shall be recorded into protocol by the inspector as specified in article 4.1.5.3.

(Inspektoři OOLD/SL mají k dispozici níže uvedený systém pro analýzu nálezů úrovně 1 a úrovně 2 z hlediska jejich bezpečnostního významu. Nálezy zaznamenává inspektor do protokolu, jak je uvedeno výše v ustanovení 4.1.5.3.)

(a) Level 1 finding:

(Nález úrovně 1)

Level 1 findings are issued by respective OOLD/SL inspector after identifying a significant non-compliance with Regulation (EC) No. 216/2008 and its implementing regulations, with organization's procedures, and manuals, conditions of issued approvals, certificates or approved special operations which might seriously endanger flight safety.

(K vydání nálezu úrovně 1 přistoupí příslušný inspektor OOLD/SL poté, co zjistí významný případ nedodržení příslušných požadavků nařízení (ES) č. 216/2008 a jeho prováděcích pravidel, postupů a příruček organizace nebo podmínek oprávnění, osvědčení nebo schváleného zvláštního provozu, jež závažným způsobem ohrožuje bezpečnost letu.)

(...)

In case of Level 1 findings, the OOLD/SL inspector must immediately inform the OOLD/SL director. CAA CR management decides if appropriate corrective actions are to be implemented in accordance with §91(2) of Act No. 49/1997 Coll. leading to a ban or restriction of activities. If necessary, the CAA CR management implements corrective actions leading to AOC invalidation, restriction or suspension depending on severity of Level 1 finding until the operator's organization has successfully implemented corrective actions.

(V případě nálezů úrovně 1, musí inspektor OOLD/SL neprodleně oznámit tuto skutečnost řediteli OOLD/SL. Vedení ÚCL ČR následně rozhodne, zda přijme odpovídající opatření v souladu s §91(2) zákona č. 49/1997 Sb., vedoucí k zákazu nebo omezení činnosti a v případě potřeby přijmout opatření, kterým zruší platnost AOC, nebo tuto platnost zcela nebo částečně omezí nebo pozastaví

² Commercial air transport department/Flight Division (Oddělení obchodní letecké dopravy/Sekce letová)

v závislosti na míře závažnosti nálezu úrovně 1, dokud organizace provozovatele neprovede úspěšné nápravné opatření.)

(b) Level 2 finding:

(Nález úrovně 2)

Level 2 findings are issued by respective OOLD/SL inspector after identifying a non-compliance with Regulation (EC) No. 216/2008 and its implementing regulations, with organization's procedures and manuals, conditions of issued approvals, certificates, that can jeopardize safety of performed flights.

(K vydání nálezu úrovně 2 přistoupí příslušný inspektor OOLD/SL poté, kdy zjistí neshodu s příslušnými hlavními požadavky nařízení (ES) č. 216/2008 a prováděcích pravidel k tomuto nařízení, s postupy organizace a příručkami, s podmínkami vydaných schválení, osvědčení, která by mohla ohrozit bezpečnost prováděných letů.)

Procedures for work with the above stated Level 1 findings and in particular procedures for work with the Level 2 findings identified by OOLD/SL inspectors within the continuous surveillance of AOC holders are included in Directive CAA-SL-049-n-17. Procedures for work with findings, in particular of Level 2, contained in this Directive are mandatory for both AOC holders and OOLD/SL inspectors.

(Postupy pro práci se zjištěnými nálezy výše uvedené úrovně 1 a zejména postupy pro práci se zjištěnými nálezy úrovně 2, které byly zjištěny inspektory OOLD/SL v rámci průběžného dozoru držitelů AOC jsou obsahem směrnice CAA-SL-049-n-17. Postupy pro práci se zjištěnými nálezy, zejména úrovně 2, které jsou obsahem této směrnice jsou závazné jak pro držitele AOC, tak pro inspektory OOLD/SL.)

The above Directive includes the following Appendices for work with identified Level 2 findings:

(Výše uvedená směrnice obsahuje následující přílohy pro práci se zjištěnými nálezy úrovně 2:)

- | | |
|--------------------|--|
| Appendix 1 | Operator's corrective action plan – prepared by AOC holder |
| Appendix 1A | Evaluation of CAA CR corrective action plan – prepared by OOLD/SL inspectors |
| Appendix 2 | Proof of implementation of operator's corrective action – prepared by AOC holder |

Appendix 2A	Evaluation of implementation of CAA CR corrective action – prepared by OOLD/SL inspectors
Appendix 3	Request for extension of deadline for corrective action implementation – prepared by AOC holder if applicable
Appendix 3A	CAA CR statement to request for extension of realization deadline – prepared by OOLD/SL inspectors
(Příloha 1	<i>Plán nápravné činnosti provozovatele – zpracuje držitel AOC</i>
Příloha 1A	<i>Vyhodnocení plánu nápravné činnosti ÚCL ČR – zpracují inspektoři OOLD/SL</i>
Příloha 2	<i>Prokázání realizace nápravy/nápravného opatření provozovatelem – zpracuje držitel AOC</i>
Příloha 2A	<i>Vyhodnocení realizace nápravy/nápravného opatření ÚCL ČR – zpracují inspektoři OOLD/SL</i>
Příloha 3	<i>Žádost o prodloužení lhůty na realizaci nápravy/nápravného opatření – zpracuje držitel AOC dle použitelnosti</i>
Příloha 3A	<i>Stanovisko ÚCL ČR k žádosti o prodloužení lhůty realizace – zpracují inspektoři OOLD/SL</i>

(c) Instructions for processing Appendix 1A by OOLD/SL inspectors

(Pokyny pro zpracování Přílohy 1A inspektory OOLD/SL)

OOLD/SL inspectors record evaluation of operator's corrective action plan into Appendix 1A. The corrective action plan is submitted by Operator in form of Appendix 1.

(Inspektoři OOLD/SL zaznamenávají do Přílohy 1A výsledky posouzení a vyhodnocení plánu nápravné činnosti (corrective action plan) provozovatele, který provozovatel předkládá formou zpracované Přílohy 1.)

(...)

OOLD/SL inspectors shall perform this evaluation of corrective action plan for each finding within a maximum of 14 calendar days and submit Appendix 1A back to the Operator by e-mail.

(Inspektoři OOLD/SL musí toto posouzení a vyhodnocení předloženého plánu nápravné činnosti ke každému konkrétnímu nálezu provést během nejvýše 14-ti kalendářních dní a zaslat Přílohu 1A obratem zpět provozovateli krátkou cestou e-mailem.)

(...)

(d) (...)

(e) (...)

(f) Extension of deadline for corrective action implementation

(Prodloužení lhůty na realizaci (implementaci) nápravy/nápravného opatření)

If it is necessary to extend the deadline for corrective action implementation, the OOLD/SL inspectors proceed in accordance with provision (6) of Directive CAA-SL-049-n-17, which is an integral part of ISM.

(V případě nutnosti nebo potřeby prodloužit lhůtu na realizaci nápravy/nápravného opatření, postupují inspektoři OOLD/SL v souladu s ustanovením (6) směrnice CAA-SL-049-n-17, která je nedílnou součástí ISM.)" [5]

Analyzed part of the model in Figure 14 consists of two pools. The first pool, called *Continued oversight*, represents the general level of the whole process. This entire level consists of Call activity objects marked with the (+) sign, which means that each of these activities hides a subprocess underneath it. One such subprocess is shown in the second pool, which has the same name as the penultimate activity in the general level, namely *Dealing with findings and corrective actions*. In the second pool are the Human task objects, which are the final activities that have a defined responsibility or role. If required, it is possible to create another subprocess in the subprocess to avoid unnecessarily complex activity maps. In the second pool, there are also Gateways, which are used to split or merge the flow or to direct it according to the specified condition. Events Start and End are typically used to start and end the process. Both Start and End can be used multiple times in one pool, but each additional Start or End object should have its own start or end state. For example, if we use End twice with the same name, then the system understands it as the same end state [27].

As written above, the whole process model of the manual also consists of several pools, which mostly represent subprocesses of Call activity objects. The creation of the subprocesses of this manual in Bonita Studio proceeded in the same way as already described in the previous subchapter.

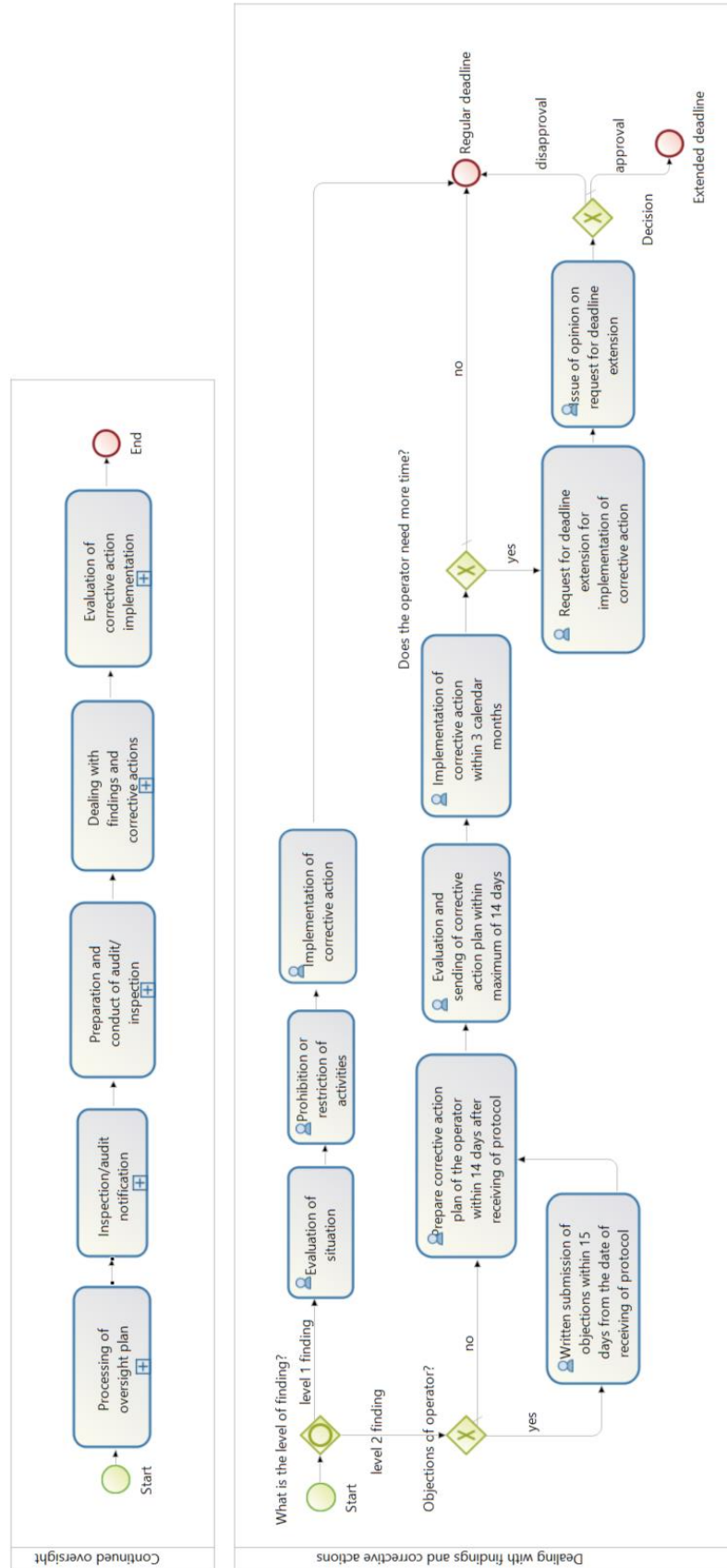


Figure 14: Part of the process model of Chapter 4, Inspecting staff manual

Table 4: Actors and deviations of individual activities from Figure 11

Dealing with findings and corrective actions					
Task (Activity)	Actor	Deviation 1	Deviation 2	Deviation 3	Deviation 4
Evaluation of situation	Director of Flight Division	Non-evaluation of situation	Evaluation of situation incorrectly	-	Evaluation of situation lasting long
Prohibition or restriction of activities	Director of Flight Division	Non-prohibition or non-restriction of activities	Option is chosen incorrectly	Prohibition or restriction performed late	-
Implementation of corrective action	AOC holder	No implementation of corrective action	Implementation of corrective action incorrectly	-	Implementation lasting long
Written submission of objections within 15 days from the date of receiving of protocol	AOC holder	Non-submission of objections within 15 days	Submission of objection within 15 days incorrectly	Objections submitted late	-
Prepare corrective action plan of the operator within 14 days after receiving of protocol	AOC holder	No corrective action plan	Corrective action plan prepared incorrectly	Corrective action plan prepared late	-
Evaluation and sending of corrective action plan within maximum of 14 days	Inspector	Non-evaluation and non-sending of corrective action plan	Evaluation and sending incorrectly	Plan evaluated and sent late	Evaluation and sending of plan lasting long
Implementation of corrective action within 3 calendar months	AOC holder	No implementation of corrective action	Implementation of corrective action incorrectly	-	Implementation lasting long
Request for deadline extension for implementation of corrective action	AOC holder	Not requesting for deadline extension	Requesting for deadline extension incorrectly	Request submitted late	-
Issue of opinion on request for deadline extension	Inspector	Non-issue of opinion on request for deadline extension	Option issued incorrectly	Option issued late	Issue of option lasting long

The process model of the manual, like the process model of the directive, is modeled according to STAMP, specifically from the point of view of STPA analysis. This means that the control structure of the system processes in the manual was also modeled using feedback control loops. The process model of the manual was created in Bonita Studio in the same way as the directive model described above, so it is not necessary to repeat the procedure of processing the model in BPMN modeling tool Bonita Studio.

As addressed in the previous subchapter, information such as controllers and deviations recorded in Bonita Studio is difficult to illustrate here, therefore a table with this information was also created. As in the previous model of the directive, Table 4 lists all final activities (Human task) with controllers (Actor) and deviations from the part of the manual process model, which is shown in Figure 14.

5.4.3 Work with selected documents and advantages of process models

The previous subchapters illustrated examples from two types of process documentation, namely the directive and the manual. As can be seen from the examples, each document has a different structure. The process modeling based on these two documents proceeded similarly, however, working with different type of document always required different orientation in its structure. Given that the CAA does not currently have any process documentation graphically visualized, it was more difficult to orientate oneself in the authority's processes. During modeling, it was necessary to get acquainted with the operation of the whole organization, including querying the CAA experts.

From the parts of the models that are also mentioned here, it is possible to see that, unlike the text documentation, the process models do not change in the structure. Thus, process models can improve the orientation of the civil aviation authority in its own processes, and this can also speed up the administrative adjustments of documents or even speed up some activities.

Besides other things, in Bonita Studio it is possible to create an Organization project, where all persons can be mapped, including their roles in the organization, and these persons are organized into working groups and subgroups. The organizational structure of persons (users) can then be interconnected with actors who are assigned to the activities in the diagram, so CAA can gain a new overview of its processes in connection with specific persons who perform individual activities.

6 STAMP-based safety data collection and processing with process models

In the previous chapter, the procedure for creating a process model according to the theory of STAMP using BPMN software based on selected process documentation of CAA was described. The created process models part of which is presented in the previous chapter, serve as a basis for the proposal of a procedure for the safety data collection and processing according to STAMP for civil aviation authorities.

The Safety Data Collection and Processing System (SDCPS) by authorities serves to generate classified information that can be further analyzed to obtain statistics and conclusions that will help prevent further accidents or incidents. The current system of evaluation of safety information operates based on monitoring certain safety indicators and their mutual comparison. These indicators mainly arise from the classification and processing of occurrences using existing standard aviation safety taxonomies. These taxonomies define terms that refer to safety occurrences from the whole aviation domain. The ECCAIRS taxonomy, or its reduced version Reduced Interface Taxonomy (RIT), is now used in the European environment. The ECCAIRS and RIT taxonomy are based on the ICAO ADREP taxonomy, which is used outside the European environment [28]. The ADREP/ECCAIRS taxonomy is currently the basis for data collection and processing at CAA.

Recently, however, new approaches to safety have emerged. One such newly developed approach is STAMP, which allows a relatively smooth transition between Safety-I and Safety-II. STAMP includes two analyses (STPA and CAST), which are based on STAMP. These two analyses deal with the problem from the systemic point of view, while the current analyses solve only the selected part of the system. STAMP therefore provides a suitable solution for improving SDCPS and thus also improving aviation safety.

CAST analysis deals with examining accidents and incidents at the system level. Given the fact that safety data are obtained mainly from occurrence reporting, it is appropriate to use the approach of this analysis. In order to find the real cause of the occurrence, it is necessary to model the safety control structure for a given type of hazard using feedback control loops. Based on the model, the control structure can then be examined in detail and its shortcomings identified.

The use of this accident analysis is very desirable due to the systemic approach, but the disadvantage is its complexity, which is caused by the need to always model the existing

control structure and then examine it in detail. For this reason, it is more beneficial to use both CAST and STPA analyses. Initially, it will be a more demanding process, but after modeling the structure according to STPA, the CAST analysis process will be facilitated and made faster. STPA analyses the hazards in the system as a whole and, like CAST, requires modeling of the control structure. Thus, STPA uses the model to examine the control structure of the entire system, where it identifies unsafe control actions that could lead to a hazardous state of the system.

After the collected data is processed into information, further research and analysis can easily take place. It follows that data processing is one of the important components of the whole analysis. In order to reduce the complexity and speed up the investigation of occurrence according to CAST, it is necessary to make the processing of collected data more efficient. If the control structure of all processes of the whole system is modeled based on process documentation, as STPA does, a process model is created with feedback control loops, in which unsafe control actions or deviations are then defined. During the processing of occurrence data for CAST analysis, it is not necessary to model the control structure of the participating parts of the system that are related to occurrences, because there will be an up-to-date model of the entire system. The deviations of individual activities then have the function of factors that could have contributed to the occurrence or even caused it directly.

Modeling the control structure of the entire civil aviation authority will reduce the complexity of processing data on occurrences that are of internal nature or that affect the CAA's activities in some way. However, because events occur mostly in operation, it is necessary to progressively model the control structure in the individual organizations that participate in aviation. The control structure of organizations should be modeled by each organization separately, according to its own process documentation. Due to the advantages of a systemic approach, the models will help organization to identify weaknesses in the system. Reduced process models of these complete process models can then be provided by the organization to the civil aviation authority when investigating occurrences that affect the organization. Alternatively, in cases where organizations are not willing or do not have a model to share, it is possible to create idealized models of organizations that can be proposed based on legislation and general information on how companies work. After modeling the control structures at organizations and at CAA, a complete process model is created, which provides a system view and enables the processing and further analysis of safety data by means of

a systemic approach. Modeling the whole process structure of an organization is exacting, and therefore models should be created preferentially in large organizations, where there is a high risk of accidents and incidents, and after then in smaller organizations. In addition to the complexity of the modeling itself, it is also necessary to mention that the process model must be regularly updated to constantly provide an up-to-date platform. This aspect of complexity must also be considered, because it brings a new function and responsibility to the organization.

For the safety data collection, processing and evaluation, SDCPS software should be created that would allow the user to process and then evaluate the data based on the procedure proposed above. Figure 15 represents a scheme in detail to show the relations between the proposed process model according to STAMP and SDCPS, which could be the foundation for the future design of SDCPS software.

In Figure 15 there are several coloured fields, and each represents a different kind of information. The blue field forms the basic proposal for the operation of the SDCPS Software. More types of information come into the blue field, which are divided by colour according to their character. SDCPS software must be able to integrate safety data with process data, which arise mainly from the process models of the authority, but also from simplified process models of aviation organizations. The safety data are in a dark yellow field and come as an initial report from the mandatory and voluntary occurrence reporting system. This data provides us fundamental information about the occurrence, such as when and where the occurrence happened, what happened, who was present, and so on. In order to be able to classify the occurrence in some way, it is appropriate to use the established ADREP/ECCAIRS taxonomy, which is commonly used today, for the basic classification of the occurrence or to determine, for example, a loss event. The ADREP/ECCAIRS taxonomy is in Figure 15 shown as light yellow field. The use of taxonomy is appropriate in terms of ensuring compatibility with other currently used systems that use taxonomy. At the same time, it will still be possible to produce established statistics based on the common taxonomy.

The next field is a green field that shows the process data. Process data are processed into process models, the creation of which was explained in the previous chapter. CAA process model consists of a control structure according to STAMP. It can be seen from the scheme that Activity corresponds to the Controlled process, just as Actor corresponds to the Controller. Deviations are created for each Activity and Deviation then present us Factors that could have contributed to the occurrence or even caused it.

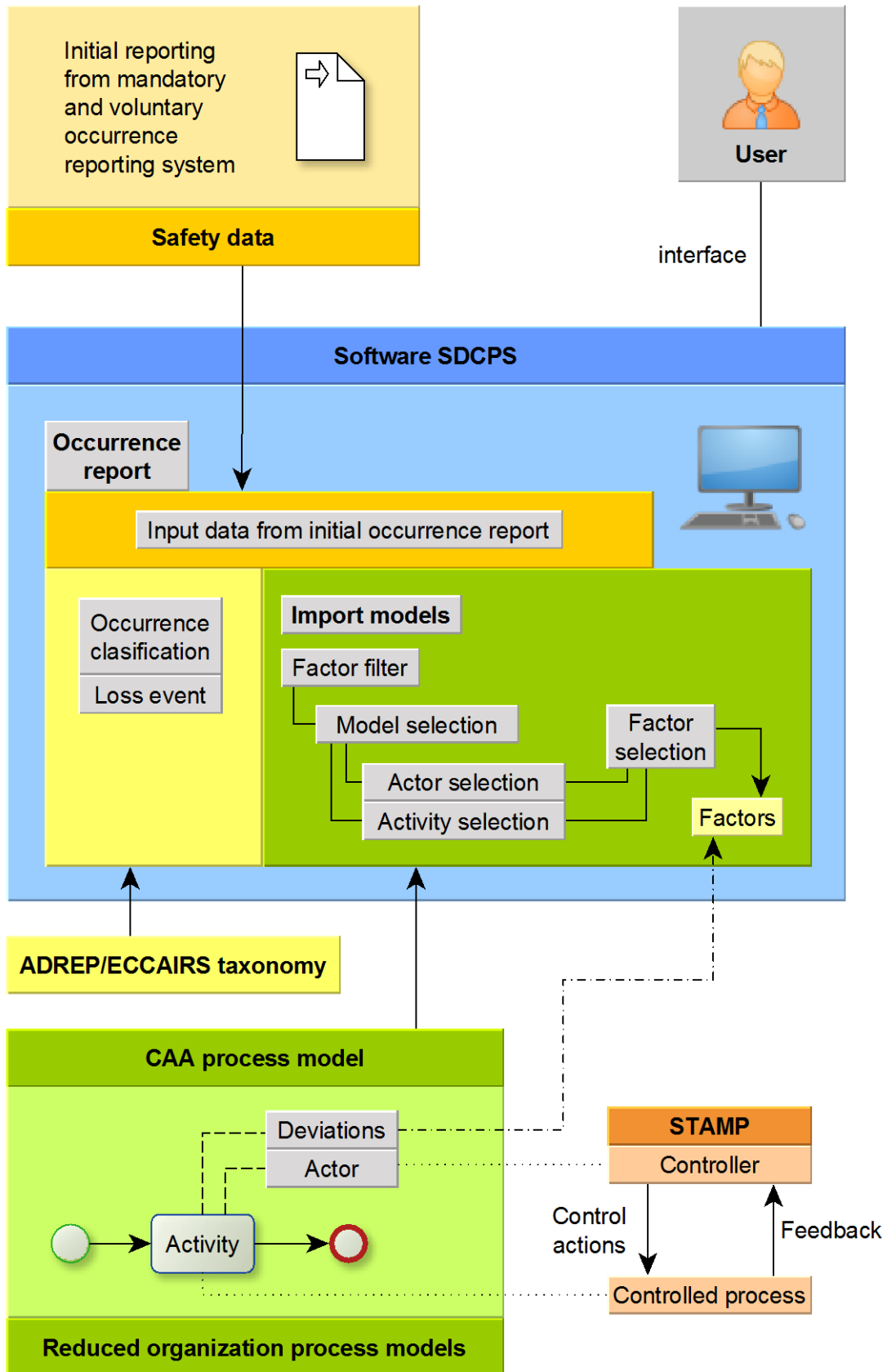


Figure 15: STAMP-based proposal of SDCPS

It is therefore necessary to import a valid current CAA model into the SDCPS Software, but also reduced models of the organizations to which the occurrence relates. Simplified process models will provide a platform for finding causal factors outside the structure of CAA. However, it is not necessary for CAA to have detailed models of organizations that include processes that are not related to safety data. Since the process models of organizations as well as of CAA can be constantly changing, it is necessary to import current models, but also to save older versions of models, so that it is always clear which version of the model was used and which version was valid at the time, when the occurrence happened. After importing all the necessary current models, it is possible to search for factors. Because there are many factors (deviations) in process models, it is necessary to somehow filter them when searching, in order to speed up and facilitate the user's work. The first filter should therefore be to select the process model in which the user wants to search for factors. For example, whether he or she wants to search in CAA model or in the model of the airport where the occurrence took place. After selecting the model, he or she could look for factors (deviations) according to the specific Activity where the error occurred or directly according to the Actor, which is responsible for a certain Activity and, therefore, for unsafe control actions. The user can then select a specific factor and classify particular occurrence. With the help of relations, the individual factors could then be connected to provide a complete scheme. Afterwards, it would be possible to see the relationships that have occurred between the individual factors and infer some knowledge about their occurrence.

The SDCPS Software approach proposed in this way will provide the user with a systemic approach to occurrences, while reducing the complexity and speeding up further data analysis. At the same time, CAA could use software to monitor and analyse problem areas or even relationships both at CAA and between CAA and organizations, and in some cases even between organizations.

When creating SDCPS software, it is also necessary to consider that this software must be compatible with current safety data collection and processing systems (such as SISel, which is now used in trial operation at CAA CR). Current systems are also used for data record and processing of received reports. This data processing is based only on the standard aviation taxonomy ADREP/ECCAIRS. Based on the taxonomy, systems then enable data sharing evaluation and, if necessary, monitoring of statistics using established safety performance indicators. Thus, systems operate based on taxonomy and other established safety performance indicators but do not include systemic

approach to safety data. But it is clear, that the transition from the Safety-I approach to the Safety-II approach will not be immediate, so it is necessary to design this new SDCPS software so that it is compatible with the currently used systems and is able to interact with them. For this purpose, separate issue may be compability of the proposed solution, because part of the occurrence classification would use new STAMP-based classification (see Figure 15), which is not compatible with current version of ECCAIRS. On the other hand, converting the terms may translate STAMP-based classifiers into ECCAIRS, althouht that would mean some loss of information due to ECCAIRS being more abstract than STAMP. Nevertheless, this would at least maintain compatibility with the existing data reporting and sharing schema.

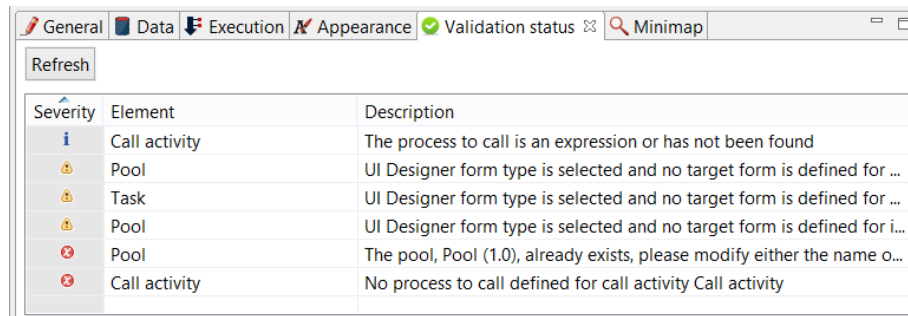
7 Validation

The proposal of the procedure of safety data collection and processing according to STAMP for civil aviation authorities, which was presented in this work, was validated to verify its functionality. The validation of the proposal took place at three levels. The first level of validation dealt mainly with the first part of the proposal, namely the creation of process models using BPMN in Bonita Studio. The second level of validation was performed through regular consultations with CAA CR members. This level focused on the creation of process models from the selected part of the process documentation of CAA, as well as on the future use of the entire proposed procedure in operation. The last (third) validation is based on the application of real data, which explains the use of the proposed procedure for safety data collection and processing in practice. All three levels of validation are described in the following subchapters.

7.1 Validation using Bonita Studio

Validation using Bonita Studio was mainly used to verify the syntax correctness of process models during modeling. Validation in Bonita Studio takes place from the point of view of BPMN verification and simultaneously to verify meeting all software requirements. Bonita Studio has Validation status tab (Figure 16) in panel number 4, as described in the Bonitasoft chapter. If this tab is open, there is a Refresh button. After pressing the button, the validation of the entire model is refreshed. In Validation status it is possible to see three columns, namely Severity, Element and Description. In the Severity column we can see three signs: blue – INFORMATION, yellow – WARNING and red – ERROR. The second Element column lists the objects affected by the validation notification, and the third Description column explains the specific validation issue.

Figure 16 is only to show how validation works in Bonita Studio. During the modeling of processes in this software, a regular check was performed using Validation status, so that there are no BPMN errors in the model.



Severity	Element	Description
i	Call activity	The process to call is an expression or has not been found
⚠	Pool	UI Designer form type is selected and no target form is defined for ...
⚠	Task	UI Designer form type is selected and no target form is defined for ...
⚠	Pool	UI Designer form type is selected and no target form is defined for i...
✖	Pool	The pool, Pool (1.0), already exists, please modify either the name o...
✖	Call activity	No process to call defined for call activity Call activity

Figure 16: Validation status in Bonita Studio

7.2 Validation by consultations with CAA CR

The second level of validation took place based on validation cooperation with CAA CR. Based on the provision of part of the process documentation, CAA was also willing to provide regular consultations, during which the accuracy of the created process models, which arose based on the provided documentation, was verified. This ensured continuous validation of the information entered into the process models and validation of the correct arrangement of this information during the modeling.

CAA CR also expressed interest in the whole topic of the proposed procedure for the safety data collection and processing according to STAMP and provided further advice and requirements, which were also considered and included in the proposal. CAA therefore evaluated this proposal of the procedure as a possible future solution of the issue and thus also provided a certain validity of this proposal.

7.3 Validation based on the use of real data

This type of validation was performed using real data, which explains how the proposed procedure would work in practice and how it would provide better information for further analysis and evaluation. For this validation, publicly available information from the aviation occurrence final reports, which can be found on the AAll CR website³, was used. Publicly available data were chosen for validation because they do not contain any confidential information and are not subject to secrecy.

In order to perform this type of validation, it was necessary to go through the occurrence final reports in detail and find such final reports with which it is possible to show well the systemic approach of the proposed procedure for safety data collection and processing

³ <https://uzpln.cz/zpravy-ln>

according to STAMP. One occurrence final report was selected, which is well related to one of the solved parts of the process models, Inspecting staff manual, and at the same time it is good to see the systemic problem. Other selected occurrences serve more as a supplement and example that the systemic problems are present in most occurrences.

The selected occurrence represents an incident that happened on August 6, 2013 at Karlovy Vary Airport. The operator of one company performed work on board the Airbus A320, which was parked on the stand of the airport area. The operator was leaving the front door and did not notice that the ground handler had pushed the airstair away. The operator fell on the apron and suffered severe injuries. [29]

Among the causes of the occurrence are listed [29]:

- non-compliance with procedures for handling of airstair,
- unauthorized manipulation of the operator with the front door,
- non-compliance with the described internal rules of all participating organizations,
- insufficient internal audit activity,
- failure to carry out oversight activities of the state authority (CAA) at the operator of Karlovy Vary Airport.

These causes indicate a systemic problem. Many factors contributed to this occurrence, and these factors come from various organizations. The causes show that oversight, both internal and external, was not carried out well and that working procedures were not followed.

The above-mentioned occurrence text represents the input safety data. Based on this information, an occurrence can be classified, or a loss event can be determined according to the ADREP/ECCAIRS taxonomy. To determine the factors according to STAMP approach, we must have process data in the form of process models. At this occurrence, it is possible to show how important a systemic approach to the investigation of the occurrence is and it is necessary to have a process model of CAA, a reduced model of Karlovy Vary Airport and a reduced model of two other participating organizations. After importing these four models, it is possible to select a specific model and search for Factors by Actor or Activity. In this occurrence, it is possible, for example, to select the reduced process model of the organization 1 (R. o. 1 p. model = Reduced organization 1 process model) where the operator worked, and according to Actor (Operator), the factor (deviation) can be found that, for example, did not check the

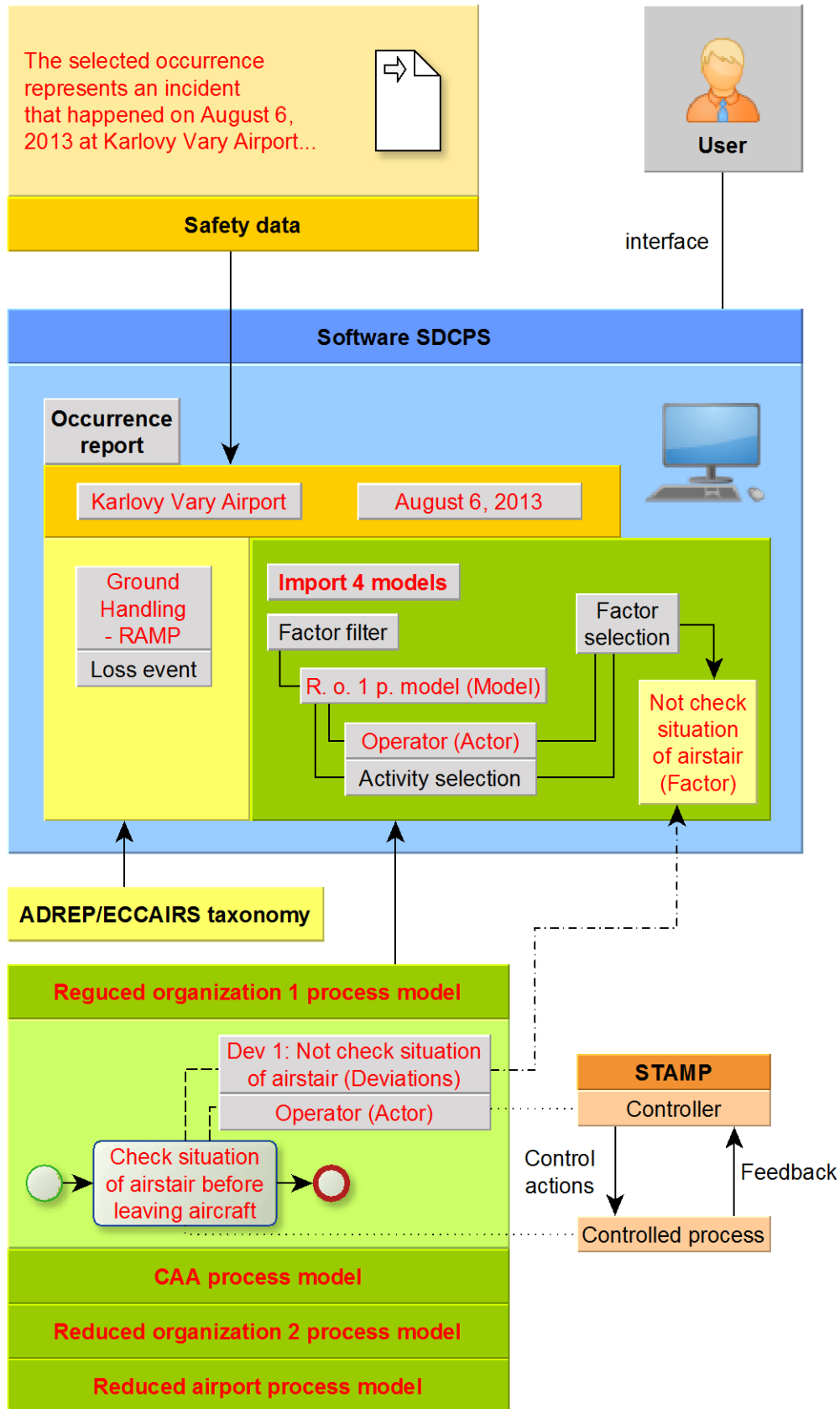


Figure 17: Validation based on real occurrence

situation of the airstair when leaving the aircraft. This example is shown in Figure 17, where the information from the occurrence is highlighted in red.

Because CAA did not perform regular oversight, it follows that a factor (deviation) from CAA environment can also contribute to the occurrence that happens in practice, so it is necessary to look for factors in these CAA processes as well. One such is, for example, regular oversight, which was also addressed in Chapter 5.

In other searched occurrences, the final reports are usually closed by one cause. For example, a common conclusion is the failure of a human factor or non-compliance with a procedure [30][31]. However, a systemic approach would find out why the procedure was not followed and what factors contributed to it. Systemic approach would not consider a failure of human factors as a root cause, but only a starting point for more elaborate investigation.

The following Table 5 provides a comparison of current and the proposed procedure of safety data collection and processing.

Table 5: Comparison of current and proposed SDCPS

	Current SDCPS procedure	Proposed SDCPS procedure
Approach	System component-base	Systemic
Factors classification	Using ADREP/ECCAIRS taxonomy	Using specific data from process models based on STAMP
Platform	No data process platform required	Data process platform based on process models
Change of process documentation	No effect	Need to process change into process models

8 Discussion

Any new approach to an issue is demanding, because it is not enough to follow the theory of approach, but it is also necessary to incorporate the new approach into the current conditions and a certain environment. It is the same with new approaches to safety. Safety-II approach is suitable for use in systems that are sociotechnical, which are almost all systems today with developing technology. However, the use of Safety-II approach techniques has a very slow onset, because in the entire functioning structure it is practically impossible to immediately change the approach and do everything differently. The transition from Safety-I to Safety-II must take place by progressively changing all the activities performed.

STAMP approach was chosen to achieve the goal of this thesis. STAMP approach is systemic, and therefore also brings many more demanding and detailed solutions than the older approaches used so far. However, STAMP brings such a solution that could significantly reduce the error rate of systems in the future and thus prevent more serious consequences.

The use of STAMP in aviation, specifically in the issue of safety data collection and processing is very desirable from the point of view that CAST analysis allows it using systemic approach. Thanks to the systemic approach, it brings many advantages but also few disadvantages for investigators. Using the control structure model, investigators can find many weaknesses in the system and reinforce all these weaknesses by changing procedures or introducing more oversight of certain activities. In addition, they can find real causes of occurrences that, according to older analyses without a systemic approach, cannot be found. On the other hand, there are many disadvantages of this approach to investigation. The investigation is more demanding because it is necessary to model the control structure in detail, which then needs to be examined in detail, and this takes a lot of time and usually involves a lot of staff in such an analysis.

The proposal of the procedure for the safety data collection and processing according to STAMP for civil aviation authorities, which is presented in this thesis, is intended to facilitate and speed up the user's work with data, which will be further analysed by a systemic approach. In order to be able to implement this procedure, a suitable solution is to create a new SDCPS software that would help its user as much as possible with the processing of safety data originating mainly from the mandatory and voluntary occurrence reporting systems.

For SDCPS software to work with STAMP systemic approach, it must have a specific data platform, from which process systemic data can be obtained. This platform consists of a process model created according to STAMP. For this modeling, it is necessary to find some software that will allow the export of inserted data and further work with them. BPMN modeling tool Bonita Studio was used in this thesis, but it is of course possible to create models in other software that meets all requirements. In order to create a complete process model of the organization, it is necessary to model all processes from the process documentation. This brings considerable problems, because the entire process flow is not always recorded in a text document at once, but there is a lot of additional information between the individual activities, which acts as a disruptive element during the creation of process models. Another problem during modeling is that the person responsible for each activity is not always precisely mentioned, so many new questions arise that may already point out a weakness of the system during modeling.

For the CAA, as well as other organizations, to create process models based on process documentation, it is likely that additional staff will need to be employed to model the organization processes, because modeling is relatively time consuming. Nevertheless, after modeling all organization's processes, it is necessary to monitor changes in the process documentation and regularly apply these changes to the existing process model. The model should always be up to date. Therefore, employees will have to continue to focus on the model and keep it up to date, so it is not just a one-time work. This need probably creates new jobs in organizations, and this is associated with new economic expenditures of the organization, which will have to cover the salary of new employees.

If a new procedure for safety data collection and processing should be put into practice, the best solution of which is to create software, then it is necessary to take into account costs of creating the software itself, but also creating an interface for importing process models created in the modeling tool outside the proposed software.

When creating SDCPS software, it is necessary to consider the compatibility between this new software and the currently used systems. Again, the problem is that it is not possible to arrange for the entire approach to aviation safety to change at one point, so we must expect a gradual change. We will ensure this change precisely by the fact that the software will be proposed and created so that it can communicate and interact with other SDCPS systems that are currently used.

The complete systemic approach to aviation safety is suitable, but STAMP itself is quite demanding, and therefore the software user should not be burdened by a detailed study of STAMP, for the needs of working with the software. The software should be created so that the knowledge of STAMP is implemented in it using knowledge technologies and the user is not burdened by complex operations.

The new approach to the safety data collection and processing should provide civil aviation authorities with a broader overview of the problematic components of the entire aviation structure. However, in addition to CAA process model itself, it is essential to have reduced process models of organizations to look for problems in other structures than CAA control structure. However, due to the complexity of modeling, it is not possible to ensure that all aviation organizations have their processes modeled at once, so it is necessary to consider that process models of organizations will be created gradually and probably first for larger organizations and then possibly for smaller ones. The second issue is to define the scope of the reduced model that the organization should provide to the authority. It is possible to have access to detailed models of organizations, but they should not expect to be provided by organizations to CAA. It is appropriate to create idealized reduced models of organizations that would be proposed based on legislation and general information on how companies work. These reduced models would be maintained by CAA.

Existing SDCPS systems operate on standard aviation taxonomies, based on which different types of statistics are generated that compare different safety performance indicators. As already mentioned, it is necessary to ensure compatibility for this type of statistics. At the same time, however, the new systemic approach can also bring further analyses from the recorded data and thus monitor new types of statistics.

The CAA process model could also find other use-cases. For example, CAA could perform analyses of its complete process model whether its employees are able to manage the amount of work for which they are responsible. This could be monitored if there is a library of employees within the process model. Employees would be assigned to individual Actors and therefore to Activities in the process model. Bonita Studio enables this, so it would be possible to use process models in this way as well.

The entire proposal of procedure for the safety data collection and processing at the civil aviation authority has many positive aspects for improving the entire aviation safety, but there are also some problem areas. These problem areas are mainly the issue of costs associated with putting the proposed procedure into practice, but also the issue of new

jobs, and therefore new employees. However, a systemic approach to safety should ensure that systemic weaknesses are identified early, and should also prevent accidents and incidents, which in turn induce a lot of expenditures. Therefore, if this systemic approach were to be supported, it is almost certain that costs induced by occurrences will be reduced while aviation safety will be improved. This is a public interest to be defeated by the Authority.

Conclusion

This thesis was focused on the creation of a proposal for the safety data collection and processing according to STAMP for civil aviation authorities. In order to achieve this goal, it was necessary to get acquainted with a large amount of new and important information. First, it was necessary to get acquainted in detail with the activities of the civil aviation authority and with its position and powers in dealing with aviation safety. Considering the goal, issues related to safety oversight, both external and internal, as well as the system of data collection and work with them were studied in detail. Specifically, the mandatory and voluntary reporting system was addressed. Finally, the internal structure of CAA, its safety management and types of process documentation were studied, in which all processes taking place at the authority are described. Due to the validation cooperation with CAA CR, the research of the current situation at the authorities was carried out primarily at CAA CR.

Since the proposal of safety data collection and processing is based on the systemic approach of STAMP, it was necessary to study this theory and analyse it in detail. STAMP also includes two analyses, namely CAST and STPA. Both analyses have also been studied in detail for further use in the proposal.

The process model according to STAMP was a basis for the creation of the entire proposal of the procedure for the safety data collection and processing. This process model was modeled based on the processes recorded in the CAA process documentation. Process documentation for these needs was provided by CAA CR. Due to the extent of this documentation, its entire processing was not possible, and therefore only its part was selected, on which the procedure of model creation was described and explained. Part of the documentation was selected for its suitability for the topic, and therefore one directive and one manual were chosen. The selected directive deals with the processing of safety information and the selected manual deals with the continued oversight of AOC holders. In order to be able to process the documents into the process model according to STAMP, it was necessary to find a way to do this. The BPMN modeling tool, which allows the creation of process models, was considered to be a suitable solution. For this tool to meet all the requirements for this type of modeling, a qualitative research of the available tools was performed, and finally the BPMN modeling tool Bonita Studio by Bonitasoft was chosen.

As already mentioned, the selected process documentation was processed into models in Bonita Studio, where the processing procedure in this modeling tool was shown in detail. Furthermore, the application of STAMP was explained in detail on the model and again the solution in Bonita Studio was shown in detail. Specific information from process models according to STAMP (controllers and deviations) were given in the tables for the sake of clarity. After creating the process models, it was possible to propose and describe a procedure for safety data collection and processing using STAMP. For the complete proposal of the procedure, a scheme was created, in which it is possible to see the relations in detail.

At the end of this thesis, it was necessary to verify both the process models and the entire proposed procedure. The entire validation consists of three levels. The first level of validation was performed during process modeling using BPMN syntax verification in Bonita Studio. The second level of validation took place through regular consultations with CAA CR, which provided verification of process models, but also partial verification of the possible use of the entire proposal in practice. The third (last) level of validation was performed based on the application of real data to the proposal of the procedure for the safety data collection and processing. Specific data were selected from publicly available final reports published on the AAll CR website.

Finally, the achieved results were discussed and their advantages and disadvantages when used in practice were specified. The entire proposal of the procedure for the safety data collection and processing is therefore based on a new systemic approach to safety and, at the same time, the issue of placing the proposal of the procedure in the current conditions and environment, which cannot be changed immediately, is considered. The progressive implementation of a systemic approach to safety could be a step towards identifying weaknesses in the system and at the same time increasing safety in aviation.

The proposal of the safety data collection and processing procedure based on a systemic approach is also subject to several limitations. These limitations include first the extensive task, namely the modeling of all processes that take place at CAA. Process modeling is relatively time consuming and it will probably be necessary to employ new staff for this activity. The second limitation comes with the need to maintain the created models up to date. Process documentation is continuously changing and these changes must also be made in process models. The specialist who will deal with modeling as well as model changes must have knowledge of BPMN and STAMP, but must also understand aviation issues.

If these limitations are overcome and a system platform is created for the new SDCPS software, then it will be necessary to find an expert who can create this software and then maintain it. When the systemic data platform and software have been created, it will be possible to extend the idea of a systemic approach to other areas of data collection, such as data from inspections and audits and implementation of changes. Nevertheless, the process models themselves can form the base for other CAA activities that may not yet be known today.

References

- [1] ČESKÁ REPUBLIKA. Předpis L19: Dodatek N - Státní program bezpečnosti České republiky. In: *Letecká informační služba*. 2013. Available from: <https://aim.rlp.cz/predpisy/predpisy/index.htm>
- [2] EASA. *Úřad pro civilní letectví: Dokumenty* [online]. 2020 [cit. 2020-02-03]. Available from: <https://www.caa.cz/dokumenty/easa/>
- [3] Organization of civil aviation in the Czech Republic. *Civil Aviation Authority of the Czech Republic: Authority* [online]. 2020 [cit. 2020-02-03]. Available from: <https://www.caa.cz/en/authority/organization-of-civil-aviation-in-the-czech-republic/>
- [4] Předpisy. *Úřad pro civilní letectví: Dokumenty* [online]. 2020 [cit. 2020-02-03]. Available from: <https://www.caa.cz/dokumenty/predpisy/>
- [5] ÚŘAD PRO CIVILNÍ LETECTVÍ. *Hlava 4, Příručka inspektora: Postupy pro průběžný dozor nad držiteli AOC*. Změna 2. Praha, 2017.
- [6] ÚŘAD PRO CIVILNÍ LETECTVÍ. *Směrnice ÚCL/S-SP-006-1/2017: Příručka inspektora oddělení letišť*. Verze č. 2. Praha, 2019.
- [7] ÚŘAD PRO CIVILNÍ LETECTVÍ. *Směrnice ÚCL-288: Systém sledování shody a interní audit*. Změna č. 2. Praha, 2019.
- [8] Safety Audit Results: USOAP interactive viewer. *ICAO: Safety* [online]. 2011 [cit. 2020-02-11]. Available from: <https://www.icao.int/safety/pages/usoap-results.aspx>
- [9] Nařízení Evropského parlamentu a Rady (EU) č. 376/2014. In: *Úřední věstník Evropské unie*. 2014, L 122/18. Available from: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0376&from=CS>
- [10] Prováděcí nařízení Komise (EU) 2015/1018. In: *Úřední věstník Evropské unie*. 2015, L 163/1. Available from: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32015R1018&from=CS>

- [11] Průvodce hlášením v civilním letectví. *Ústav pro odborné zajišťování příčin leteckých nehod* [online]. 2020 [cit. 2020-02-11]. Available from: <https://uzpln.cz/pruvodce-hlaseni>
- [12] ÚŘAD PRO CIVILNÍ LETECTVÍ. *Organizační řád ÚCL-15*. Změna č. 9. Praha, 2016.
- [13] Organizační struktura ÚCL 02/2019. In: *Úřad pro civilní letectví* [online]. 2020 [cit. 2020-02-11]. Available from: <https://www.caa.cz/wp-content/uploads/2019/07/2019-2-1.pdf>
- [14] Organizační struktura. *Úřad pro civilní letectví: Úřad* [online]. 2020 [cit. 2020-02-11]. Available from: <https://www.caa.cz/urad-pro-civilni-letectvi/organizacni-struktura/>
- [15] ÚŘAD PRO CIVILNÍ LETECTVÍ. *Směrnice ÚCL-331: Zpracování informací o bezpečnosti*. 1. vydání. Praha, 2019.
- [16] HOLLNAGEL, Erik, Robert L. WEARS a Jeffrey BRAITHWAITE. *From Safety-I to Safety-II: A White Paper* [online]. The Resilient Health Care Net: Published simultaneously by University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia, 2015 [cit. 2020-03-09]. Available from: <https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf>
- [17] LEVESON, Nancy. *Engineering a safer world: systems thinking applied to safety*. Cambridge, Mass.: MIT Press, c2011. Engineering systems. ISBN 978-0-262-01662-9.
- [18] LEVESON, Nancy G. a John P. THOMAS. *STPA Handbook* [online]. 2018 [cit. 2020-03-16]. Available from: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- [19] LEVESON, Nancy G. *An STPA Primer: Version 1* [online]. 2013 [cit. 2020-03-16]. Available from: <http://www.santoslab.org/pub/high-assurance/module-risk-management/reading/STPA-Primer-v0.pdf>

- [20] LEVESON, Nancy G. *CAST Handbook: How to Learn More from Incidents and Accidents* [online]. 2019 [cit. 2020-03-16]. Available from: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- [21] KLIMEŠ, Cyril. *Modelování podnikových procesů* [online]. Ostrava: Ostravská univerzita v Ostravě, 2014, 120 s. [cit. 2020-04-13]. Available from: <https://www1.osu.cz/~zacek/mopop/mopop.pdf>
- [22] *BPM portál: BPM prakticky - 3. část: Úvod do BPMN* [online]. BPS Business Process Services s.r.o., 2003-2007 [cit. 2020-04-13]. ISSN 1802-5676. Available from: <http://bpm-sme.blogspot.com/2008/03/3-uvod-do-bpmn.html>
- [23] KLUZA, Krzysztof, Piotr WIŚNIEWSKI, Krystian JOBCZYK, Antoni LIGĘZA a Anna Suchenia (MROCZEK). *Comparison of Selected Modeling Notations for Process, Decision and System Modeling* [online]. In: . 2017-9-24, s. 1095-1098 [cit. 2020-04-13]. DOI: 10.15439/2017F454. Available from: <https://annals-csis.org/proceedings/2017/drp/pdf/454.pdf>
- [24] PACNER, Jan. *Procesní modelování operací s daty* [online]. Brno, 2015 [cit. 2020-05-06]. Available from: https://is.muni.cz/th/la0gl/thesis-process_modeling_of_data_operations.pdf. Diplomová práce. Masaryk University, Faculty of Informatics. Vedoucí práce RNDr. Jaroslav Ráček, Ph.D.
- [25] About us. *Bonitasoft* [online]. 2020 [cit. 2020-05-06]. Available from: <https://www.bonitasoft.com/about-us>
- [26] Diagrams. *Bonitasoft Documentation* [online]. 2020 [cit. 2020-05-06]. Available from: https://documentation.bonitasoft.com/bonita/7.10/_diagrams
- [27] Common BPMN Modeling Mistakes and Best-Practices: Basic Events. *Gblog* [online]. 2013 [cit. 2020-05-11]. Available from: <http://blog.goodelearning.com/subject-areas/bpmn/common-bpmn-modeling-mistakes-best-practices-basic-events/>
- [28] VITTEK, Peter, Andrej LALIŠ, Slobodan STOJIĆ, et al. *METODIKA pro vytváření indikátorů bezpečnosti a jejich využívání pro potřeby řízení bezpečnosti leteckých organizací: Výzkumný projekt TAČR Alfa č. TA04030465* [online]. 2016

[cit. 2020-05-11]. Available from:

http://uldbeta.fd.cvut.cz/stazeni/vedecke_vystupy/indikatory.pdf

- [29] ÚZPLN. ZÁVĚREČNÁ ZPRÁVA o odborném zjišťování příčin incident na letišti Karlovy Vary, pád osoby z letadla A320 poznávací značky VQ-BRE dne 6. srpna 2013. [online]. Praha, 2013 [cit. 2020-05-12]. Available from: https://uzpln.cz/pdf/incident_CiySbBGs.pdf
- [30] ÚZPLN. ZÁVĚREČNÁ ZPRÁVA o odborném zjišťování příčin letecké nehody letounů A321-131 poznávací značky D-AIRT a B737-8BK poznávací značky TC-SNM, dne 18.6.2010 na letišti Praha/Ruzyně. [online]. Praha, 2010 [cit. 2020-05-12]. Available from: <https://uzpln.cz/pdf/q32v4nbt.pdf>
- [31] ÚZPLN. ZÁVĚREČNÁ ZPRÁVA o odborném zjišťování příčin vážného incidentu A319 AFR1482 a B735 CSA77E, dne 7.9.2012 na letišti Praha/Ruzyně. [online]. Praha, 2012 [cit. 2020-05-12]. Available from: https://uzpln.cz/pdf/incident_KZqscF6P.pdf