CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

Department of Air Transport

Development of the New Generation of Safety Management System in the Aviation

Habilitation

Accredited subject-area for habilitation: Transportation Systems and Technology

Ing. Andrej Lališ, Ph.D.

Prague, 2020

Abstract

Safety management is one of the key drivers in the modern aviation responsible for the remarkable safety record of the industry. It is one of the recent tools that became a standard for all major aviation stakeholders and the requirements for its implementation and functions are constantly being updated. This process is far from its end, however, as the very domain of safety and its management is not fully explained with the theory available today. This is supported by the fact that the theory is constantly developing, with several fragmented research branches that are not consolidated, and the most recent discoveries changed the whole paradigm how safety is managed today. Now it is almost certain that it is the theory of Safety-II and resilience engineering that will drive the future management of safety to a completely new evolutional stage. This work deals with the research projects, results and scientific achievement in the domain of Safety-II based safety management system, which will represent the new generation of safety management not only in the aviation, achieved at the Czech Technical University in Prague. The work details the progress toward definition of the technical means and solutions that will enable full consolidation of the contemporary safety theory and bridge the gap between the theory and industrial practice. It details means for safety performance monitoring and predictions, utilizing stochastic modeling, the development of aviation safety ontology and its extension toward the new systemic prediction models in the theory and finally the work carried to develop the first and the second release of aviation safety data collection and processing system, which is the heart of any safety management system, compatible with parts of the new Safety-II theory. The results and discussed achievements confirm the feasibility of Safety-II compatible safety management system in the aviation and detail new discoveries that contribute to the theory of safety and its specification.

Keywords: ontology engineering, resilience engineering, safety-II, safety management system, stochastic modeling

Table of contents

List of tables

List of figures

Abbreviations

ADREP	Accident/Incident Data Reporting
APF	Aerospace Performance Factor
ARMA	Autoregressive Moving Average
ARMS	Aviation Risk Management Solutions
ASO	Aviation Safety Ontology
ATC	Air Traffic Control
BPMN	Business Process Model and Notation
CAA	Civil Aviation Authority
CAST	Causal Analysis based on STAMP
DAIW	Danger Area Infringement Warning
ECCAIRS	European Co-ordination centre for Accident and Incident Reporting Systems
FAA	Federal Aviation Administration
FRAM	Functional Resonance Analysis Method
GASP	Global Aviation Safety Plan
GPWS	Ground Proximity Warning System
ICAO	International Civil Aviation Organization
INBAS	Indicator Based Safety
MCAS	Maneuvering Characteristics Augmentation System
MLE	Maximum Likelihood Estimation
MSAW	Minimum Safe Altitude Warning
NASA	National Aeronautics and Space Administration
OLS	Ordinary Least Squares
RAG	Resilience Analysis Grid
RDF	Resource Description Framework
RIT	Reduced Interface Taxonomy
SAFA	Safety Assessment of Foreign Aircraft
SDCPS	Safety Data Collection and Processing System
SISeI	Safety Intelligence System
SMS	Safety Management System
SPI	Safety Performance Indicator
SSP	State Safety Programme
STAMP	System-Theoretic Accident Model and Processes
STCA	Short Term Conflict Alert
STPA	Systems-Theoretic Process Analysis
UAV	Unmanned Aerial Vehicle
UFO	Unified Foundational Ontology
UML	Unified Modeling Language

Introduction

Safety is in modern society is declared among the highest priorities in almost every activity we do. Modern society changed its sensitivity to accidents and incidents, becoming less tolerant to it. There are various reasons for this shift, such as increased importance of individuals or advanced technology with better safety records that changed our perception of what is normal. The result is a pressure to manage safety effectively and it is most significant in the so-called high-risk industries, i.e. industries where the overall risk is higher relative to other industrial branches. In these industries we introduce dedicated safety management systems that aim to reassure the society than things will remain under control under both expected and unexpected conditions.

Aviation undoubtedly belongs to the high-risk industries and the framework of safety management started to appear here around the year 2000. In the late 2019, with the second edition of International Civil Aviation Organization (ICAO) Annex 19: Safety Management [1] coming into force, all main aviation players (organizations) must have a safety management system (SMS) implemented. Not only this does close the loops of safety management in technology development, manufacture, operation and maintenance, but it provides new opportunities for seamless industry-wide integration of the SMS, thus the ability to see how different organizations interplay to produce the overall safety record. This opportunity is highlighted by ICAO and aviation organizations are now encouraged to consider the interfaces between their SMS and the SMS of their business partners [2].

The idea to integrate SMS and to stipulate its usage among different players stems not only from operational experience, but also from the theory of safety. Both converged to systemic approach: industries now realize that safety outcomes are hardly a product of single operator or company, but rather a product of complex behavior of different operators, technology and the overall society setting, thus a product of the so-called socio-technical system that is very characteristic for the modern society. This realization came through accident investigation where modern accidents (especially those significant) seem to be very complex events of many participants, each with rather insignificant contribution to the overall outcome. The safety theory proposes an explanation to this: it lies with emergence, i.e. a property of complex systems which exhibit specific behavior at system level that can be considerably different from a simple sum of all systems components behavior [3]. Emergence is widely present in our universe and it is very typical for complex systems, i.e. systems that cannot be fully traced in their behavior due to large amount of system elements and interconnections producing the overall system. From this perspective it seems a logical shift in our thinking to consider safety as an emergent property of modern systems, which are certainly becoming ever more complex thus ever harder to trace.

While the aviation so as the other high-risk industries move toward integration of SMS and extension of their functionalities, safety theory strives to provide new tools that could provide the necessary technical support for further shift in safety management. Several authors already proposed new models and methods that build on the effect of emergence and necessity to consider system-level point of view to manage safety. But these models and methods do not compare with any of the previous models and methods developed thorough the 20th century (such as the still popular Swiss cheese model [4] or SHELL [5]). By considering system level more important than component level, and by introduction of the notion of safety as emergent property, they represent radical shift in our thinking about safety, so radical that even the very meaning of what is safety is now questioned. In result, resilience and resilience engineering [6] emerged as a theoretical discipline necessary to complement the conventional approach to safety. The complementing theory is now referred to as Safety-II, or the second generation of approach to safety, whilst the conventional approach is now called Safety-I.

Because of all this development, the framework of SMS will hardly remain intact. Current industrial SMS systems, including the aviation, are Safety-I but will need to be developed further to become compatible with Safety-II as well. This is not an easy task, since there are many use cases the SMS supports and each requires substantial update to become Safety-II compatible. Further, the theory is by far not complete about the models and methods required to implement Safety-II in everyday operations. Many research teams worldwide are working with fragments of the theory and aim to close the gap between industrial practice and the new notions of safety theory. Despite this, we already know something about the new shift that needs to be done and the results of current research do and will further enable specification of the new SMS framework, together with its implementation in high-risk industries, including the aviation.

This work is oriented to provide an overview of some fragments of the research, which relates to the shift of the aviation SMS framework from Safety-I to Safety-II. The fragments relate to the work done by the author at the Laboratory of Aviation Safety and Security, Faculty of Transportation Sciences, Czech Technical University in Prague, that relates to this novel topic. It has a form of commented set of scientific publications that provide an insight into the notions and results of the research carried over the span of several years by the author and in collaboration with his research team. The work is divided into two main subject areas, namely the research on predictive risk management, which relates to the current tasks of SMS development by the industry, and the ontological foundations of Safety-II based SMS, which relates to the current research in academia. Both have in common the problem of current safety data, which is one of the core issues in the domain addressed by the author.

1 Motivation for the research

This chapter provides detailed description of the current state and motivation for the research carried by the author. It details the current standards of aviation safety management and the theoretical foundations of modern safety engineering that both represent the foundation for the research described in the next sections.

1.1 Aviation safety management

Standards for the aviation safety management are given by the ICAO Annex 19: Safety Management [1]. The document includes global standard requirements for aviation organizations, and the means to meet the standards are described in ICAO Doc. 9859: Safety Management Manual [2]. Both documents were updated recently, with new requirements coming into force late 2019. In the newest standard, ICAO declares that we are living now in the total system era (Fig. 1) and for the purpose, all key aviation organizations must have SMS implemented and shall consider interfaces between their SMS and the other SMS systems of their business partners. Here, the safety theory was aligned with aviation industrial standards, considering system-level perspective as the most significant and characteristic for the current era.

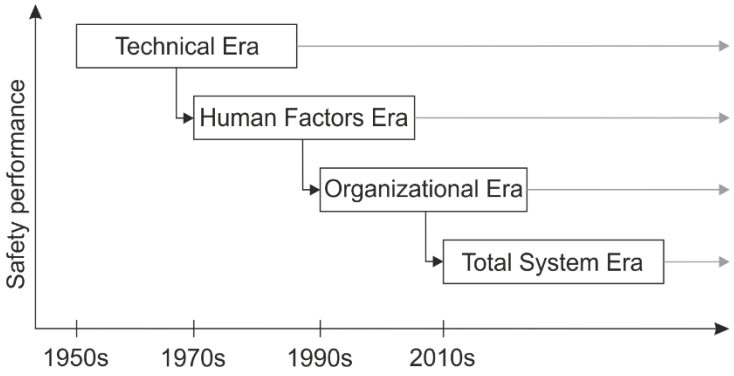


Figure 1 Evolution of safety (adapted from [2])

The SMS consists of four main components, each being composed of individual elements. The overall SMS framework in the aviation is shown in Tab. 1, detailed description of the components and elements is available in [2]. From the technical perspective, the second component (safety risk management) with both its elements is the core of the whole system. It deals with identification of safety problems and their resolution. It is driven by our very understanding of what is safety, how safety problems emerge and what can be done about them. ICAO encourages the industry to adopt the conceptualization of SHELL and Reason's Swiss cheese model, together with the idea of practical drift, to understand and explain safety.

Aviation organizations are encouraged to use the conceptualization to identify safety problems and to reach conclusions about what measures shall be taken. Once individual safety problems are identified, recorded and resolved, the core component of the SMS is used as an input for the third component (safety assurance) for various managerial use cases, detailed into respective elements in the Tab. 1. Consequently, the third component is sensitive to the quality of output from the second component.

Table 1 Aviation SMS framework – components and elements (adapted from [2])

Component	**Element**
1. Safety policy and objectives	1.1 Management commitment
	1.2 Safety accountability and responsibilities
	1.3 Appointment of key safety personnel
	1.4 Coordination of emergency response planning
	1.5 SMS documentation
2. Safety risk management	2.1 Hazard identification
	2.2 Safety risk assessment and mitigation
3. Safety assurance	3.1 Safety performance monitoring and measurement
	3.2 The management of change
	3.3 Continuous improvement of the SMS
4. Safety promotion	4.1 Training and education
	4.2 Safety communication

The SMS framework from Tab.1 is a product of decades of aviation accidents and incidents investigation and emerged progressively during the 1990s (see Fig. 1), when it became clear both from the investigation and (at that time) the newly proposed Reason's Swiss cheese model that organizations and their management play significant role in the overall safety outcome. The organizations were assigned responsibility for this role and provided with the framework for how they can manage safety and contribute to further decrease of accident rate. Considering the safety record in the aviation over the last 20 years [7], since the introduction of the framework from Tab.1, the effect of its implementation is compelling as the accident rate steadily decreased.

Moving to the current era, ICAO declares that the SMS framework needs to be considered for seamless integration, not only within respective organization (e.g. with quality or documentation management system), but especially with other organizations in the

environment, where interfaces exist and interactions occur. Special emphasis is put on the roles of states, or more precisely the civil aviation authorities and delegated regional institutions representing states, and on their implementation of the SMS framework (commonly referred to as the State Safety Programme (SSP)). By this, ICAO intends to facilitate establishing safety management, that will allow the total system point of view and from where the system safety problems could be identified, and not only the problems of individual organizations. States and regions will play the key role in this concept, as they have all the necessary means to establish the system-level point of view and the means to take effective measures at this level.

ICAO has published a long-term vision of aviation safety development until 2028, where it details the steps to be taken at the state level (see the Global Aviation Safety Plan (GASP) [8]). Apart from implementing and maturing the SSP, the GASP emphasizes need to progressively mature safety data collection, processing and analysis, which is the technical core of the second component of the SMS framework. As a long-term vision until 2028, ICAO states implementation of predictive risk management, i.e. maturing the second component until meaningful safety predictions can be established. ICAO states that *"safety analysis will be integrated into all aspects of future aviation systems and used to predict risks prior to implementation of operational changes"* [2]. This implies that safety models and methods allowing such predictions exist and that safety data are of sufficient quality with respect to the models and methods. ICAO is not specific about the technical solution in this respect, but common industrial interpretation of this vision is that by means of the existing and already adopted safety conceptualization (Swiss cheese, SHELL and the practical drift mentioned before), and available technical solutions for aviation safety data integration (especially the ICAO Accident/Incident Data Reporting (ADREP) and the European Coordination Centre for Accident and Incident Reporting Systems (ECCAIRS) taxonomies, which were built with this conceptualization), the vision can be achieved. However, there clearly exists room for research activities regarding this vision of ICAO, that can either capitalize on verified prediction methods and models from other domains than aviation safety, or that can possibly question the very conceptualization of safety adopted by ICAO.

1.2 Systemic models and methods of safety

The evolution of safety (depicted in Fig. 1) followed the theory of safety developed mostly by academia and various research activities, i.e. there are several safety models and methods that aim to deal with technical, human factors and organizational issues related with safety, that emerged during the 20th century (see an overview in [9]). 21st century, however, brought a completely new era in the theory, namely the consideration of the system as a whole to

explain and predict safety. This shift was not only another step in the evolution, simply going above the organizational level (although it started in that fashion), but it was complete redefinition of several aspects of safety models and methods developed during the last century. This is due to the fact that at system level there are phenomena such as emergence, resonance or complexity, that are non-linear in their nature, thus being in direct conflict with our previous (in this respect simplistic) models and methods of safety.

This was probably best described by prof. Hollnagel in his book about the shift from Safety-I to Safety-II [10], where he argues about why redefinition is needed and what are the aspects that must be redefined. He provided the basic axioms of Safety-II (the second generation of approach to safety that considers the system level) so as the very first method that allows Safety-II data collection and analysis (the so-called Functional Resonance Analysis Method (FRAM) detailed in [11]). Prof. Hollnagel considered the shift so radical, that in his recent book [12] he argues that the word 'safety' does not fit anymore to what the future of safety management shall be about, if our goal is to further decrease accident rate and get more control about what we consider safety today. In his opinion, the future shall be about resilience engineering rather than safety engineering and we shall be concerned about the resilience of our modern socio-technical system to achieve further improvement. In the recent book he already proposed second method that is based on Safety-II and helps the user assess and develop resilient socio-technical system. The method is called Resilience Assessment Grid (RAG). Apart from his own work, his ideas were adopted in the European aviation by the European Organisation for the Safety of Air Navigation (EUROCONTROL) whitepapers relevant to aviation safety (such as [9] or [13]) and are subject to current research.

Parallel to the work of prof. Hollnagel is the work of prof. Leveson at the Massachusetts Institute of Technology. Prof. Leveson proposed a new accident prediction model named STAMP (Systems-Theoretic Accident Model and Processes) [3] where she proposes to access the system level by utilizing systems theory. In its core, STAMP uses concepts from feedback control theory to achieve the system description. In addition, prof. Leveson with her team attempted to provide model and methods that could be easily aligned and implemented with current industrial business processes, yet enable system level analysis. Due to this, the original model intended for accident prediction was quickly extended and became suitable for all safety management use cases, covering system design and development, manufacture, operation, change and investigation of accidents and incidents. The model, however, is not fully aligned with the theory of Safety-II proposed by prof. Hollnagel, because it explains safety as a control problem, considering causality instead of resonance as the key driver. Nevertheless, the model provides means to achieve system level description useful for safety management and enables its user to deal with some types of safety issues and phenomena at this level. The model with

its methodologies cannot be considered as conflicting with FRAM or RAG methods, but rather as taking different perspective and allowing to solve different type of safety issues. Application in the aviation safety is still rather limited to the United States, where the most significant users currently are Boeing and the National Aeronautics and Space Administration (NASA)[1].

Apart from the formalized systemic models and methods, there are some safety researchers that did not propose a model or method, but rather a set of practical notions and implications, which are grounded in the axioms of Safety-II. Probably the most influential is prof. Dekker who published numerous books mostly focused on human factors and complexity in the context of Safety-II. His work on practical drift [14] is especially relevant to aviation safety management, since it elaborates the notion (currently presented by ICAO as one of the key safety conceptualizations) further to account for complexity, emergence and resonance, i.e. the system level phenomena.

All the mentioned approaches to safety in the theory have in common the system level point of view, and phenomena present at the level (thus they are called systemic). They each take different perspectives and are compatible with each other (as also indicated in [15]). However, this points to the fact that the theory is by far not complete and there is no universal systemic prediction model of safety that can be used to further develop the SMS framework from the previous section. The research and application of the systemic models is about making analytical choices which of the models and methods suits best respective need, and often involves theory extension to bridge the gap between the theory and practice. On the other hand, it is now becoming clear that older prediction models of safety (including the Swiss cheese and SHELL used by ICAO) are obsolete and the very foundations of the safety risk management component of the SMS will need to undergo significant change in the future. Each model and method for predicting safety requires different data and exercises different mechanism of safety analysis, so a change of a prediction model may completely redefine SMS processes and the perception of what is and what is not a safety issue.

1.3 Safety-II theory and axioms

Due to practical reasons, it is out of the scope of this work to introduce the systemic models and methods in more detail. In case of interest, the reader may refer to any of the referenced publications to learn about the theory. It is, however, important to briefly introduce and differentiate the axioms of the Safety-II theory, in comparison with Safety-I (the conventional, industrial approach to safety management). This comparison is provided in Tab. 2.

[1] See presentations from MIT STAMP workshops: https://psas.scripts.mit.edu/home/stamp-workshops/

In the table, individual axioms hold only in each theory. Certainly, it is not adequate to consider Safety-I axioms now as wrong; they proved to be effective in our current safety management. The point is that these axioms do not hold as soon as we attempt to manage safety of complex socio-technical systems; they only hold for non-complex systems which were typical for the past, but are still present in many instances today.

Table 2 Comparison of the axioms of Safety-I and Safety-II theories (adapted from [10])

Safety-I		Safety-II	
A1:	Systems are decomposable.	A1:	Human performance, individually or collectively, is always variable.
A2:	Functioning of the components can be described in bimodal terms.	A2:	It is neither possible nor meaningful to characterize components in terms of whether they have worked or have failed, or whether the functioning is correct or incorrect.
A3:	It is possible to determine the order in which events will develop in advance.		

Aviation is a good example in this respect; history aircraft, no matter how complex they seemed, were not complex. The modern Boeing B787 Dreamliner, compared to the B707, utilizes software, electronic systems and advanced automation, which make possible pathways of unwanted interactions untraceable. There are too many ways a problem may occur and the pathways may be very well composed of normal, designed behavior, with no apparent failure or malfunction of any components. What is more, the aircraft is serviced and updated before we can learn enough about how particular setting, software or electronics perform, so the system now retains its complexity throughout the entire lifespan. In such setting, the axioms of Safety-I do not hold. The entire aviation industry, being now globalized, underwent similar shift and due to many connections among all the aviation stakeholders it gradually became a complex system.

Following the theory by prof. Hollnagel and prof. Dekker, complex systems cannot be traced thus it makes no sense to attempt their decomposition or determine order of events when something goes wrong. Similarly, bimodal functioning (such as success or failure) is overly inadequate to describe states of these systems. We need to talk about large spectrum of variabilities that may emerge in the system and attempt to search for non-linear interactions and their potential adverse effects. Non-linear interactions are a natural outcome of incomplete system description and insufficient time to learn the details. Human performance is and will remain the key player in the non-linear interactions as it is the very complexity which prevents automation and elimination of human factors.

Going back to the axioms from Tab. 2, this not only means that the working mechanism (etiology) how safety is achieved or lacking is different in Safety-I and Safety-II, but the very

manifestation of what is safe and what is unsafe now differs too. The difference in shown in Tab. 3.

Table 3 Comparison Safety-I and Safety-II in terms in definition of safety (adapted from [10])

	Safety-I	Safety-II
Governing principle	Causality	Resonance
Manifestation (definition of safety)	As few things as possible go wrong	As many things as possible go right

The governing principle is built on the axioms from Tab. 2. In the current safety management (Safety-I) we construct chains of contributing factors leading to the negative outcome, connected with causal relationships. In Safety-II, we talk about variability combination and its propagation along the system instead, where it is important to identify potential resonance due to the variability combination. Unlike in Safety-I, where contributing factors and the eventual outcome are always negative by their nature, in Safety-II the variability combination and propagation may have both negative so as positive effect. By that we can understand where both strong and weak parts of an assessed system are and unlike in Safety-I, apart from addressing weaknesses by mitigation measures, we can reinforce the system by learning from its strong parts and capitalize on them. This ultimately leads to redefinition of what is considered safe per each of the theories; in Safety-I we are happy if nothing (bad) happens, whereas the goal in Safety-II is to operate our systems as much as we imagine and expect. This resolves one of the key paradoxes of modern safety management where the safest companies have little safety data, thus almost nothing to learn from, and often take the situation of past success as a guarantee of future safety. According to Safety-II, however, the safer the company, the more data about its strong points it collects and the better understanding of how safe operations were actually achieved it gets. Based on that, a company can have more confidence about the future operations.

1.4 The prospects of Safety-II SMS

With the new theory of Safety-II, SMS systems so as all the use cases of safety management will need to be shifted to account for the new axioms, mechanism and definition of safety. It is, however, not the case that Safety-II will completely replace Safety-I, thus future SMS will not mean complete replacement of what we have and use today. As mentioned before, Safety-I axioms and methods are still valid for non-complex systems, so Safety-II rather extends what we have today with new tools and support for dealing with complexity. However, not even the

aviation is complex in its entirety; when dealing with local issues in aviation organizations or in aircraft design that can be considered as very loosely connected with the system level, i.e. being rather isolated, then current SMS framework is adequate for safety management. It is probably not even possible to exercise full analysis of complexity at the level of a single aviation organization, because Safety-II models and methods require significant effort and expertise, whilst individual organizations rarely possess all the data needed. In some cases, complexity may emerge within the operation of a single aviation organization, especially in the large ones such as major airlines or air navigation service providers, but we shall not forget that the most significant complexity responsible for the overall outcome in the aviation is produced at the level of the industry, exceeding the boundaries of the industry as such [14].

In such setting, the vision of ICAO in the aviation is sound and it facilitates achievement of Safety-II compatible SMS framework in the future. We need to integrate the SMS systems across the industry and build system level points of view with the SSP framework. At this level, we will be able to distinguish where significant complex phenomena occur and drive the industry to select adequate approach to improve safety, whether by taking Safety-I or Safety-II approach. Both will need to be applied simultaneously, but the choice (drawing the line) will need to be supported with arguments. It is also likely, that some analyses will require simultaneous application of multiple models and methods, originating in both Safety-I and Safety-II theories.

Taking the technical point of view, the SMS framework (Tab. 1) is set well in the components and elements as managerial system, but as already mentioned, components 2 and 3 with their elements will need to be extended with models and methods of Safety-II and with respective decision making about the nature of the issues, which will exist at the level of particular organization and its SMS. Each aviation stakeholder will need to be aware of its contribution to the industry and the true nature of their issues, making them capable of taking adequate decisions about safety measures.

2 Safety performance and predictive risk management

Safety performance monitoring and measurement is one of the most important elements of any SMS, because the measured performance informs management of the overall safety achievement in respective company. In simple terms, the measurement of safety performance encompasses all safety data and records available and attempts to estimate how safe a company operation was over the period of interest. The ICAO vision of predictive risk management is closely tied with it, because the very safety performance is be subject of predictions as well. Given the historical safety record and knowing what factors drive the overall safety performance, management can be aided for future decision. Without this measurement, it would be hard, if not impossible, to make sense of the safety data at the company level.

This section details the author's work with respect to safety performance predictions, which was the initial step toward the second generation of the aviation SMS. The research was based on Safety-I and the safety data currently available in the aviation.

2.1 Mathematical predictions

Because no advanced safety performance predictions exist in the aviation (currently they are based on expert assessment of a set of safety performance indicators) and because the measurement of the performance lays down data collection and processing schema, the first studies toward the Safety-II SMS were carried in this domain. The assumption was that a research of mathematical methods for safety performance predictions in the aviation could provide initial requirements for data collection, before any particular safety model or method is considered. Appendix A contains detailed study and selection of suitable mathematical modeling tools.

LALIŠ, Andrej. Time-series analysis and modelling to predict aviation safety performance index. *Transport Problems*. 2017,12 (3), pp. 51-58. DOI: 10.20858/tp.2017.12.3.5

Appendix A

The study analyzed available research in the domain of aviation safety performance predictions, and the state-of-the-art was considered the measurement of the safety performance by means of Aerospace Performance Factor (APF), as adopted in the European aviation by EUROCONTROL, and in the U.S. by Federal Aviation Administration (FAA) [16]. The APF provided unique but still practical way how to aggregate safety data into a single

variable that could be modeled with standard mathematical methods. EUROCONTROL did basic prediction by trending and application of descriptive statistics [17], yet the methodology and aviation safety data allow application of more advanced prediction techniques. The study in Appendix A converged with the choice of suitable mathematical modeling to stochastic systems, since the APF produces time-series and the input safety data for the APF computation can be used as predictors in stochastic models. In addition, it is clear that the signal obtained by the APF contains some inherent noise, mostly due to uncertainty about data completeness and consistency (which is typical for Safety-I as people individually and collectively are reluctant to share information about the negatives), thus modeling with uncertainty became one of the key requirements. In the end, the study selected two candidate methods: the ordinary least squares (OLS) based linear regression and the maximum likelihood estimation (MLE) based autoregressive modeling with moving average (ARMA). Both methods had slightly different requirements, advantages and disadvantages, and one of the conclusions was that it is necessary to test their performance with real aviation safety data.

2.2 The problem of aviation safety data

In the course of the search for all possible sources of safety data, new issues emerged. The APF so as both the selected mathematical methods required larger amount of data than could be acquired from any single aviation organization. Since EUROCONTROL and FAA have large datasets collected at regional level from different member states, this was no issue when the APF was adopted and computed in their studies. However, for the purpose of this work, these sets could not be used for advanced mathematical modeling, due to confidentiality restrictions and data ownership. Only anonymized aggregates from public data sources were available. Out of these, the most extensive source of the aviation safety data were public repositories maintained by the EUROCONTROL on its dedicated performance monitoring websites[2]. Similarly, valuable source of safety data were various annual performance review reports, published by the agency, which provided some additional details. Despite of all the effort spent during the data collection process, it was not possible to get all safety data at sufficient granularity for the purpose of the stochastic modeling. Thus, the granularity had to be increased and the subsequent study about data resampling and generation is presented in the appendix B to this work.

[2] http://ansperformance.eu/,
http://www.eurocontrol.int/prudata/dashboard/eur_view_2014.html,
http://www.eurocontrol.int/prudata/dashboard/rp2_2015.html

The study in the appendix was, in simple terms, concerned with a breakdown of single value into several new values of higher level of detail (granularity), so as with production of entirely new (i.e. completely synthetic) datasets. This was particularly desirable since only annual figure of incidents was available whilst monthly distribution of the incidents was required by each stochastic model. The study was also concerned with cases where no data at all were available, but some expert assumptions could be used. In its results, it proposed how to combine expert knowledge on the incident rate changes throughout the year, given seasonality and other factors that influence the occurrence, by means of representing the knowledge with mathematical functions. In the end, it was possible to break down all values of insufficient granularity and so to produce an APF signal (time-series) of more than one hundred data points, indicating the progress of safety performance over the span of eight years in the European region. For the purpose of this work, no completely synthetic data were needed.

It could be argued that the resampled data introduced additional bias, which is certainly true. Without that, however, no research on predictions with stochastic modeling would be possible. In addition, the goal of the work toward predictive risk management was not to predict actual safety record but rather to check the possibility of using stochastic modeling for the purpose, and consequently to identify requirements for the modeling in advance, so that any future data collection and processing can consider those.

LALIŠ, Andrej, Vladimír SOCHA, Petr KŘEMEN, Peter VITTEK, Luboš SOCHA and Jakub KRAUS. Generating synthetic aviation safety data to resample or establish new datasets. *Safety Science*. 2018, 106, pp. 154-161. DOI: 10.1016/j.ssci.2018.03.013.

Appendix B

2.3 Building mathematical models

The process of building the mathematical model was based on the results from Appendix B and is described in details in Appendices C and D to this work. The studies utilized OLS and MLE based methods to produce separate candidates for stochastic models. It was possible to estimate two separate models with each method, where both conditional and unconditional forecasts were tested. The APF signal proved to be deranged in its mean, i.e. strongly dependent on predictor data. This is confirmed by the fact that autoregressive analysis couldn't propose valid stochastic model. Among the conclusions, OLS based conditional forecasts (i.e. linear regression) were considered the most suitable method for predicting aviation safety performance, but there were also other interesting conclusions reached during the work.

One of these conclusions is that the APF computation with monthly distributed data about safety outcomes (occurrences) and with subsequent monthly distribution of predictor data produced 108 data points during eight years period. Eight years in modern aviation comprise many changes and updates, i.e. the assessed background system is not the same throughout the entire period. This may be related with the conclusion that APF signal is deranged in its mean, but couldn't be confirmed in the study due to lack of predictor data about the background system. On the other hand, the 108 data points were severely limiting stochastic modeling, for which at least hundreds to one thousand data points would be ideal. The very setting of safety performance measurement was consequently questioned among the results and, arguably, there is new framework needed for how to measure and monitor aviation safety performance if stochastic modeling shall be used effectively for mathematical predictions.

With respect to the limited dataset, MLE couldn't be conclusively pronounced as not suitable for predicting aviation safety performance. It could only be confirmed, that with the current setting of aviation safety data collection, MLE is unlikely to produce valid prediction model. In addition, conditional forecasts with MLE were not possible due to insufficient data sample for the method.

LALIŠ, Andrej, Vladimír SOCHA, Jakub KRAUS, Ivan NAGY and Antonio LICU. Conditional and unconditional safety performance forecasts for aviation predictive risk management. In: *2018 IEEE Aerospace Conference*. IEEE, 2018, pp. 1-8. DOI: 10.1109/AERO.2018.8396648. ISBN 978-1-5386-2014-4.

Appendix C

LALIŠ, Andrej, Vladimír SOCHA, Peter VITTEK and Slobodan STOJIĆ. Predicting safety performance to control risk in military systems. In: *2017 International Conference on Military Technologies (ICMT)*. IEEE, 2017, pp. 392-396. DOI: 10.1109/MILTECHS.2017.7988791. ISBN 978-1-5090-5666-8.

Appendix D

Despite of all the issues regarding data resampling, insufficient dataset and inability to build and test all possible model variations with stochastic modeling, including the questioning of the state-of-the-art for safety performance measurement in the aviation (the APF methodology), the most important goal of the study was achieved: it became clear what the data requirements for Safety-II SMS are, if stochastic modeling is to be used effectively for predictive risk management. The requirements can be formulated as follows:

- safety data collection and processing must be updated to allow producing time series of at least few hundred data points
- safety performance measurement must be developed further to avoid limitation of Safety-I datasets, both in data sample size so as the limitations in data quality
- background system description must be introduced and maintained in a form that is qualitatively or quantitatively measurable to track the evolution of the background system

Some of these requirements reflect the perspective of Safety-II and can be resolved by the theory and its new discoveries. However, only with the stochastic modeling it became clear that high quality data about predictors are needed and what the data sample size must be to allow producing meaningful predictions of safety performance.

Finally, the study in Appendix E was dedicated to provide basic alignment between available stochastic models and possible inclusion of background system description, here as per STAMP systemic model of safety. The study proposed how state-space model aligns with the safety performance monitoring and predictions, together with feedback control diagrams used by STAMP. The study provided basic ideas how the new theory of STAMP fits into the previously described work and what are the next steps to take. In that sense, the results formed the foundation of the recent research on proposing data architecture of Safety-II SMS system in the aviation.

LALIŠ, Andrej, Peter VITTEK and Jakub KRAUS. Process modelling as the means of establishing semi-automated safety management. In: *Proceedings of 20th International Scientific Conference*. Transport Means 2016.

Appendix E

3 Engineering the ontological foundations of Safety-II SMS

The research described in the previous section provided an insight into the author's work aimed at supporting enhancement of the risk management to allow for predictions. These predictions were grounded in the mathematics, more specifically stochastic modeling, and the research results indicated that (a) predictive risk management is possible with the utilization of stochastic modeling, (b) the stochastic modeling has great potential to reduce subjectivity and limit mental processing of safety analyst to interpret safety performance measurement and predictions and (c) initial requirements for safety data can be inferred from the suitable mathematical methods that allow predictive risk management. With all these results, core software solutions for future SMS can be proposed.

This section details the work carried toward building the new SMS system. The work consisted of two main parts: development of the first version of the system for Czech aviation organizations and the Civil Aviation Authority, founded on the existing industrial standards, and development of the second version of the system, which extends to cover some aspects of Safety-II theory with the STAMP prediction model of safety. In each of the work the author contributed to different parts of the research, which will be specified in respective text.

3.1 Developing the first release of the new generation SMS

Referring back to the aviation SMS framework from Tab. 1, the core of the system lies with the second element, i.e. safety risk management. In terms of software, the core technical solution is a safety data collection and processing system (SDCPS) which supports all the use cases of the second element. The SDCPS is formally described by ICAO in the Doc. 9859 and it is mandatory part of all aviation SMS systems. In ICAO terms "*Annex 19 requires States to establish safety data collection and processing systems (SDCPS) to capture, store, aggregate, and enable the analysis of safety data and safety information to support their safety performance management activities. … Service providers are also required to develop and maintain the means to verify their safety performance with reference to their safety performance indicators and safety performance targets, in support of their safety objectives by means of SDCPS. The SDCPS is a generic term used to refer to processing and reporting systems, databases and schemes for exchange of safety information and recorded information.*" [2] The SDCPS is thus a type of data storage system, by means of which operational records of different origins (occurrence reporting, audits, safety inspections) can be stored in a database, from which the information and knowledge about overall safety record could be extracted, including but not limited for the purposes of safety performance measurement.

The SDCPS became the core focus in the next domain of the author's work and the goal was to propose a system of safety performance indicators (SPIs) that would allow effective safety performance measurement and monitoring and to propose and develop corresponding SDCPS system. This research was carried within the project No. TA04030465 with the support of Technology Agency of the Czech Republic, during the years 2014 to 2017, parallel to the research of the predictive risk management. The author participated in the project as a project team member. Author's main contribution was provision of safety expertise with regard to safety performance and its indicators, i.e. support to assurance of all results in terms of workflow, applicability in aviation organizations, compatibility with aviation SMS standards and regulations and with the previous research on safety performance predictions. The research partners were major aviation stakeholders in the Czech Republic, specifically the Air Navigation Services of the Czech Republic, Prague Airport, Czech Airlines Technics and Delta System Air (DSA), which all shared their expertise and safety data necessary to execute the research. The research team for this task ensured multiple disciplines representation, by merging two different faculties of the Czech Technical University in Prague, namely the Faculty of Transportation Silences and Faculty of Electrical Engineering, combining expertise in aviation safety management and knowledge management systems.

3.1.1 The Aviation Safety Ontology

One of the key questions in the research was proposing the set of SPIs that could be used in the aviation industry. Until today, there have been several studies that aimed to propose the most suitable framework for the SPIs (e.g. deliverable from Aviation Safety and Certification (ASCOS) project [18] or report by the Safety Management International Collaboration Group [19]) to provide initial setup for the corresponding SDCPS. Many of these used aviation safety taxonomies available, especially ICAO ADREP and ECCAIRS. Both taxonomies were proposed to be used with the integrated schemas for safety reporting (e.g. the schema laid down by [20] and [21] in Europe) and with corresponding SDCPS systems at ICAO and EU level - the ADREP and ECCAIRS systems, respectively. The benefit of grounding the SPIs with these formalized taxonomies was threefold. First, the taxonomies are based on large aviation safety data samples, collected at regional and global level, and they naturally cover all major issues from different types of aviation operations. Second, the taxonomies are arranged in hierarchical structures that fit well the APF method for safety performance measurement and monitoring, thus could be completely reused. Third, the taxonomies are the foundation of global and regional reporting schemas laid down by civil aviation authorities, i.e.

all aviation stakeholders have to report their reportable incidents and accidents using the schema.

Building on the previously described research, the SPIs in the Czech Republic could simply be established as a subset of ECCAIRS, similar to how the Reduced Interface Taxonomy (RIT) was established. RIT was proposed at the EU-level to filter ECCAIRS for the purpose of mandatory reporting, since ECCAIRS consists of thousands of terms that are hard to navigate and use effectively. The subset in the executed project was slightly different though, as it was necessary to establish subsets per aviation stakeholder, due to the differences in the operations. This was done and the required subsets were proposed. However, new issues emerged: maintainability of these SPI sets with regular updates of the ECCAIRS taxonomy, and the effectiveness of their usage. The ECCAIRS, so as its filtered subsets, couldn't prove comprehensible and easy to use for aviation inspectors and safety management staff.

The situation was resolved by means of ontology engineering. For the first time, ECCAIRS taxonomy was completely decomposed and the original hierarchical structure was abandoned. The terms were, however, retained and only a new structure was proposed. The structure is now known as the Aviation Safety Ontology (ASO) and is available online[3]. Fig. 2 depicts the core solution that the ASO is grounded in.

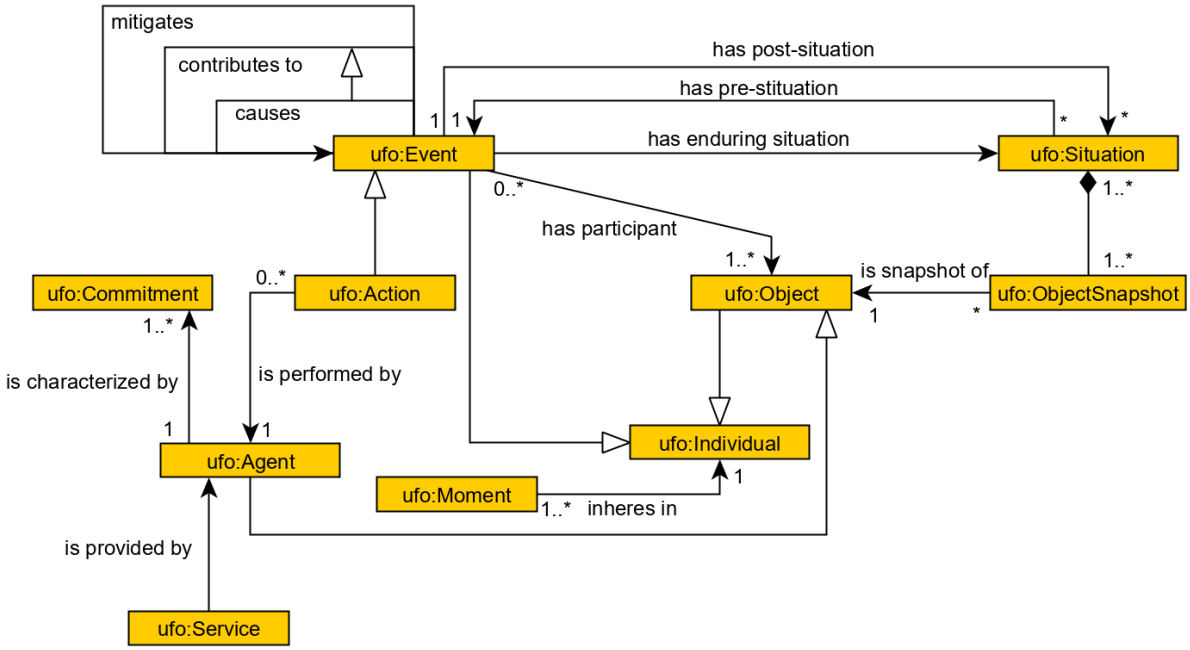


Figure 2 Core conceptualization of the Aviation Safety Ontology

[3] https://www.inbas.cz/aviation-safety-ontology

The figure represents a conceptual model (i.e. a metamodel) that structures the entire taxonomy. The key filtering concepts were rather simple at this stage (object, individual, event, situation etc.) but they allowed modeling of the taxonomy terms semantics. The original hierarchical structure of the ECCAIRS taxonomy is mostly expert based, i.e. shaped by the safety investigators who used the terms for classification of aviation safety occurrences. The only exception are human factors-related terms (explanatory factors in ADREP and ECCAIRS), which follow the structure imposed by SHELL model. The ASO proposed a structure that is grounded in the Unified Foundational Ontology (UFO, hence the *ufo* stereotypes in Fig. 2), an ontology that is founded on philosophical ontology, cognitive psychology, philosophy of language and linguistics, thus largely domain-independent ontology (see more details in [22]). This is in a strong contrast with the philosophy of aviation safety taxonomies and it provides clear benefits. Not only is the UFO-based structure more objectively specified (i.e. various people with different background are more likely to make the same sense of the data), but the structure allows natural querying (such as asking for all events where particular role, e.g. ramp agent, participates), partial automation (the structure is computer-readable, owing to the formalism of the UFO) and integration of several systems, that may have various specifications (i.e. supporting the vision of seamless SMS in the aviation).

The ASO also introduced new requirements for the safety database. To allow storing data according to the conceptual model from Fig. 2, it was necessary to store the data in the context of the ASO objects and predicates, thus an RDF tripplestore was proposed as a base technical solution. Here, it is necessary to emphasize, that the aviation safety taxonomy is considered to be data, to which particular occurrences are mapped by user classification. Detailed description of the research carried with respect to ontology modeling of the ECCAIRS taxonomy is provided in the Appendix F to this work.

KŘEMEN, Petr, Bogdan KOSTOV, Miroslav BLAŠKO, Jana AHMAD, Vladimír PLOS, Andrej LALIŠ, Slobodan STOJIĆ. Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems. *Journal of Aerospace Information Systems*, 2017, 14(5), pp. 1-14. DOI: 10.2514/1.I010441.

Appendix F

3.1.2 Prototype for aviation organizations

After the ontology was complete, the first prototype of the new generation SDCPS could be developed. To ensure maximum compatibility with the current industrial SMS systems, the newly developed SDCPS uses questionnaires with data fields composed of mostly pre-defined dropdown lists with ECCAIRS-based terms. The questionnaires, however, were proposed as adaptive, i.e. based on the information the user fills, different content is displayed. Adaptation of the reporting form is based on the ASO and significantly reduces its complexity.

Most of the reporting form adaptability is allowed through the use of *situation* concept and its part *object snapshot* from the ASO. The objects being present in respective event determine what content shall be displayed to the user. Here, for instance if the final event was runway incursion, it is given by definition that a runway must participate in the event, and it cannot happen in the air. Consequently, content (data fields) related to runway is displayed.

For the sake of improved user-friendliness and comprehensibility, a module called chain designer was proposed. The module allows interactive modeling of contributory factors of an occurrence, where the user has the option to provide both contributing and mitigating factors, by the relationships *mitigates*, *contributes to* and *causes*, as per the ASO from Fig. 2. The module with example occurrence is shown in Fig. 3.

The safety dashboard was proposed as a report generated from the data stored according to the ASO and allows drawing knowledge map of a safety occurrence of interest, depicted in Fig. 4. The figure depicts occurrence rate of particular contributory factors (proportional to the size of each node – the larger the node, the more of the occurrences) and the relations among the contributing factors (thickness of arrow corresponds to the rate of the relation occurrences in safety data). Arrow colors are consistent between Figs. 3 and 4.

Following the research, the very notion and framework of SPIs was partly redefined. In terms of the developed SDCPS, it is not a predefined set that company professionals shall propose based on their own experience or based on experience of external subjects, i.e. other organizations of the same type or from the civil aviation authorities. An SPI became a structured query that can be changed whenever needed.

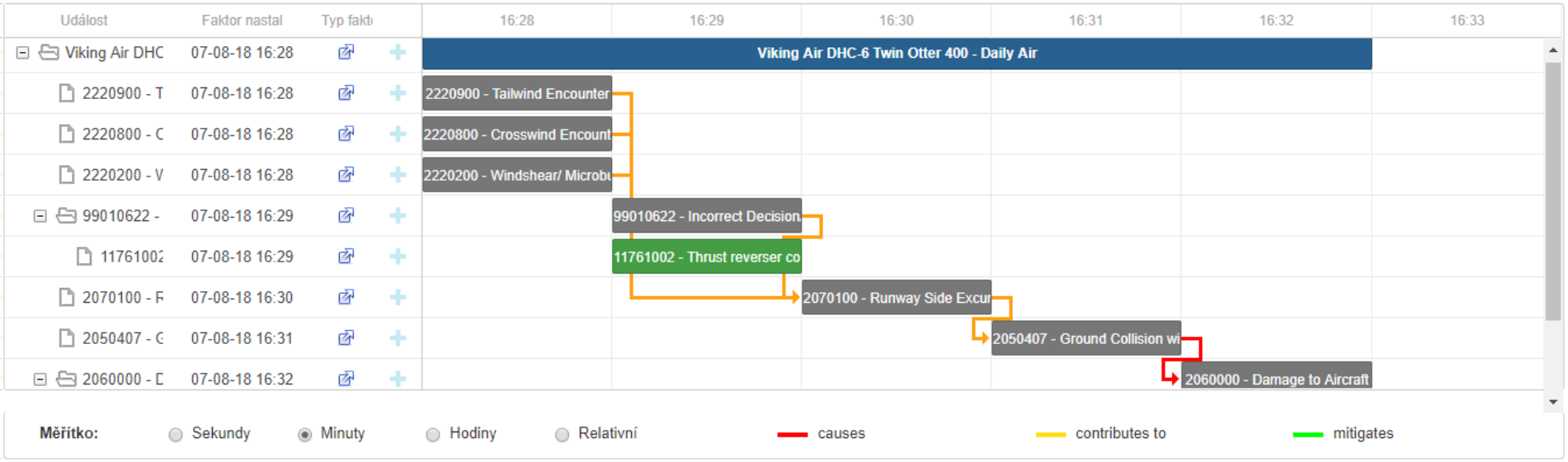


Figure 3 The chain designer

For example, a runway incursion is currently distinguished in ECCAIRS taxonomy as either by aircraft, vehicle, person or animal. If a new type of runway incursion emerges in the future, e.g. a runway incursion by unmanned aerial vehicle (UAV), this means no change the safety database as the new type of runway incursion will only require introducing UAV as one of the possible participating objects in the event, and not necessarily introducing new label in the taxonomy or update to some of the predefined SPIs list. The new SPI providing information about trends of such potential new occurrence is then simply a query with the same database. Its potential aggregation into safety performance measurement was not part of the research, even though it can be performed with similar logic, i.e. based on participating objects, the overall measurement may be automatically adjusted within the SDCPS.

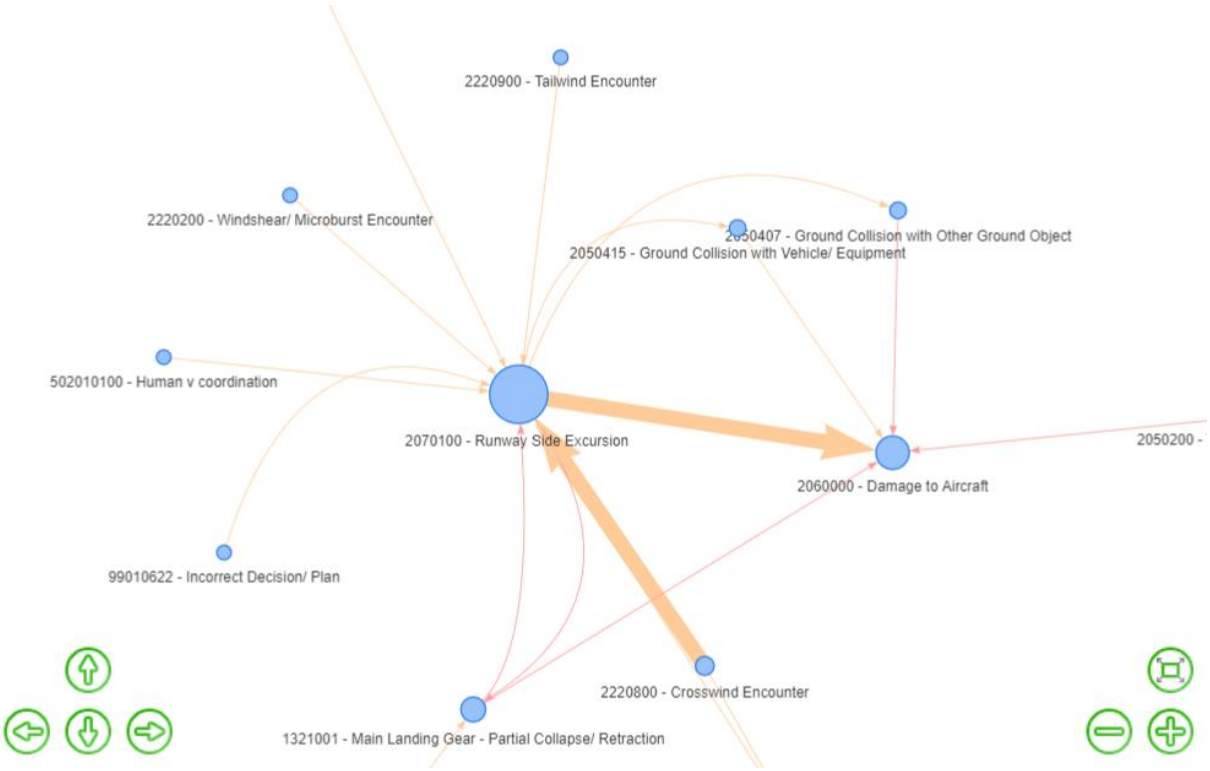


Figure 4 Example of the knowledge graph generated by the developed SDCPS

The system was named INBAS[4] Reporting Tool (RT) and the prototype was deployed at all the four research partners of the project for real operations testing. The common platform deployed in multiple aviation organizations allowed another benefit: safety data exchange. Data exported from one deployment of the RT could be directly transferred into another deployment and complemented with additional information from the perspective of the other party, thus building the full picture of particular safety occurrence, in line with the vision of

[4] Indicator Based Safety (INBAS) was the research project acronym

integrated SMS by ICAO. Regardless of the individual deployments evolution, owing to the ASO, data integration among all the deployments is further assured. The testing brought practical experience with the system and allowed its fine-tuning. Final version of the INBAS Reporting Tool is available online[5] and two of the participating organizations (Prague Airport, Czech Airlines Technics) decided to implement and further develop the RT within their own SMS system. Additional details about the INBAS Reporting Tool, its development and challenges with implementations are provided in the Appendix G to this work.

VITTEK, Peter, Andrej LALIŠ, Slobodan STOJIĆ and Vladimír PLOS. Challenges of implementation and practical deployment of aviation safety knowledge management software. *Journal of Aerospace Information Systems*. 2017, 14(5), pp. 1-14. DOI: 10.1007/978-3-319-45880-9_24.

Appendix G

3.1.3 Prototype for the Civil Aviation Authority

In 2015, the Civil Aviation Authority (CAA) of the Czech Republic joined the base research toward the Safety-II SMS (SSP). The research was carried within the project No. TB0400MD010 with the support of Technology Agency of the Czech Republic. Authors contribution to the research within the project was of the same nature as the contribution detailed with respect to the project No. TA04030465. Here, the emerging INBAS Reporting Tool was considered as the base platform, to enable future integration of aviation organization SMS systems with the state-level SSP. The ASO ontology was updated to include concepts specific for the use cases of civil aviation authorities, specifically from the domain of safety audits, and proposed initial schema how data from safety audits and safety occurrences could be integrated, again by means of the ASO. Such integration was never achieved in the industry before; data from audits and safety occurrences had to be consolidated by safety professionals and decisions about further steps taken at respective boards or within safety action groups.

Considering the use case of audits, it is now possible to use ECCAIRS terms for classification of audit findings, in the very same fashion as for occurrence classification. There are some limitations thought that were discovered during the research. These regard the inherent limitation of ECCAIRS with respect to audits: the events are mostly operational and do not allow for detailed description of latent conditions, e.g. of administrative nature. Another

[5] https://github.com/kbss-cvut/reporting-tool

ECCAIRS limitation is its mere Safety-I foundation, i.e. the taxonomy is primarily negative and prevents description of some conditions, that may seem normal but gain their safety relevance with particular context (e.g. crew rest time of certain extent that may not suffice given the larger scope). This limits both the extent of the information that can be stored in such SDCPS so as the usage of mitigation (positive) relations with the chain designer.

The system dedicated to the CAA was named SISel (Safety Intelligence System) and deployed in the CAA operations. SISel was implemented with special business intelligence module (safety dashboard) that allows for different perspectives in the safety data, e.g. perspective of particular aviation organization, or safety issue. It was integrated with ECCAIRS system, Safety Assessment of Foreign Aircraft (SAFA) audits and Aviation Risk Management Solutions (ARMS) methodology was implemented for risk assessment. Currently, SISel is actively used for safety management and its further development is planned. Detailed description of the research of SISel with some perspectives about integrated SDCPS systems by means of the INBAS Reporting Tool platform is provided in the Appendix H to this work.

LEDVINKA, Martin, Andrej LALIŠ and Petr KŘEMEN. Towards Data-Driven Safety: An Ontology-Based Information System. *Journal of Aerospace Information Systems*. 2018, 16(1), pp. 22-36. DOI: 10.2514/1.I010622.

Appendix H

3.2 Developing the second release of the new generation SMS

The first release of the new generation SMS, both in the variation of INBAS Reporting Tool and SISel, established the technical platform and represented natural first step toward the Safety-II SMS. The system was developed in cooperation with the aviation industry, which was necessary to achieve practical and useful solution, but it has some limitations as it was impossible to make radical evolutional changes to the SMS framework given the existing infrastructure in the aviation.

The executed research established key technical solutions. It quickly became clear that the new system must be a complete redesign of the existing technical solutions, because of the complexity of the industry. Existing aviation safety taxonomies (the ECCAIRS, RIT or ADREP) are proposed, organized and managed by aviation professionals, but the issues with them are not negligible. Despite introducing significant improvement in how they structure safety data, guide the users to classify and build the sets of SPIs, whilst enabling data exchange and safety

performance measurement, they limit the quality of safety data in an unwanted manner. Not only they became too robust and hard to use, but also hard to manage and update. In result, data quality, namely completeness, consistency and relevance can be questioned. In addition, the workflow of the current SDCPS systems used in the aviation does not reflect any of the current (systemic) safety models and methods, but rather builds on the practical expertise and knowledge from the industry, thus inherits similar limitations as the aviation safety taxonomies.

The key technical solution to reduce the afore-mentioned limitations is deployment of ontology engineering, especially the use of foundational ontologies. This brings a completely new perspective into the solutions available, as the taxonomies with the information collected and processed by an SDCPS can be grounded in domain-independent conceptualization and allow for resolution of inconsistencies of the domain-dependent conceptualization behind the current SDCPS workflow and the aviation safety taxonomies. This solution, however, means change to the safety databases and change to the workflow of an SDCPS, thus introducing the mentioned redesign of the current solutions.

After achieving this in the first release described in the previous section, the next stage was introduction of the new systemic safety prediction models and methods that are at least partly grounded in Safety-II, into the new SDCPS systems. The three models and methods that fit the purpose are STAMP, FRAM and RAG. They each take different perspective and due to practical reasons, for the second release only one of them had to be selected. The final decision was made to start with the STAMP model, due to (1) the model being the latest evolutional stage of Safety-I models, thus compatible to large extent with the existing theoretical foundations of the current SMS systems; (2) its capability to enable system-level point of view and consideration of ways to control emergent phenomena that do not pose radical evolutional change to the existing SMS solutions, and lastly (3) its application scope now covering all the use cases of the SMS systems. The selection of STAMP did not exclude FRAM or RAG from the research, it only postponed their incorporation into the system for the third release of the new SDCPS system in the future.

Considering all the following research toward the second release of the new generation of aviation SMS, the author proposed and managed the vision so as its achievement by different parts of the research team. The author directly participated in the ontology modeling and validation, STAMP theory application and verification, so as in the formalization of the new methodologies that detail the results of the research projects related to the second release.

3.2.1 The STAMP ontology

Model STAMP has its own conceptualization, which is not compatible with the current aviation SMS systems. The core source of the incompatibility is the introduction of contributory factors derived from feedback control theory and the introduction of system-level perspective for each safety case, be it occurrence reporting, audit or safety study. Introducing the new conceptualization into the previous software solution based on ASO required first building STAMP ontology, clarifying the conceptual foundations of STAMP and allowing for their alignment with the ASO, thus proposing integrated architecture for data and workflow of the second release of the SDCPS software. To retain the ontology as a core of the new system is in line with the established philosophy for the newly developing Safety-II SMS, stemming from the previous research done by the author and the research team he was member of.

The conceptualization of STAMP was based on the available STAMP literature, both the base publication [3] so as several case studies, which validated STAMP and its methods in different industrial branches. Key information and workflow were extracted and modeled by means of the UFO concepts and patterns. Afterwards, the ontology was tested with Czech aviation organizations and their safety data, with the use case of occurrence reporting. The conceptualization and the progress toward achieving the ontology brought some new perspectives and discoveries in the domain of aviation safety that will be detailed in the following text. To understand the scientific contribution, key parts of the ontology will be shown and explained with their implications for the aviation safety management.

The work related to the development and validation of STAMP ontology was carried in the research project No. TJ01000377 with the support of Technology Agency of the Czech Republic. Project partners were Prague Airport and Czech Airlines Technics, so the project directly built upon the experience with respective deployments of INBAS Reporting Tool. Due to this, decision was made to prepare the second release based on the INBAS Reporting Tool. Detailed description of the researched ontology with some perspectives of its methodological integration with SDCPS systems is provided in the Appendix I to this work.

HANÁKOVÁ, Lenka., Andrej LALIŠ, Bogdan KOSTOV, Markéta KAFKOVÁ, Jana AHMAD, Slobodan STOJIĆ and Katarína SZENTKERESZTIOVÁ. *Methodology for improving analysis and management of risk with the utilization of conceptual modeling*. Certified methodology by the Ministry of Transport, Czech Republic, 2019.

Appendix I

3.2.2 Core conceptualization of STAMP

The core of the ontology is depicted in Fig. 5. The basic concepts *Control*, *Constraint*, *Variable* and *Controlled Process* follow the theory of STAMP, explaining safety as a control problem. The *Variable* concept specifies what is (or shall be) controlled in order to avoid safety occurrences, here specifically the manifestation of *Hazard*. Note that the concepts *Safety Occurrence* and *Hazard* were updated (compared to the published version of the ontology) to make explicit their mapping to the terms used in the aviation safety domain.

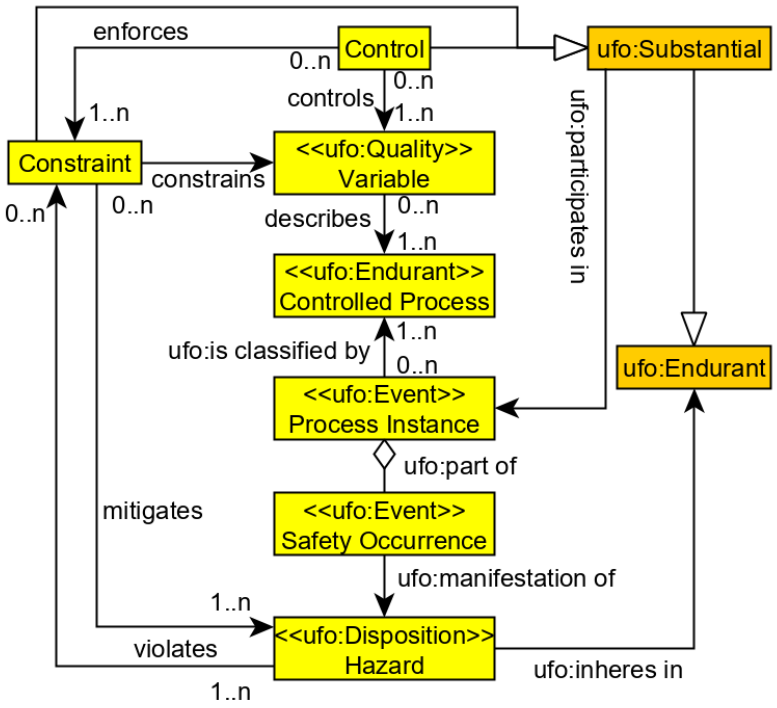


Figure 5 Core conceptualization of the STAMP ontology

For instance, a *controlled process* may be a flight, where the *variables* are speed, altitude and heading. The *control* of the aircraft is designed to manipulate these *variables* by means of the aircraft control systems, and in practice it is obviously exercised by the pilot or autopilot. *Hazard* related to this process may be unauthorized maneuver such as flying too low, entering an airspace without permission or simply not following an instruction of the Air Traffic Control (ATC). From the control perspective, we want the designed *control* to avoid these situations by manipulating the *variables* adequately, i.e. adjusting the speed, altitude and heading so that an aircraft does not execute an unauthorized maneuver. This implies enforcing the safety *constraints* derived from *hazards*. STAMP defines safety *constraints* as requirements for the system behavior. They are directly inferred from the *hazards*, i.e. if the *hazard* is an aircraft performing unauthorized maneuver, then the corresponding safety *constraint* is “an aircraft

must not perform an unauthorized maneuver". In this respect, the STAMP ontology specifies that *constraints mitigate hazards* and, vice versa, *hazards violate constraints*. The *control* is then certainly a composite of the flight crew with their training and management, through the ATC service and its background up to the safety systems installed directly aboard the aircraft (Ground Proximity Warning System (GPWS), build-in flight envelope protection etc.) or on ground (Short Term Conflict Alert (STCA), Danger Area Infringement Warning (DAIW), Minimum Safe Altitude Warning (MSAW) etc.). In STAMP terms, to design and execute *control* is the only way how we can do something about the *hazards* and so it is of extreme importance to do it well.

The rest of the conceptualization in Fig. 5 specifies how *hazards* relate to the *controlled process*. The *controlled process* is a pattern in the STAMP ontology, i.e. a description of what should be done under which circumstances, corresponding to the process documentation normally available in aviation organizations. If we want to talk about particular instances of the *controlled process*, i.e. particular events happening in space and time, these are referred to as *process instance*. A *controlled process*, e.g. a flight, may have large number of instances during a period and in some location, say during a year in particular airspace, and each of them are distinguished by the concept *process instance*. Some parts of some *process instances* meet the criteria for what is a *safety occurrence*, i.e. there was some significant safety-relevant deviation from the description of the *controlled process* and the actual *process instance* realization, such as the position of the aircraft did not respect flight clearance (e.g. unauthorized penetration of airspace). These parts of *process instances* (i.e. *safety occurrences*) are *manifestations of hazards* as per the STAMP ontology. This closes the loop of the conceptualization; the orange color boxes and stereotypes in yellow boxes then finally represent grounding of the STAMP ontology in UFO.

Now shifting the focus on the grounding of the concepts (by stereotypes and inheritance), the most interesting discovery is that the *Hazard* concept is modeled as ufo:Disposition. In UFO, dispositions are existentially dependent entities realizable through the occurrence of an *Event* [23]. In simple terms, dispositions are capabilities or vulnerabilities that inhere in objects, thus are existentially dependent on particular objects. For example, an aircraft has the disposition *to fly* owing to its technical design, but so it has the disposition (or here rather vulnerability) to *disintegrate* (e.g. due to overspeed) simply because it is not possible in our world to manufacture an aircraft with infinite strength of its structure. In this fashion, the *hazard* mentioned before (unauthorized maneuver) is similarly a *disposition* of the aircraft, since in our world aircraft are capable of executing such maneuvers. Here, it may be argued that this *disposition* is not existentially dependent on an aircraft only, but also on its crew and the existence of some general rules of flight, but this level of detail is omitted in this work. The UFO

ontology, however, provides means to model any level of detail in this respect by means of the *complex disposition* concept, with similar logic as *complex event* [24].

When comparing the definition of *hazard* with other relevant sources, there are two important *hazard* definitions to be regarded:

"A system state or a set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)" [3] (definition in STAMP theory)

"A condition or an object with the potential to cause or contribute to an aircraft incident or accident." [2] (ICAO definition)

In the context of the STAMP ontology, both definitions are to some extent ambiguous. The very definition of *hazard* by the author of STAMP is a "*system and its state or set of conditions"* with the *"worst-case environmental conditions".* What "system states" are relevant to safety? What "conditions" shall we focus on while performing safety study? How do we know what are the "worst-case environmental conditions"? These are just few examples of basic questions that may follow the definition. It certainly provides for interpretation variance, or more precisely, does not guide the user enough during hazard identification. It is apparent that the author of STAMP relies with the selection and identification of system-level hazards on the safety analyst expertise and his or her knowledge of the analyzed system.

Similar ambiguity is contained in ICAO definition, since a *"condition or an object with the potential"* may be interpreted very differently by people with various background and experience, essentially leading to similar questions as those following the STAMP literature definition of *hazard*. In fact, ICAO says that *hazards* are contributory factors and as such it indirectly encourages the user to filter them from the ADREP (or ECCAIRS) taxonomy.

By contrast to the definitions above, the STAMP ontology says that there must be an object (or objects), which possess a *disposition* (the *hazard*) that can be *manifested in* particular event. The *manifestation of hazards* are the accidents and incidents, thus the *safety occurrences* (see Fig. 5). This definition requires the safety analyst to start from safety occurrences and identify participating objects with their dispositions to propose hazards. The definition of *hazard* is more precise, as it limits the interpretation variance of the previous two definitions in STAMP or by ICAO. It is also a definition that provides clear guidance for how to control *hazards* in respective environment, since by knowing the specific objects, which generate the hazards, it is not difficult to infer related conditions and investigate what can be done about them.

To allow for producing and maintaining large schemas with system description, the base conceptualization of safety control structure shown in Fig. 6 was developed. The figure

proposes object-oriented description of structure components (the safety control structure from STAMP) and relations among them (the structure connections). The base conceptualization specifies that *control structure* consists of *structure elements*, which can be either *structure components* or *structure connections*. This implies that STAMP-based relations following the control loop are represented as separate components, and not as relations in the STAMP ontology. The reason for this is that STAMP relations cannot be directly represented by means of UFO relations.

Details of the control structure are provided in Fig. 7. Here, the basic concepts from STAMP representing a control loop are modeled, i.e. *Sensor*, *Actuator*, *Controller*, *Control Algorithm*, *Process Model* and *Controlled Process*. The relationships (arrows in STAMP schemas) are represented as *Feedback Control Connection* (arrows from controlled process through sensor up to controller), *Action Control Connection* (arrows from controller through actuator to controlled process) and *Information Control Connection* (arrows between controllers).

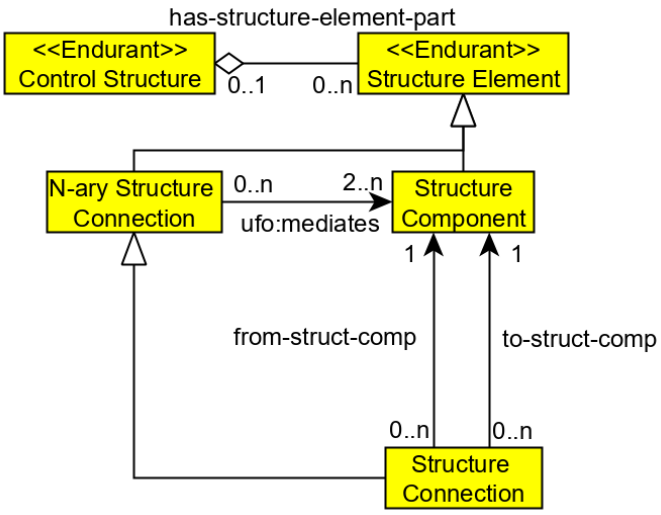


Figure 6 Base conceptualization of the control structure in STAMP ontology

Considering how *controllers* actually work in the aviation industry, it is often the case that single person exercises control in several control loops, thus representing different controllers at different times. Fuel truck driver, for example, represents a truck driver while transporting the fuel from airport reservoirs to an aircraft, whereas after parking the truck in the position for fueling the aircraft, he becomes the fueler, i.e. the person in charge of fueling the aircraft. From STAMP perspective, these are two different control loops, since the controlled process differs (truck driving and fueling) and so do the corresponding sensors and actuators.

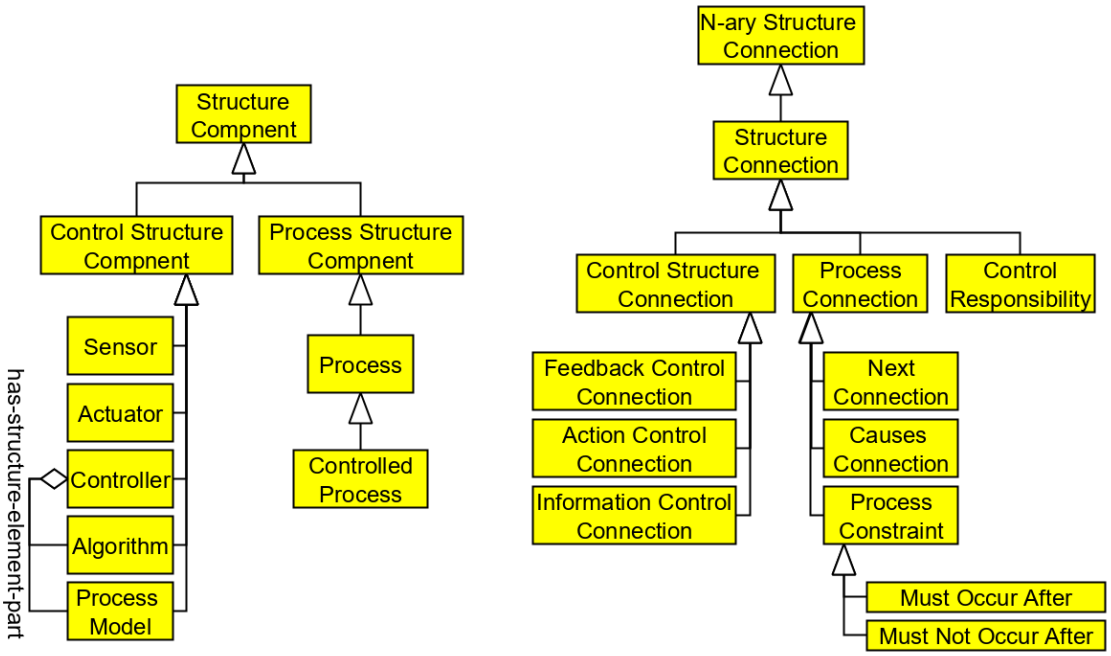


Figure 7 Detailed conceptualization of the control structure in STAMP ontology

At this stage, it is clear that the STAMP ontology is elaborated in much more detail than the ASO ontology. Only the safety control structure representation in the STAMP ontology with basic mapping to hazards, safety constraints and occurrences includes about 30 concepts whereas the ASO covered the core of the domain with 10 concepts. This is one of the shortcomings of the STAMP-based analyses anyway, as the full system description according to the theory is not practical, and sometimes even not possible. The authors of STAMP discuss the need to limit safety analyses to particular cases, or occurrences, and thus encourage safety analysts to produce a snapshot with system description every time an analysis is carried. Even though the STAMP ontology was originally considered as an extension of ASO to enable STAMP-based system level analyses, the new ontology provides technical means for effective robust modeling, thus overcoming the original issue discussed by the authors of STAMP. In this respect, the key question became how to facilitate the robustness of the STAMP-based analyses in the aviation industry and what other concepts shall be added for the purpose in the STAMP ontology.

As a solution to the problem of robustness with regard to the safety control structure, it was proposed to reuse organization process documentation, which already contains the information. The documentation is normally available electronically with Business Process Model and Notation (BPMN) [25], where the flow of the process activities with the responsible persons is defined. From the documentation it is clear how controllers are distributed so as how the process is normally carried. Since there is always a flow of controlled processes, often

even parallel, the STAMP ontology had to account for *Process Connections*, and not only *Control Structure Connections* (see Fig. 7).

The basic relation is *Next Connection*, which allows for expressing the chronology of the process tasks. The two remaining connections allow modeling of specific connections from the safety perspective, namely the *Causes Connection* and *Process Constraint*. The former allows modeling of causal chains of events (cf. Fig. 5 where *Safety Occurrence* is *part of Process Instance,* i.e. *safety occurrence* must happen as an instantiation of the *controlled process* description) and the latter allows for modeling of safety *constraints*. A *constraint* is basically set of relationships delimited at the level of the process description to deliberately avoid manifestation of hazards. For example, if the fueler receives an information about leaking fuel, he or she should take pre-defined measures to mitigate the risk (e.g. stop the process, report the occurrence, apply protection measures and similar). The basic process constraints are *must occur after* and *must not occur after* that relate two process steps, or more precisely two event types, to represent the expected nature of the *constraint*. Finally, there is *Control Responsibility* as the last *structure connection* (see Fig. 7). This concept is designed to map a *responsibility* to particular *controller*, i.e. to allow expressing who is expected to react under which conditions, and how. Details of this mapping are depicted in Fig. 8.

From Fig. 8 it follows that a controller has assigned the *Control Responsibility* designed to meet the goal of particular safety *constraint* or set of safety *constraints*. While the *constraints* are derived directly from *hazards*, *control responsibility* needs to be specified in terms of the *process constraint*, i.e. what a particular *controller* is expected to do under which circumstances.

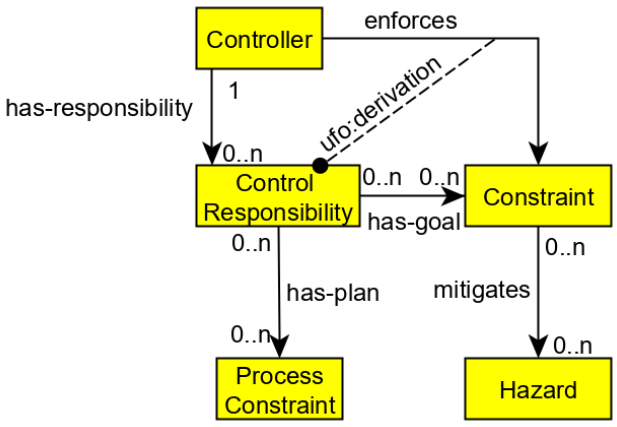


Figure 8 Mapping controller's responsibility to constraints and hazards

Considering now Figs. 5-8 representing the *safety control structure* in the STAMP ontology, the level of detail and the conceptual structure is more precise than the STAMP related literature provides. Not only is the STAMP ontology now guiding (limiting) the safety analyst how to model a safety control structure, but it is providing support to achieve complete, consistent and relevant description of the structure, in a computer-readable format. It has clear advantage of providing the possibility to reuse relevant information about controllers and controlled processes from industrial BPMN-based process documentation, thus saving the time and resources needed to establish particular snapshot of a safety control structure to be used with respective STAMP-based analysis. In fact, the ontology allows establishing complete system description (the entire safety control structure), with the use of the industrial process documentation that shall be maintained by the already existing tasks of process documentation management. The ontology in this respect specifies additional information needed for the purpose of STAMP analysis, that shall be managed either by the process documentation management, or by the SDCPS system as part of an organization SMS. Consequently, the use of STAMP ontology induces some additional effort to establish complete safety control structure and system description, however, it is practically achievable and brings some benefits, e.g. no detailed expertise of the relevant processes or system by the safety analyst is needed, it takes less time and effort to navigate, identify, classify and investigate into an occurrence in terms of STAMP, and the complete system description allows for total system assessment, that may not be possible with usual STAMP analyses.

Furthermore, owing to the formalism and available tools of the UFO ontology, it is possible to implement the STAMP ontology into a software solution, which can assist the user with STAMP-based analyses, and also infer the necessary information partly or fully automatically, i.e. further improving the workflow and user-friendliness of the future STAMP-compatible SMS. To exemplify the inference, if there is an occurrence during the aircraft fueling, it is sufficient for the user to define what the *controlled process* was, while the ontology can infer the relevant controllers, sensors, constraints and hazards, filtering the classification schema (data fields content) of possible contributory factors. The occurrence reporting form would generate data fields with relevant classification and after storing the record, the safety data would be directly mapped onto the existing process documentation. In case all the safety occurrences are stored in this fashion, the total system safety assessment will be enabled.

Taking into account all the mentioned practical implications about the STAMP ontology and the way it allows to carry STAMP-based analyses, the new Safety-II based SMS software will allow these features for the first time. There is no other software solution, what would allow implementation of the STAMP theory into the SMS framework to the extent it is now possible with the STAMP ontology.

3.3 Use case of occurrence reporting

The STAMP ontology supports all safety-relevant use cases, i.e. safety-guided design and engineering, safe operation and control of systems and accident investigation. Since the INBAS Reporting Tool was developed as an SDCPS to collect and process safety data from operations (in the Czech aviation organizations mostly used for safety occurrence reporting and investigation), the use case of investigation was selected as the first to be implemented within the new SDCPS software solution.

This use case has to follow CAST (Causal Analysis based on STAMP) [26], which is a method proposed by the authors of STAMP to support accident investigation use case. This method attempts to explain particular occurrence as a control problem, by means of the safety control structure and particular manifestation of safety issues related to the structure. The use case is described in detail in the Appendix I to this work, together with the STAMP ontology. In this section, only selected scientific highlights related to the use case are discussed.

An instructive example of how aviation safety data change with the application of STAMP ontology is depicted in Fig. 9. The figure shows an example of occurrence where conveyor belt driver at the airport damaged aircraft during ground handling process. Safety data in the contemporary meaning are colored in red and magenta. These are the boxes (here all instances) connected with relations compatible with both STAMP and ASO ontologies. They represent the proximate events from CAST, or a chain of events as used with INBAS Reporting Tool (cf. Fig. 3). Using causality in this regard is not compatible with Safety-II, i.e. a chain of events that represents cause-effect relationships is truly a Safety-I perspective. On the other hand, the meaning of the *caused* relationship is not semantically delimited in the ontology, but rather preserved from the ASO ontology until resonance becomes part of the SDCPS ontology with adoption of FRAM and RAG related concepts. Only then it will be possible to draw more precise line between the usage of the governing principles from Tab 2. To outline few possible perspectives, one of the modeling alternatives is it that the *caused* relationships will be transformed into some type of relationship that rather represents chronology of the occurring factors than necessarily a cause-effect relationship. In other alternative, it still may be true that under some conditions the *caused* relationship, in the sense of representing cause-effect, will hold given the granularity of the system under consideration (i.e. a non-complex system). This will, however, need to be decided in the future research; the STAMP ontology does not address the issue yet.

Going back to Fig. 9, STAMP ontology introduces the yellow, orange, blue and green concepts, together with their relationships. These concepts represent aviation safety data extension, i.e. data that are not collected today, or are collected separately with no reference to safety

management. Yellow color represents data about the safety control structure as per the theory of STAMP, orange boxes specify unsafe control actions derived from the safety control structure, blue color-coded boxes represent data normally available with process documentation, that can be reused for the STAMP-based analyses, and finally green boxes represent the possibility of specifying participating objects in the controlled processes (recall the new *hazard* definition, which is a disposition of participating objects in an occurrence).

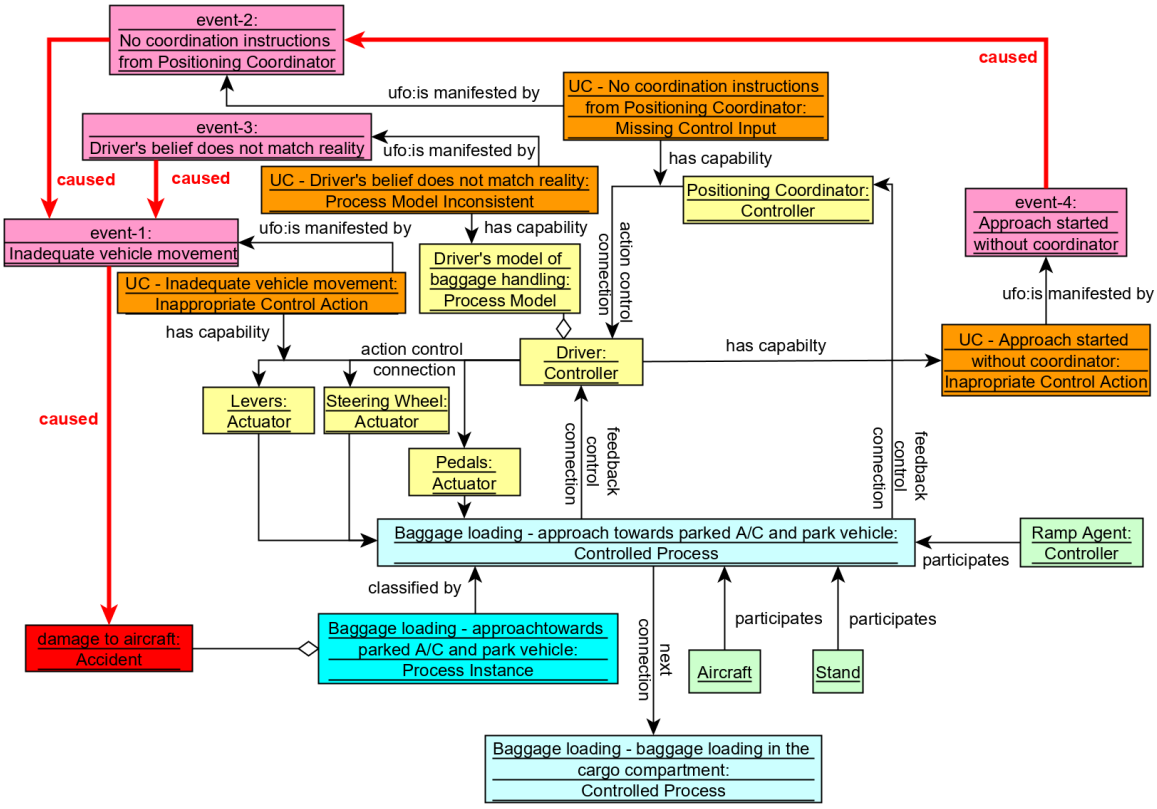


Figure 9 Safety occurrence reporting with STAMP ontology

The mapping and instantiation in Fig. 9 follow the STAMP ontology, but only part of the data needs to be provided by the user. Today, to represent a chain of events (either with INBAS Reporting Tool, SISel or any other available software in aviation safety), the safety analyst needs to investigate into the occurrence and with his or her expertise filter the parts of the occurrence (that are the most important) and then search for the most suitable classification, e.g. from the ECCAIRS taxonomy. With the STAMP ontology, this process becomes an interplay of the user interaction, automatic inference and reuse of other data sources[6].

[6] Note that Fig. 9 is an attempt to visualize the new aviation safety data architecture, but in practice the data will be stored in a database (such as RDF4J suitable for storing information about subjects, predicates and objects) by means of occurrence reporting and investigation forms, where the user fills in the information and does not need to draw similar schemas.

In case of the occurrence in Fig. 9, the user needs to specify either that something happened to a conveyor belt driver, or during baggage loading process – approach toward parked aircraft (here with the possibility to either specify more detailed process steps, or more generic, such as “aircraft handling”[7]), or that something happened to an aircraft, or that it happened on stand. The user may even provide multiple choices simultaneously, starting from the accident, i.e. only specifying relevant hazards/safety constraints etc. There are many alternatives an occurrence report can be stored, all leading to the same outcome. Given the user’s choice, the STAMP ontology can progressively filter the safety control structure and automatically execute some steps of CAST, directing the user to the step, when asked to specify the chain of events (or just events with unknown relationships, if necessary) composing the overall occurrence. Here, the events that can possibly happen are derived from process documentation, or from a combination of the process documentation with generic STAMP taxonomy (available in [3]).

The classification event types (in Fig. 9 the part of the event labels after colon, adhering to Unified Modeling Language (UML) notation [27]) are derived as a negation of the expected, normal behavior specified in the process documentation. Example of an event type derived from process documentation is “Approach started without coordinator“ in Fig. 9. The documentation normally specifies that an approach with conveyor belt into a position from where baggage can be unloaded from or loaded into the aircraft, must be initiated with the positioning coordinator on site, supervising the process. An example of an event derived from generic STAMP taxonomy is “Driver’s belief does not match reality” as an instance of “Process model inconsistent” event type, which is an event type provided by the authors of STAMP aligned with the process documentation (with the “Driver’s belief does not match reality”). Event types suitable for classification of particular occurrence are thus also filtered and displayed to the user for selection, and possible specification (such as stating that “Process model inconsistent” was present, in this particular example as the “Driver’s belief does not match reality”).

With respect to an occurrence, the user shall be encouraged to think of as many as possible relevant hazards, safety constraints, processes etc. and specifying them. All the background mapping can be inferred by the ontology to reduce the burden of the safety analyst, providing him or her with more room to think about the overall occurrence. For instance, in Fig. 9 fully sufficient would be to specify that something happened during baggage loading process – approach toward parked aircraft, select the event types for events 1-4 and finally state what was the accident (the red box). All the other mapping is inferred automatically by the ontology

[7] Note that this limits the classification choice accordingly, i.e. selecting that something happened during aircraft ground handling leads to display of more possible hazards and safety constraints compared to when more specific process is selected.

and with the use of the process documentation. The alternative pathways described before increase user-friendliness and reduce the chance of storing incomplete or irrelevant data. The methodology in Appendix I provides more practical views on this occurrence, which will not be discussed here.

As long as all the safety data are stored as in the example in Fig. 9, system-level safety dashboard and statistics can be proposed. Here, it can be argued that the currently available safety dashboards in aviation SMS system do provide some overview related to the entire system, but this does not compare with the system level perspective enabled by the application of STAMP and the ontology. The clear difference is that all data are stored with mapping to process documentation, i.e. to the description of how management imagines the work is carried in respective operations. Safety dashboard can be, therefore, composed of queries with the new data, such as (1) which processes are most often present in safety occurrences? (2) how do these processes fail or contribute to the occurrences? (3) which roles (controllers) are present in the occurrences and (4) in which ways inadequate control occurs? These are all questions that are both diagnostic and formative, i.e. they diagnose the system but inherently guide the safety analyst to take appropriate measures. This is something the current safety dashboards with safety performance indicators are missing, since they only evaluate occurrence of events, such as how many runway incursions there were this year? Such queries are only diagnostic, but not formative.

Now considering the safety performance measurement and predictions (recall the APF methodology with the mathematical predictions mentioned at the beginning of this work), they inherit the problems of safety performance indicators, since the measurement and predictions is exclusively based only on diagnostic queries. The formative part provided by the STAMP ontology enables entirely new information that can become predictors in the stochastic models. With the tracking of the process documentation modifications, effectiveness of particular measures can be evaluated. Evaluation of the new predictors may possibly guide the safety management to either take different measures, or check if the issue is not the difference between the formal description of the system and the actual practice in operations. Either way, the management can be guided to take adequate measures in a way that is currently not enabled in the industry.

Lastly, few remarks should be made about the achieved step toward Safety-II with the new STAMP ontology. Even though resonance was not yet incorporated into the ontology, some of the positive data related to Safety-II already are. The new SDCPS based on STAMP ontology will use description of how normal work is carried to explain how occasionally things fail. This is clear step toward Safety-II, as in Safety-I only failures and malfunctions are considered, with

cause-effect relationships. The STAMP ontology avoids this limitation by considering the possibility that normal work precedes accidents and gives the possibility to the safety analyst to identify how this can be possible. This relates to the setup of the safety control structure, which may not be adequate for controlling specific safety issues in particular environment. In Safety-I perspective, only the manifested failures are monitored by safety experts, where occasionally some of them may finally question the normal work conditions. In STAMP, by contrast, the normal work documentation is present in every analysis and can provide perspectives, from which it may become evident how normal work actually contributes to the accidents, even to less experienced safety analysts.

3.4 Use case of safety studies

Parallel to the development of the STAMP ontology, separate use case was researched for the sake of its incorporation into the future Safety-II SMS. The use case regards safety studies, i.e. safety assessment of modified or a new system. In the aviation, this use case is frequent, not only for major changes in the industry (new type of aircraft, new airport or runway, new type of communication, navigation or surveillance equipment with respective procedures etc.), but also smaller-scale changes, such as redesign of an aircraft stand or change of key safety management personnel in an organization. The use case is specific for attempting fictional investigation into possible future accidents, thus dealing with predictions and estimations.

Because of the STAMP ontology, the use case of safety studies was also based on the theory of STAMP. Not only this provides immediate opportunity for implementation with the STAMP ontology, but similar to the selection of STAMP for the SDCPS, the model would be preferred for this research anyway, because of the same reasons as for the SDCPS. The method provided by the authors of STAMP to carry system safety assessment is STPA (Systems-Theoretic Process Analysis) and the research of the safety studies was based specifically on this method.

Returning back to the conceptualization of STAMP, we as a society cannot do more about preventing accidents than to design and execute adequate control, that can minimize the likelihood of an accident. To design and execute *control* well, however, is not an easy task. STAMP says that we shall start from the system-level, i.e. first define the hazards that occur as a product of the overall system behavior. Here, the question might be what the system is, but for the sake of practicality and reference to the previous examples, let us assume the system is the aircraft and do not account for ATC service or other environmental aspects relative to aircraft. Given the safety records and the aviation safety taxonomies, to set up a finite set of possible system-level hazards is not an issue. In the example, they are all about

aircraft getting into some hazardous condition, be it a location of the aircraft or loss of some critical technical functions due to extrinsic or intrinsic causes. As a second step, STPA proposes to define safety *constraints*, i.e. requirements for the system behavior. In this logic, it is possible to establish and detail complete set of *hazards* and safety *constraints*, which allow for design and execution of corresponding *control*. In the example of an aircraft, this is normally done by developing the aircraft control systems and training the flight crew.

While the theory of STAMP is clear at first glance, it is apparent that STAMP analysis may get quickly out of control. To establish complete set of an aircraft-related hazards, with detailed mapping to constraints, corresponding systems and pilot actions that provide the necessary control, is a painstaking task that cannot be managed by a single person. In this respect, the developed STAMP ontology can provide support similar to the occurrence reporting use case.

Separate question for safety studies is risk assessment, which was not addressed in the previous use case. As soon as hazards are identified, and possible accident scenarios derived from the safety control structure in place, the second key activity is to execute risk assessment and prioritize or decide about the necessity and nature of mitigation measures. The authors of STAMP discuss the questionable nature of conventional risk matrix, especially the problem of probability estimation [29]. When assessing new system or modification of existing system, history data may not be applicable or available and so it is common that safety experts estimate the probability. The estimation is obviously biased, however, and in some case it may be wrong (e.g. with the B787 batteries, Maneuvering Characteristics Augmentation System (MCAS) system on B737 MAX series aircraft etc.). The authors of STAMP already proposed some measures that can be adopted [3] [29] but the question in this research was whether there can be new assessment tool introduced in the aviation that would limit this bias and provide support for more precise evaluation. The tool was proposed as a new type of risk matrix, here using the concept of safety space (see Fig. 10).

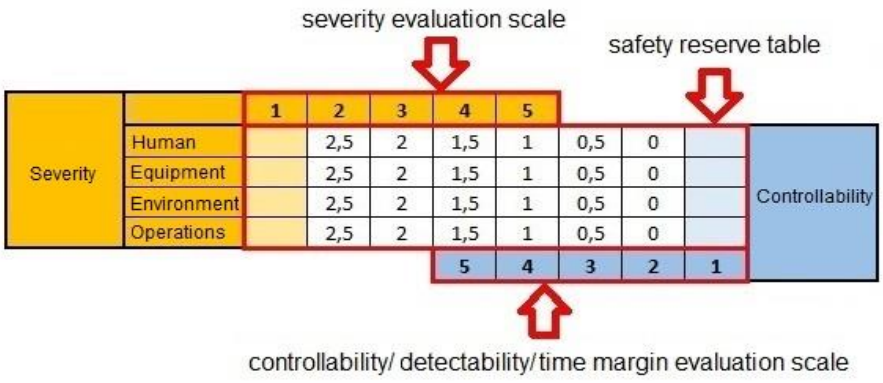


Figure 10 The concept of safety space for risk assessment

The matrix in Fig. 10 has two parameters similar to the conventional risk matrix, but probability is replaced with other criteria, namely controllability, detectability and time margin. The goal was to propose and reuse parameters that are easier to assess than probability, more specifically, parameters that can be assessed given the STAMP-based system description (especially the safety control structure). The new criteria together with the retained severity assess accident scenarios that can be inferred from the established safety control structure and assess whether and how much opportunity there is to execute control over the progressing scenario (controllability), how well the sensory network is designed to aid the controllers with timely and precise information about the progressing scenario (detectability) and how much opportunity (time available) there is for each controller to properly execute necessary control. Severity is retained from risk matrix, i.e. the last criterion is assessment of how severe the outcome would be should the accident scenario realize completely. The only difference to conventional risk matrix severity is specification of the impact on humans, environment, equipment and operations separately, as the severity may be different for each.

The concept of safety space works similar to risk matrix, where higher probability means less tolerance to severity and vice versa. In Fig. 10, severity 5 is the most serious, whereas the scale for controllability is reversed, i.e. controllability 5 is the lowest. Overall risk is the sum of the values in the safety space that are not used by either of the criteria. If severity is 2 for all specifications (human, equipment, …), it means that the matrix cells with values of 2,5 would be all covered with yellow, similar to the cells in the column under the severity value 1, and the sum of the remaining values in the safety space would be by 10 less than with severity level 1. From this it follows that scenario with severity 5 in all criteria and with simultaneous controllability 5 would mean overlap of the two criteria in the safety space, resulting in lack of safety space, and subsequently negative values of risk. The assessment in Fig. 10 shows only the table for severity-controllability, but similar tables would be established for the other two criteria, together composing the overall risk assessment. Finally, Fig. 11 presents risk tolerability with the same use of color coding as in standard risk matrix.

Figure 11 Risk tolerability with the new safety space concept

The research brought new discoveries that are relevant for the aviation. Is was confirmed that STAMP can be used for the use case of safety studies effectively, retaining the key methodological aspects of the current safety studies in the aviation (cf. Safety Assessment Methodology by EUROCONTROL [30], which is fully compatible with the new risk assessment)

but still executing the key step toward Safety-II based SMS, i.e. providing the system-level perspective and description of normal work, that serves as a foundation for hazard and risk analysis. What needs to be changed is conceptualization of hazards and accident scenarios, in line with the theory of STAMP and the developed STAMP ontology. Then, the proposed risk assessment can complement the hazard identification, where probability does not need to be assessed anymore, but is replaced with easier-to-assess criteria. Further, the output is still representable in the logic of current risk matrix and can be computed with basic IT tools, such as Microsoft Office, or easily implemented into any advanced SMS solution, including the second release of SDCPS developed by the author and his team. It does not pose significant change to the paradigm of how safety studies are carried today, nor does it introduce significant requirements for new infrastructure or personnel training.

Description of the researched use case of safety studies with details of how the safety space-based risk matrix shall be applied in the aviation is available in the Appendix J to this work. The work was carried in the research project No. TJ01000252 with the support of Technology Agency of the Czech Republic. Project partner was Prague Airport.

LALIŠ, Andrej, Slobodan STOJIĆ, Markéta KAFKOVÁ and Oldřich ŠTUMBAUER. *Methodology for performing safety studies in the aviation by means of quantitative methods.* Certified methodology by the Ministry of Transport, Czech Republic, 2019.

Appendix J

4 Conclusions

The goal of the described research in this work was to progressively research and develop solutions that will enable Safety-II SMS in the aviation. The research started from the domain of safety performance monitoring and predictions, because this is one of the key features of any SMS and the mathematical means that enable predictions lay down requirements for data to be used for effective predictions. Afterwards, the new aviation safety data architecture was researched based on the current architecture and aviation safety taxonomies, and the first domain ontology was released (the Aviation Safety Ontology). Based on the ontology, the new safety data collection and processing system was developed and deployed for testing with major aviation organizations in the Czech Republic. In the later stages, the system was extended and modified for the use case of aviation safety oversight and deployed also with the Civil Aviation Authority of the Czech Republic. The research continued with the extension of the domain ontology to cover first of the systemic prediction models of safety, specifically the STAMP. The ontology was developed and tested with aviation safety data from the research partners. It provides technical means for all the safety-related use cases, but the use cases of occurrence reporting and safety studies were researched first.

The results of the research indicate that it is possible to use stochastic modeling for safety performance predictions and that the modeling techniques provide basic requirements for data to be used for effective predictions. The research of the new data architecture showed that ontology-based solutions provide the technical foundation for effective management of robust data and information, which are typical for contemporary aviation, and that the ontology enables adaptive occurrence reporting forms, which are necessary for interaction with the user and for user-friendliness. In fact, the ontology provided improved data architecture compared to the expert-based hierarchical structures available in the taxonomies, as the ontology is computer-readable and its semantics enables advanced querying of the data stored according to it. It also redefined safety performance indicators from expert-based and maintained event types with particular operations to a query with the new ASO-based safety database. The first release of the safety data collection and processing system was validated with the research partners and two of them use the system in real operations until today. The release for the Czech CAA is also used in the operations today. The subsequent research on the STAMP ontology showed that it is possible to incorporate STAMP model into the aviation SMS framework and provided technical means to achieve it. The STAMP ontology resolved similar issues as did the ASO ontology with aviation safety taxonomies, i.e. the ontology specified details of the STAMP model that are normally left to interpretation of respective safety analyst, enabled organization and industry-wide application of STAMP-based methods and workflow, and ultimately introduced the first key steps toward the development of Safety-II foundations

of the aviation SMS. The second release of the safety data collection and processing system will work actively with system description and use normal work specification according to STAMP to explain why and how accidents happen.

The research, however, is limited in some aspects. First, the safety performance predictions were researched with limited data samples. This is the issue of the current data architecture in the aviation and so the stochastic modeling will need to be repeated as soon as there are new architecture data available in sufficient amount, i.e. at least three consecutive years. This can be done with the aviation safety ontology-based data but preferably shall be done after the second release of the SDCPS is deployed in the real operations, presumably during the year 2020, with sufficient data collected with the system. The reason for this is the fact that the second release will enable entirely new predictors for stochastic modeling that are not available today and that will enable larger datasets than are possible today. Separate limitation is the fact that only five aviation organizations (including the CAA) tested and validated the developed systems and ontologies. In the future, larger sample of diverse organizations shall be included in the testing and validation of the solutions. The last limitation is the fact that only the use cases of occurrence reporting and safety studies were covered so far, and none of them can be considered at the final stage of development, due to other safety models and methods than need to be considered in the future.

With respect to the above-mentioned, there are still some challenges left for future research. Safety-II based SMS covers several use cases in different types of aviation organizations, of which some were not addressed yet, so as there are more systemic prediction models of safety available today than the STAMP. The future research will need to thoroughly cover the remaining use cases and theoretical foundations of Safety-II, with thorough validation with as many as possible aviation safety organizations to complete the system. It is clear that the achievement of aviation Safety-II SMS is ambitious goal and more effort still needs to be spent on further research and development tasks. However, it is very important to take these next steps, if the level of safety is to be retained or improved in the future aviation operations.

References

[1] ICAO. *Annex 19 - Safety management: international standards and recommended practices*. Montréal, Quebec: International Civil Aviation Organization (ICAO), 2016. ISBN 978-92-9249-965-5.

[2] ICAO. *Doc 9859: Safety Management Manual (SMM)*. Fourth Ed. Montréal: International Civil Aviation Organization (ICAO), 2018. ISBN 978-92-9258-552-5.

[3] LEVESON, Nancy. *Engineering a safer world: systems thinking applied to safety*. Cambridge, Mass.: MIT Press, 2011. Engineering systems. ISBN 978-0-262-01662-9.

[4] REASON, James. The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society B*. 1990, 327(1241), pp. 475-484.

[5] EDWARDS, Elwyn. Man and machine: Systems for safety. In: *Proceedings of British Airlines Pilots Association Technical Symposium*. London: British Airlines Pilots Association, 1972, pp. 21-36.

[6] HOLLNAGEL, Erik, David WOODS and Nancy LEVESON. *Resilience engineering: concepts and precepts*. Burlington, VT: Ashgate, 2006. ISBN 978-0754649045.

[7] Aviation Safety Network. *Statistics* [online]. Flight Safety Foundation, 2019 [cit. 2019-09-10]. Available from: https://aviation-safety.net/statistics/

[8] ICAO. *Doc 10004: 2017-2019 Global Aviation Safety Plan* [online]. Second Ed. Montréal, Canada: International Civil Aviation Organization (ICAO), 2016. Available from: http://www.icao.int/Meetings/a39/Documents/GASP.pdf

[9] EUROCONTROL. *A White Paper on Resilience Engineering for ATM* [online]. Brussels: European Organisation for the Safety of Air Navigation (EUROCONTROL), 2009. Available from: https://www.eurocontrol.int/sites/default/files/2019-07/white-paper-resilience-2009.pdf

[10] HOLLNAGEL, Erik. *Safety-I and Safety-II: The Past and Future of Safety Management*. CRC Press, 2014. ISBN 978-1-4724-2305-4.

[11] HOLLNAGEL, Erik. *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*. CRC Press, 2012. ISBN 978-1-4094-4551-7.

[12] HOLLNAGEL, Erik. *FRAM: Safety-II in Practice: Developing the Resilience Potentials*. Routledge, 2018. ISBN 978-1-138-70892-1.

[13] EUROCONTROL. *From Safety-I to Safety-II: A White Paper* [online]. Brussels: European Organisation for the Safety of Air Navigation (EUROCONTROL), 2009. Available from: http://www.skybrary.aero/bookshelf/books/2437.pdf

[14] DEKKER, Sidney. *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems*. Ashgate Publishing, Ltd., 2011. ISBN 978-1-4094-2221-1.

[15] GRANT, Eryn, Paul SALMON, Nicholas STEVENS, Natassia GOODE and Gemma READ. Back to the future: What do accident causation models tell us about accident prediction? *Safety Science*. 2018, 104, pp. 99-109. DOI: 10.1016/j.ssci.2017.12.018.

[16] LINTNER, Thomas M., Steven D. SMITH, Antonio LICU, Radu CIOPONEA, Simon STEWART, Arnab MAJUMDAR and Marie-Dominique DUPUY. *The measurement of system-wide safety performance in aviation: Three case studies in the development of the aerospace performance factor (APF)*. 2009.

[17] EUROCONTROL. *The Aerospace Performance Factor (APF): Developing the EUROCONTROL ESARR2 APF* [online]. Brussels: European Organisation for the Safety of Air Navigation (EUROCONTROL), 2009. Available from: http://aloftaviationconsulting.com/publications/ECTL_APF_Implementation_Plan.pdf

[18] ROELEN, A.L.C., J. VERSTRAETEN, L. SAVE and N. Aghdassi. *Framework Safety Performance Indicators*. Deliverable 2.1. 2014. Aviation Safety and Certification of new Operations and Systems (ASCOS), EU FP7 funded research project. Available from: https://www.ascos-project.eu/downloads/ascos_wp2_nlr_d2.1_version-1.5.pdf

[19] SM ICG. *Measuring Safety Performance Guidelines for Service Providers*. Safety Management International Collaboration Group (SM ICG), 2013. Available from: https://www.skybrary.aero/bookshelf/books/2395.pdf

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

[21] Commission Implementing Regulation (EU) 2015/1018 laying down a list classifying occurrences in civil aviation to be mandatorily reported according to Regulation (EU) No 376/2014 of the European Parliament and of the Council. Brussels: *Official Journal of the European Union*, 2015, L163/1.

[22] GUIZZARDI, Giancarlo. *Ontological foundations for structural conceptual models. Enschede*, Netherlands: Centre for Telematics and Information Technology, Telematica Instituut, 2005. ISBN 90-75176-81-3.

[23] GUIZZARDI, Giancarlo and Gerd WAGNER. Dispositions and Causal Laws as the Ontological Foundation of Transition Rules. In: *Proceedings of the 2013 Winter Simulation Conference: Simulation: Making Decisions in a Complex World*. 2013, pp. 1335-1346.

[24] GUIZZARDI, Giancarlo, Gerd WAGNER, Riccardo de ALMEIDA FALBO, Renata S. S. GUIZZARDI and João Paulo A. ALMEIDA. Towards Ontological Foundations for the Conceptual Modeling of Events. In: *Lecture Notes in Computer Science*. Springer, 2013, pp. 327-341. ISBN 978-3-642-41923-2.

[25] ALLWEYER, Thomas. *BPMN 2.0: Introduction to the Standard for Business Process Modeling*. Second Ed. Books on Demand, 2016. ISBN 978-3-8370-9331-5.

[26] LEVESON, Nancy. *CAST Handbook: How to Learn More from Incidents and Accidents* [online]. 2019. Available from: https://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf

[27] ARLOW, Jim and Ila NEUSTADT. *UML 2 and the Unified Process: Practical Object-Oriented Analysis and Design*. Second Ed. Addison Wesley, 2005. ISBN 978-0321321275.

[28] LEVESON, Nancy and John P. THOMAS. *STPA Handbook* [online]. 2018. Available from: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[29] DULAC, Nicolas and Nancy LEVESON. Incorporating Safety Risk in Early System Architecture Trade Studies. *Journal of Spacecraft and Rockets*. 2009, 46(2), pp. 430-437. DOI: 10.2514/1.37361.

[29] EUROCONTROL. *Safety assessment methodology – e-SAM* [online]. Brussels: European Organisation for the Safety of Air Navigation (EUROCONTROL), 2006. Available from: https://www.eurocontrol.int/sites/default/files/content/documents/nm/safety/SAM_Electronic_v2.2.zip

[30] LEVESON, Nancy and John P. THOMAS. *STPA Handbook* [online]. 2018. Available from: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Appendix A

LALIŠ, Andrej. Time-series analysis and modelling to predict aviation safety performance index. *Transport Problems*. 2017,12 (3), pp. 51-58. DOI: 10.20858/tp.2017.12.3.5

TRANSPORT PROBLEMS 2017 Volume 12 Issue 3
PROBLEMY TRANSPORTU DOI: 10.20858/tp.2017.12.3.5

Keywords: aerospace performance factor; safety evaluation tools; safety performance index; signal analysis; stochastic control

Andrej LALIŠ
Czech Technical University in Prague, Faculty of Transportation Sciences
Horská 3, Prague 2, 128 03, Czech Republic
Corresponding author. E-mail: lalisand@fd.cvut.cz

TIME-SERIES ANALYSIS AND MODELLING TO PREDICT AVIATION SAFETY PERFORMANCE INDEX

Summary. Safety performance index is a tool with the potential to grasp the intangible domain of aviation safety, based on quantification of meaningful aviation safety system properties. The tool itself was developed in the form of Aerospace Performance Factor and is already available for the aviation industry. However, the tool turned out to be rather unsuccessful as its potential was not fully recognised by the industry. This paper introduces performed analysis on the potential and it outlines new features, utilising time-series analysis, which can improve both the recognition of the index by the industry as well as the motivations to further research and develop methodologies to evaluate overall aviation safety performance using its quantified system properties. This paper discusses not only the features but also their embedding into the existing approach for the development of aviation safety, highlighting possible deficiencies to overcome and relating the scientific work already performed in the domain. Various types of appropriate time-series methodologies are addressed and key specifications of their use with respect to the discussed issue concerning safety performance index are stated.

1. INTRODUCTION

Aviation safety is one of the most studied domains today. Technology used by airplanes and airports reached a very high level of safety and reliability; nevertheless, accidents and serious incidents still happen. Even though the frequency is very low – only 4 fatal accidents in almost 38 million flights per year 2015 [1] – there still exists significant political commitment [2] to improve this performance. Recent commercial aviation incidents and accidents are, however, becoming more and more complex issues [3], which makes this commitment quite a challenge. For various reasons, traditional methods for preventing them do not work sufficiently any more. As an instance, the otherwise very successful Reason's model is rather ineffective against the background of today's aviation safety issues [4], primarily due to the industry complexity, in which not only its components but also complex interactions between them matter. Surely, the model can still be used for understanding particular issues in terms of proximity events, but to truly achieve the goal of any further and stable aviation safety improvement, the solutions are still to be researched today. It is the complexity that makes today's accidents difficult to prevent.

To a certain extent, it is questionable how much the existing level of safety in aviation can still be improved, but given the present status and goals in the domain of aviation safety [2] and system theory and safety engineering knowledge [4], further improvements appear manageable. Because the industry is a socio-technical system in its very nature, solutions must first be capable of handling the intangibility induced by the presence of humans both in the operations as well as high in the management and organisational structure. Even though humans as individuals are still the subject of research in aviation [5, 6], neither the human factor nor the technology itself is recognised as the core

issue [7]. The industry demands more systemic solutions to handle the high complexity of its internal and external interactions.

To date, these interactions are handled by human controllers, whether it is regulation or management of the respective aviation organisation. Decades of industry globalisation and commercial flying established rules and regulations for the best practice to handle the most common emerging issues [8, 9], but a gap still exists as far as the flawed interactions of recent accidents are concerned. Not only are they complex and difficult to effectively prevent, but they suggest that there are some background issues that are hardly manageable because of commercial privacy or many different motivations and goals of the humans involved. The interface between aviation components in many cases lies between two or more separate organisations that often compete on the market and are unwilling to share safety information to the extent that would allow completing the full picture of what happened, which is also recognised in recent surveys indicated by lower reporting activity [10].

One of the possible solutions to this rigour is to research, develop and implement tools, which would be based on quantification of system properties, which are reasonably quantifiable while still intangible. Some such attempts already exist: key safety performance indicators and safety performance measurement are the examples of efforts to quantify intangible safety. These efforts are limited and still fragmented, however, as no effective aviation safety performance framework exists.

Tools capable of effective quantification of respective system properties are to be complemented by system theory-based knowledge and best practice. This way, current safety management can be shifted to a brand-new level, exploiting the capabilities of today's mathematics and safety engineering. Undoubtedly, the solutions to be researched have serious potential to surpass existing safety management in both effectiveness and complexity and it arguably needs to be decomposed into two main separate parts: the quantification of system properties and system theory-based safety engineering. This paper will provide an overview of the approach to solutions being developed to quantify aviation safety system properties within an on-going junior research project.

2. PERFORMANCE INDEX

Safety performance indicators can be subjected to deeper analysis and aggregated into safety performance, sometimes referred to as safety performance index. This index serves as a tool providing an integrated view on safety data and assessing how well the actual safety management is performing within the respective organisation or industry, depending on the type of indicators being aggregated [11]. It has the potential to influence safety management's decisions as it points safety managers to the most influencing issues in terms of the overall level of safety at any time, prioritising their work towards areas of higher concern.

In the domain of aviation safety, the way to obtain a safety performance index was defined as Aerospace Performance Factor (APF). The APF is based on hierarchically structured safety performance indicators, weighed by their pair-wise comparison by subject-matter experts. The core equation to obtain the APF is as follows [12]:

$$APF = \frac{\sum_{i=1}^{k} W_i \cdot N_i}{appropriate\ denominator} \tag{1}$$

where 'W' is weight of respective safety performance indicator, 'N' is the number of indicator observations and 'k' refers to total number of safety performance indicators in the system. The appropriate denominator may depend on the type of aviation organisation and, for example, hours flown or sectors flown in the time interval of interest can be used here [13]. Safety performance indicators used by EUROCONTROL to calculate the APF were defined based on ESARR2 requirements (see Fig. 1) and are specified for Air Navigation Service Providers.

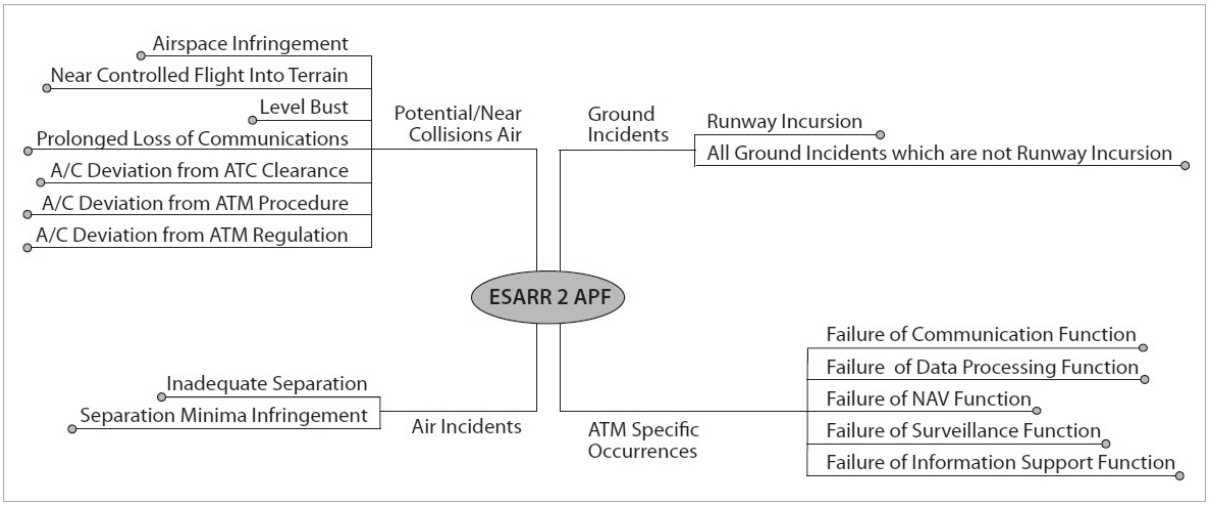


Fig. 1. APF safety performance indicators [12]

These indicators comprise just the tip of the aviation safety iceberg, but to outline the methodology, they are sufficient. Monthly quantified APF for the time interval from January 2006 to December 2008 using the safety performance indicators from Fig. 1 is depicted in Fig. 2. The APF is shown in black colour, its constituents (four main groups of indicators) in grey and the red line is a simple linear regression analysis to indicate the trend. In this case, the APF refers to the achieved level of safety for the European Air Traffic Management (ATM) system, providing safety management with overall safety performance supervision. The safety management concerned may subject the achieved APF to analysis and see which of its constituents has contributed most to influence the APF.

From the perspective of resolving issues outlined in the previous chapter, the APF or safety performance index offers a tool to quantify system properties, but it heavily depends on the selection of safety performance indicators to be aggregated. Omission of any 'symptoms' to be captured by the indicators may lead to serious incapability of the index to perform as intended. This problem is amplified by the fact that the aviation industry is highly dynamic and these indicators need to be constantly revised. Another issue is the quality of safety data, which originate from different sources whether within an organisation or between two or more aviation stakeholders. These sources frequently overlap and when it comes to classification or description of the issue, it is not rare that they draw a slightly different picture. Certainly, this is also caused by the absence of an effective framework for aviation safety data classification, but there are already efforts spent to resolve this issue [14].

Despite the methodology being already available in year 2009, so far, the application of this tool for commercial aviation has been very limited. Both issues described above contributed to the lack of its application, but the potential for future extension and application still exists. It can be recognised, especially, in the context of today's industry-wide efforts [2] to develop safety management to the stage at which tools to quantify system properties will find more extensive application within future risk management of advanced safety management systems. Important to note is that despite the present situation in aviation, the APF methodology affected the definition of safety performance indicators adding some requirements for their form and structure.

3. NEED TO PREDICT

There is some unexploited potential of the APF itself, which could expedite deployment of the solutions being researched today. The potential is recognised with regard to predictive analysis of the signal obtained from APF measurement in time (see Fig. 2).

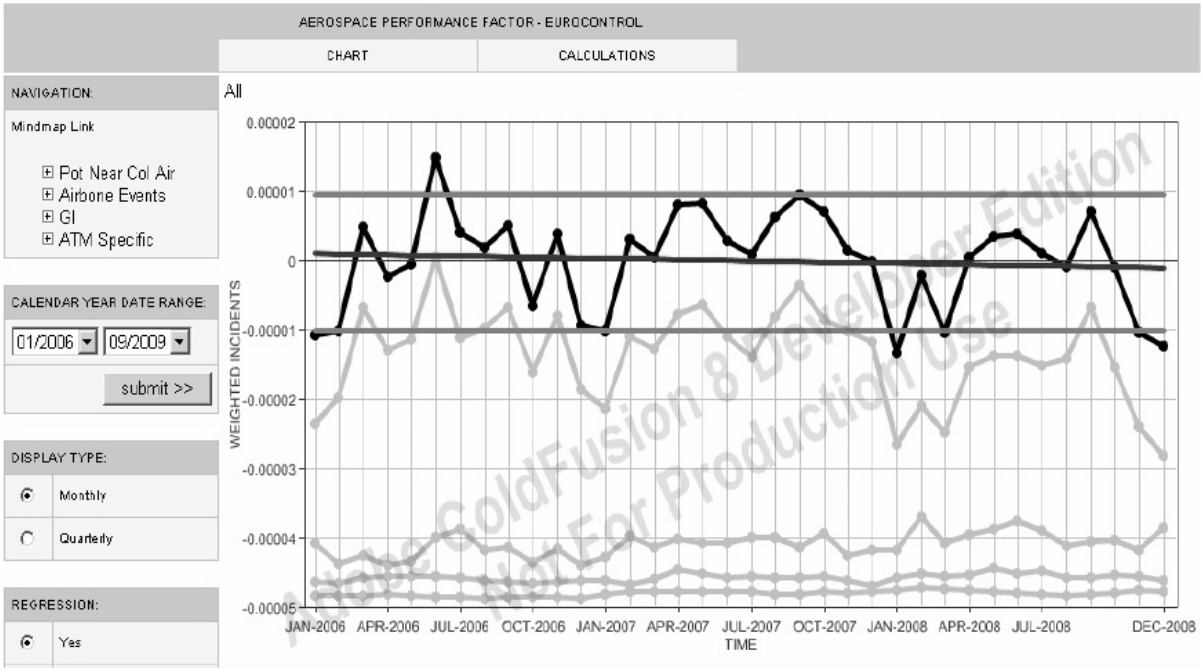


Fig. 2. APF measured from 2006 to 2008 [13]

The safety management's decision process on whether to take some actions can be facilitated by providing the management with predictions. If the management would know, given the past APF values, what will most likely happen next, it would be much easier to see at least how important it is to intervene in the system. The issue was already formulated and addressed to a certain extent in other scientific work [15]; however, the approach was specific for an Italian environment and did not account for other possible solutions to the problem. Similar demand for effective prognoses exists in economy, in which central banks monitor inflation rates or GDP growth and, based on their short-time predictions, they safeguard the stability of their controlled part of the economy, with there are already being quite advanced solutions in place nowadays [16].

The depicted APF in Fig. 2 resembles a similar kind of signal as we can observe in econometrics, which may be processed by time-series analysis in order to analyse it for further dependencies. The APF in Fig. 2 does not seem to bear any significant trends but, rather, a stable behaviour, which is also confirmed by the red linear regression. However, it may contain some dependencies when decomposed into its elements, such as seasonality, which could be discovered by robust time-series analysis. Likewise, other external variables may influence the APF. Definition of the approach to this type of analysis (predictions) and its appropriate embedding into the concepts of future safety management has the recognised potential of expediting safety management development and introducing new features to be implemented with regard to safety performance and its indicators.

4. TIME-SERIES ANALYSIS

Unlike the research already performed to predict safety performance [15], this paper promotes robust exploitation of time-series analysis. The reason is that, with respect to this, the Italian case was rather limited by its use of maximum likelihood estimation (MLE) and autoregressive and moving average models to predict safety occurrences filtered by the Pareto principle, such as Traffic Collision Avoidance System (TCAS) related issues. The problem is that the idea of predicting future events as a core solution for safety performance predictions, even as an estimation, leads to serious bias by its nature. The solution to this problem appears to be the prediction of the APF (safety performance index) instead, with optional utilisation of external and internal explanatory variables. There are

several methods that allow predictions of univariate time-series, such as the APF, to various extents [17]:

- linear trend and mean (constant) model
- random walk models
- averaging and smoothing models
- linear regression models
- autoregressive and moving average models (ARMA) and their variations

The decision of which one to choose depends on many qualitative properties of the time-series analysed, such as trend patterns, correlations among variables, seasonality, etc. In theory, the elementary decision process to follow was already defined decades ago [18].

The main characteristic of the APF signal from Fig. 2 is the clear presence of a seasonal element as measured on a monthly basis. It is also underlined by the fact that, in aviation, the demand is variable and dependent on the season of the year, influencing the denominator in the APF equation. Similarly, the signal is influenced by growth or shocks in the global economy but there are other external explanatory variables influencing the numerator of that equation too, such as effectiveness of safety management, safety culture and others that aviation safety is directly related to. Further, the signal will most likely be influenced in a dynamic way, i.e., a perturbation will resonate the sample, suggesting internal dependencies. In addition, some of the external variables may be correlated.

According to all these presumptions, our needs fit best in the last two models to further assess the APF–linear regression model capturing seasonality and explanatory variables, and in the autoregressive and moving average model of the same capabilities.

5. LINEAR REGRESSION MODELS

Linear regression models are typically based on ordinary least squares (OLS) and they obey the following form [19]:

$$y_t = c + X_t\beta + u_t \tag{2}$$

where y_t is the response series, c is the regression model intercept, X_t is the matrix of concatenated predictor data values, i.e., observation of each predictor series, β is the regression coefficient and u_t is the disturbance or noise. Time runs discretely here, i.e., $t \in \mathbb{N}$. Applied on the safety performance index, the index itself will be the response whereas the predictor will capture all the explanatory variables. Parameters β and c are calculated coefficients from both predictor and response series data.

The model requires all variables to be scalars that may cause difficulties as far as ‘soft’ variables are concerned. Fortunately, it is not necessary to include all the variables that affect the index; thus, only those that are easy to quantify should be included as a starting point. As soon as the model provides meaningful output, adding new explanatory variables shall progressively reduce the noise and make the predictions more accurate. The same is valid for all other estimations the model is capable of providing, i.e., the estimation of explanatory variables affect the index captured in parameter β.

6. ARMA MODELS

These models are typically based on MLE and they obey the following form (in lag (L) operator notation) [20]:

$$H(L)y_t = c + X_t\beta + N(L)\varepsilon_t \tag{3}$$

where

$$\begin{aligned} H(L)y_t &= \varphi(L)(1-L)^D\,\varphi(L)(1-L^S) \\ &= 1-\eta_1 L-\eta_1 L^2-\cdots-\eta_P L^P \end{aligned} \tag{4}$$

is degree P lag operator polynomial capturing the effect of both seasonal and non-seasonal autoregressive (AR) polynomials, and

$$N(L) = \theta(L)\Theta(L) = 1 - \upsilon_1 L - \upsilon_2 L^2 - \cdots \upsilon_Q L^Q \quad (5)$$

is degree Q lag operator polynomial capturing the effect of both seasonal and non-seasonal moving average polynomial (MA), ε_t is a white noise innovation process and other variables are equivalent to those in the linear regression model described above.

The model itself offers one important difference compared with the linear regression model: it has the moving average component that accounts for historical values of disturbances in the form of white noise innovation process ε_t. In simple terms, the model recognises dependence among variables and both present and historical values of disturbance. Although this feature seems to have the capability to capture interesting and valuable characteristics of the system, a problem may arise when it comes to the principle for quantification of the actual disturbance:

$$\varepsilon_t = y_t - \overline{y}_t \quad (6)$$

where $\overline{y}_t$ is the predicted value of the response series at time t-1. Because there is no better way to estimate the disturbance, it is questionable whether the moving average component would not actually bias the model and reduce its performance. The response series in the form of safety performance or APF is just an estimation of this system-wide property and, assuming that its measurement is not biased, may add additional noise to the ARMA model. However, the actual performance is to be assessed on real data in order to distinguish between the ARMA and linear regression models or, in other words, between OLS and MLE application.

7. MODEL COMPARISON

The selection of either the ARMA or the linear regression model depends on the data and system to which these time-series analysis models are to be applied. Because the required aviation safety data are difficult to obtain because of their confidential nature and potential for causing damage to brand recognition, the performance of each of these models can be assessed unbiasedly using synthesised data. Such data, however, would never be able to simulate the real environment entirely and, thus, both models to be subjected to performance analysis have strong potential to perform similarly when using artificial data. The optimal solution would be for aviation organisations to decide to try these methods to analyse quantified system properties of their own discretion in order to discover their true potential.

As per the analysis outlined in this paper, and according to the theory, the safe bet appears to be the selection of the linear regression model, because of its simplicity. ARMA models are more complex and may perform better, but one should be cautious about apparent shortcomings with the disturbance calculation and, therefore, favour autoregressive elements with possible distributed lags rather than moving average components.

Finally, it is important to mention the integration of the predictions with other properties of the aviation safety system. One should bear in mind all the traps of predicting a biased signal when key ‘symptoms’ are not captured in the quantification process or when reluctance to build the full picture of what happened exists. This is the case when moving average model components are inevitable and when serious bias is the risk. This problem may be partly solved by breaking down the safety performance into its subcomponents (clusters of indicators) and applying predictions on these elements, or trying to resolve these issues with the latest safety engineering practice, i.e., by thorough system analysis.

In all cases, application of either of these two types of models determines the form of input, i.e., it lays down new requirements for safety performance indicators. As all predictor variables are to be scalars, the same is true for safety performance indicators. Although for some this means no change, other indicators such as effectiveness of safety management or safety culture need to be transformed into reasonable form for processing. The indicators can be transformed in many ways but, at this stage, it is difficult to identify the best transformation. Thorough analysis of the model performance using real data and various indicator transformations can determine it.

8. CONCLUSIONS

This paper summarised the options for applying robust time-series analysis for the purpose of safety performance index prediction. The ambition was to shift the existing ideas and approach to explore new ways for achieving future predictive risk management, namely by exploiting both mathematical capabilities and recent safety engineering practice and principles.

Apparent limitations lie with practical verification of the analysis performed. This is due to the limitations imposed by aviation safety data confidentiality and general reluctance to share the data between aviation organisations. On the other hand, the paper provides some insight for future research, which may identify ways to overcome the data confidentiality issue. As an alternative, synthetic data may be used to fill the gaps in the available data to estimate the potential of the proposed solution. The greatest potential for future research is recognised in application of systemic solutions with employment of explanatory variables for the purpose of safety performance index predictions.

Acknowledgement

This paper was supported by the Grant Agency of the Czech Technical University in Prague, grant No. SGS16/188/OHK2/2T/16.

References

1. IATA, 2016. *Safety Fact Sheet*. International Air Transport Association. Montreal. Canada. Available at: https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-safety.pdf
2. ICAO, 2013. *2014 - 2016 Global Aviation Safety Plan: Doc 10004*. International Civil Aviation Organization, Montréal, Quebec, Canada. ISBN 978-92-9249-355-4.
3. Vittek, P. & Lališ, A. & Stojić, S. & Plos, V. 2016. Runway incursion and methods for safety performance measurement. In: *Production Management and Engineering Sciences. Proceedings of the International Conference on Engineering Science and Production Management (ESPM 2015).* Tatranská Štrba, High Tatras Mountains. Slovak Republic. 16th-17th April 2015. Bratislava: University of Economics in Bratislava. P. 321-326. ISBN 978-1-138-02856-2.
4. Leveson, N. Engineering a safer world: systems thinking applied to safety. Cambridge, MA: MIT Press. *Engineering systems*. 2011. ISBN 978-0-262-01662-9.
5. Novák, L. & Němec, V. & Soušek, R. Effect of Normobaric Hypoxia on Psychomotor Pilot Performance. In*: The 18th World Multi-Conference on Systemics*. Cybernetics and Informatics. Orlando, Florida: International Institute of Informatics and Systemics. 2014. Vol. II. P. 246-250. ISBN 978-1-941763-05-6.
6. Regula, M. & Socha, V. & Kutílek, P. & Socha, L. & Hánaková, L. & Szabo, S. Study of heart rate as the main stress indicator in aircraft pilots. In*: 16th Mechatronika 2014*. Brno: Brno University of Technology. 2014. P. 639-643. ISBN 978-80-214-4816-2.
7. ICAO, 2013. *Safety Management Manual (SMM): Doc 9859. 3rd edition*. International Civil Aviation Organization. Montréal. ISBN 978-92-9249-214-4.
8. Kraus, J. & Vittek, P. & Plos, V. Comprehensive emergency management for airport operator documentation. In: *Production Management and Engineering Sciences: Proceedings of the International Conference on Engineering Science and Production Management (ESPM 2015).* Tatranská Štrba, High Tatras Mountains, Slovak Republic. 2016. Bratislava: University of Economics in Bratislava. P. 139-144. ISBN 978-1-138-02856-2.
9. Fuchs, P. & Němec, V. & Soušek, R. & Szabo, S. & Šustr, M. & Viskup, P. The Assessment of Critica Infrastructure in the Czech Republic. *In Proceedings of 19th International Scientific Conference Transport Means*. Kaunas: Technologija. 2015. P. 418-424. ISSN 1822-296X.

10. Post, W. *ECCAIRS Survey*. Presentation at [ECCAIRS Steering Committee Meeting, Brussels, 26-27 October 2015]. Joint Research Centre. Brussels, Belgium. Available at: http://eccairsportal.jrc.ec.europa.eu/index.php/Documents/39/0/.
11. TRADE. *A Handbook of Techniques and Tools: How to Measure Performance*. 1995. U.S. Training Resources and Data Exchange Department of Energy, Washington, DC. Available at: Internet: http://www.orau.gov/pbm/handbook/handbook_all.pdf
12. EUROCONTROL. *The Aerospace Performance Factor (APF): Developing the EUROCONTROL ESARR 2 APF*. 2009. European Organisation for the Safety of Air Navigation Brussels, Belgium. Available at: http://aloftaviationconsulting.com/publications/ECTL_APF_Implementation_Plan.pdf.
13. Lintner, T.M. & Smith, S.D. & Licu, A. & Cioponea, R. & Stewart, S. & Majumdar, A. & Dupuy, M.D. *The measurement of system-wide safety performance in aviation: Three case studies in the development of the aerospace performance factor (APF).* 2009. Available at: https://www.eurocontrol.int/eec/gallery/content/public/document/other/conference/2009/safety_r_and_d_Munich/day_1/Tony-Licu-(EUROCONTROL)-Steve-Smith-(FAA)-Paper.pdf
14. EASA, 2015. *ECCAIRS Taxonomy and NoA Update. Presentation at [ECCAIRS Steering Committee Meeting, Brussels, 27th October 2015]*. European Aviation Safety Agency, Brussels, Belgium. Available at: http://eccairsportal.jrc.ec.europa.eu/index.php/Documents/39/0/.
15. Di Gravio, G. & Mancini, M. & Patriarca, R. & Costantino, F. Overall safety performance of Air Traffic Management system: Forecasting and monitoring. *Safety Science.* 2014. Vol. 72. P. 351-362.
16. Rochelle, M.E. & Gurkaynak, R.S. How Useful are Estimated DSGE Model Forecasts for Central Bankers? *Brooking papers on Economic Activity, Economic Studies Program. The Brooklins Institution.* 2010. Vol. 41 (2 (Fall)). P. 209 -259.
17. Nau, R.F. *Statistical forecasting: notes on regression and time series analysis* [*online*]. Duke University: Fuqua School of Business. Durham. 2016. Available at: http://people.duke.edu/~rnau/411home.htm.
18. Chambers, J.C. & Mullick, S.K. & Smith, D.D. How to choose the right forecasting technique. *Harvard Business Review*. 1971. Vol. 49. No. 4. P. 45-74.
19. Kutner, M.H. & Nachtsheim, Ch.J. & Neter, J. & Wasserman, W. *Applied Linear Statistical Models: 5th Edition.* Irwin, The McGraw-Hill Companies. 2005. ISBN 0-07-238688-6.
20. Box, G.E.P. & Jenkins, G.M. & Reinsel, G.C., 1994. *Time Series Analysis: Forecasting and Control. 3rd ed. Englewood Cliffs.* NJ: Prentice Hall. 1994.

Received 23.03.2016; accepted in revised form 08.09.2017

Appendix B

LALIŠ, Andrej, Vladimír SOCHA, Petr KŘEMEN, Peter VITTEK, Luboš SOCHA and Jakub KRAUS. Generating synthetic aviation safety data to resample or establish new datasets. *Safety Science*. 2018, 106, pp. 154-161. DOI: 10.1016/j.ssci.2018.03.013.

Safety Science 106 (2018) 154–161

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Generating synthetic aviation safety data to resample or establish new datasets

Andrej Lališ[a,*], Vladimír Socha[a], Petr Křemen[b], Peter Vittek[a], Luboš Socha[c], Jakub Kraus[a]

[a] Faculty of Transportation Sciences, Czech Technical University, Prague, Czech Republic
[b] Faculty of Electrical Engineering, Czech Technical University, Prague, Czech Republic
[c] Faculty of Aeronautics, Technical University of Košice, Košice, Slovakia

ARTICLE INFO

Keywords:
Aviation safety
Data resampling
Data simulation
Safety management system
Safety performance
Aerospace Performance Factor

ABSTRACT

Aviation safety data are limited in availability due to their confidential nature. Some aggregated overviews already exist but in order to effectively use the data, it is important to fill the gaps of their existing limitations. For some data, there are not enough data points in order to process them through advanced analysis. For other, only expert assumptions can be obtained. In both cases, these shortcomings can be addressed via proper data resampling or simulation where little effort can make the data suitable for various research and development initiatives. Examples of real aviation safety data made public are demonstrated together with key principles of how to perform their resampling. Then, for cases where only expert assumptions are available, general solution to the transformation of the assumptions into simulated data is introduced. The goal is to demonstrate how to transform accessible data or knowledge about aviation safety into data samples with sufficient granularity. The results provide general solution suitable not only for aviation safety data and knowledge, but also for similar transportation or high-risk industries related data issues, indicating that both the data resampling and simulation provide an option for generating datasets, which can be used for statistical inferential methods, linear regression modelling, recurrent analysis etc. Example of data resampling application is included in Aerospace Performance Factor calculation for years 2008 up to 2015.

1. Introduction

To date, aviation safety is subject of intensive research in terms of new information technology deployment. It is recognised, that further progress in this domain can be achieved by implementing technology, which collects, processes and analyses safety data in order to produce system-wide information of how the system performs on safety (ICAO, 2013). This information is to be used for safety-critical decision-making within safety management system as far as the aviation is concerned, but this principle is generally true for other high-risk industries as well (Niu and Song, 2013; Klein and Viard, 2013). One of the features of the system-wide information is that it cannot be reliably derived by individuals from the data available because aviation became very complex, i.e. hardly manageable for humans. The industry is distributed system of many types of stakeholders (airspace users, organisations, regulators, manufacturers, policy makers etc.) which use different technologies, different procedures and which overlap with each other to various extent. As a result, safety performance of one stakeholder may be severely affected by how safety is managed by other stakeholder and it can be difficult to identify this from either side.

Today's accidents only support this claim. They consist of long chain of events and contributing factors, which typically exceed responsibilities of one stakeholder and its safety management (Socha et al., 2014). From the perspective of managing safety, it is important to have some sort of full picture to be able to apply effective measures to prevent modern accidents. The distributed character of aviation, however, sets constraints for achieving such a full picture. Not only are the data and the full picture to be established distributed in parts among the stakeholders, but also the nature of both is often confidential and may have potential to damage someone's position on the market, if misused. Aviation authorities encourage organisations and other stakeholders to share safety data, experience and safety knowledge (ICAO, 2013; European Commission, 2010) but the degree of these activities is still not perceived to be satisfactory. This paper does not aim to resolve this issue but rather address its consequences, namely limited safety data availability.

Research and development initiatives in the domain of aviation safety are restricted by the safety data not being available. Whilst it may be possible to sign some bilateral confidential agreement between two parties, this is still rather difficult to achieve for multiple

* Corresponding author at: Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Horská 3, 128 03 Prague, Czech Republic.
E-mail address: lalisand@fd.cvut.cz (A. Lališ).

https://doi.org/10.1016/j.ssci.2018.03.013
Received 22 September 2016; Received in revised form 20 February 2018; Accepted 8 March 2018

stakeholders at the time. Fortunately, some of the data are regularly (annually) published by authorities in form of aggregated overview of key safety issues (such as Safety Regulation Commission, 2016; EASA, 2016 or Federal Aviation Administration, 2015), but this is true only for some segments of the industry, e.g. for air navigation services providers (ANSPs). These providers have a lot of advanced technology and data at their disposal and they are typically state-owned monopolies, which are not subject of market competition. The latter was likely the key factor for making some of their data publicly available.

To better understand the issue, it is important to note basic facts of data evolution in this domain. Safety was always measured indirectly, i.e. through its absence (Reason, 2000). It is quite hard to find any effective way to measure it directly as it is the case for conventional measurements related to more tangible issues (Hanakova et al., 2017). Overall safety is intangible system property and even where it is possible to measure it directly, it is often impractical because measuring the things which go right simply means a lot of effort to be spent in order to have meaningful records. Unlike safe state, unsafe outcomes are not only less frequent but they are much more tangible thus considerably easier to track (Hollnagel, 2014). Aviation accidents and incidents attract society from early days of its existence and for decades they were the best driver for safety improvements. As soon as they became rare, the focus just shifted to incidents and safety occurrences with their contributing factors, which, according to investigations, lead to the accidents.

Recently, a new type of data emerged in this domain. Tracking back the root causes of accidents led to the discovery of the so-called organisational factors denoting those contributing factors, which stem from how safety management and safety oversight work (ICAO, 2013). Until the discovery of the importance of how aviation organisations and regulatory bodies are set up as entities, no safety management system nor any sophisticated safety oversight were needed. Progressive requirements for gathering how organisations and regulatory bodies approach safety from management perspective appeared first around the year 2010 (European Commission, 2010; EASA). These requirements established datasets different in their very fundamentals; they assess activities which can hardly be associated with specific unsafe behaviour but which are capable of generating background on which unsafe behaviour emerges. Starting to collect this type of safety data was significant milestone for aviation safety as it brought the industry closer to generate the full picture.

Nowadays, we are closer to the full picture as the content of collected data evolved, but due to the insufficient data sharing and confidentiality restrictions, they are typically not available for research and development initiatives. This inhibits the progress of introducing new technology which could integrate and process the data so that all parties would benefit from industry-wide, open data based knowledge. So has the progress to be achieved the other way. Current research initiatives have to make the best use of public but restricted data samples to come with solutions that aviation organisations may trial and which would expedite establishing the full picture.

Data scarcity, however, is not a new issue. There are several studies available to date, which propose methodologies to overcome this issue in different applications. In fact, very few deal with this problem in scope of safety (such as Yu et al., 2017; El-Gheriani et al., 2017, which are only oriented to major accidents); much more frequent are studies oriented to system reliability, failure and risk assessment in terms of data uncertainty and its reduction. Both safety and reliability oriented studies are typically using Bayesian approach in some variations to produce a posterior distribution by combining data, expert knowledge or various simulation results. Among other methods, first order reliability method and Monte Carlo simulation (Awadallah et al., 2016), or grey system theory (Wen et al., 2011) are used in respective applications. Special attention in the literature is paid to expert elicitation, which was already formalised in several publications (such as Meyer, 2001; Keeney and von Winterfeldt, 1991 or Aven and Guikema, 2011). All the methodologies are, however, difficult to apply directly on the problem in this work as they require various inputs which are out of the scope of this paper. The problem here is of more generic nature, even though it can be complemented with the methods from other studies.

With respect to the afore-mentioned, this article describes the public aviation safety data in detail and provides solutions for how to overcome their limitations. It suggests generating either synthetic aviation safety data or resampling the data already available. The motivation to use data resampling is based on the need to decompose existing signals to increase their granularity for the purpose of further processing and analysis. Data simulation complements this approach by extending the possibility to generate entirely synthetic signals.[1] Synthetic data have their apparent limitations but the important aspect is that they can enable application of advanced analyses, even for experimental or learning purposes only, where real data do not allow it. Direct application of mathematical tools and methods, such as statistical inferential procedures, autoregression or recurrent analysis, to make inferences about safety performance (the full picture) would be otherwise impossible. To enable the tools and methods, it is important to resample the data, i.e. to transform annual figures into month, week or day distribution. For cases where no data are available, simulation based on expert assumptions can provide the solution.

Taking into account the goal, this paper deals with methodology of both data resampling and simulation. It describes data and identifies the gap for improvement. The methods are applied on selected figures from real datasets in the domain of aviation safety. At the end, aviation safety performance is computed using the resampled data to exemplify the contribution of the proposed solution.

2. Methods

This section details the proposed methodology to achieve the goal of this paper. At first, aviation safety data are specified, including their sources, relevant issues and examples. At second, data resampling follows with description of key principles of how to combine expert knowledge and real datasets to increase data granularity by the means of mathematical functions. Lastly, after the outline of data resampling principles, the methodology further specifies data simulation in order to extend the principles of generating synthetic data to situations where no real data are available.

2.1. Data characteristics

Aviation safety data comprise accidents, incidents and safety occurrences. The data are available in form of aggregated figures denoting number of observations of respective accident, incident or occurrence during given time interval. Additionally, new data types were recently introduced to aviation through the European Union-wide (EU-wide) safety key performance indicators (SKPIs) (European Commission, 2013), which are based on the so-called organisational factors. However, these are using artificial scores and due to their novelty, inherent bias and lack of relevant expert assumptions, they are not considered in the methods of this study.

Aviation accident records were gathered reliably till now and they are publicly available together with investigation reports, including conclusions and corrective measures. These data can be found on website of responsible body for respective investigation.[2] But because aviation accidents became rare, they solely cannot be used for safety management today. In terms of any research and development initiatives, much more valuable are data concerning incidents and safety

[1] For further reading on data resampling and simulation methods refer to Lahiri (2003) and Carsey (2014)).

[2] Such as Air Accidents Investigation Institute (2017) in the Czech Republic or Bundesstelle für Flugunfalluntersuchung (2017) in Germany.

occurrences. These data are published on websites of some aviation authorities, but there are not many yet.

One of the most useful data repositories is provided by European Organisation for the Safety of Air Navigation (EUROCONTROL) on its dedicated performance monitoring websites [3,4,5] and in annual safety- and operations-related reports (Safety Regulation Commission, 2016; EUROCONTROL, 2016). EUROCONTROL provides EU-wide aggregated overview of the most common safety issues in the domain of Air Traffic Management (ATM) and ANSPs in form of interactive dashboards (see Fig. 1) together with many other overall performance-related indicators, such as complexity scores, flight delays, traffic distribution etc. Because the most detailed aviation safety data are provided from this domain, they are used to exemplify generating synthetic data.

At the highest level of detail, ATM related safety data are published on (a) Separation Minima Infringements; (b) Unauthorised Penetrations of Airspace; (c) Runway Incursions and (d) ATM Specific Occurrences. The data include severity distribution for the most severe events (severity A - serious incident and severity B - major incident, as defined in (EUROCONTROL, 1999)) and are available back to the year 2004. Federal Administration Authority (FAA) publishes regularly reports of similar quality in the U.S., but unlike in Europe, no data on organisational factors (structure) are provided. In Europe, the data can also be obtained directly from providers' annual reports but these are not all consistent in their content. Some providers are more advanced in safety and others are less, which results in each ANSP publishing different data.

Table 1 demonstrates the Separation Minima Infringements (SMI) in total numbers from year 2008 to 2015. It shows EU-wide figures of these occurrences, where severity A and B Infringements are extracted and stated separately because they represent the most severe outcomes of this type of occurrence.

For aviation organisations other than ANSPs there are almost no data accessible. Owing to the recent initiatives to establish common reporting scheme in the EU (European Commission, 2014), some data from other organisations are already available on the EU level and basic statistics and knowledge were extracted into newest annual safety review by European Aviation Safety Agency (EASA) (EASA, 2016). Compared to the EU-wide data published by EUROCONTROL, however, it does not provide much level of detail, such as distribution per year and month, or per country and airport.

With respect to the mentioned facts, this study demonstrates the basic principles of resampling using data from EUROCONTROL's repositories, which relate to the listed occurrences measured at the highest level of detail. In fact, its data exclusively can be resampled with no need for complementing them with data from other stakeholders to be able to test, for instance, statistical and stochastic tools to analyse the data.

2.2. Data processing

Data processing can be performed using two methods: data resampling and data simulation. The selection of appropriate method depends on following conditions. The first is real data accessibility and the second is expert assumptions availability. In this study, data resampling is used only if real data are accessible and at least some expert assumptions are provided. Data simulation is used to synthesise data vectors where no real data are accessible but expert assumptions exist. It is possible to use the simulation also in case where no data nor any expert assumptions are available but then the output may be highly questionable.

[3] http://ansperformance.eu/.
[4] http://www.eurocontrol.int/prudata/dashboard/eur_view_2014.html.
[5] http://www.eurocontrol.int/prudata/dashboard/rp2_2015.html.

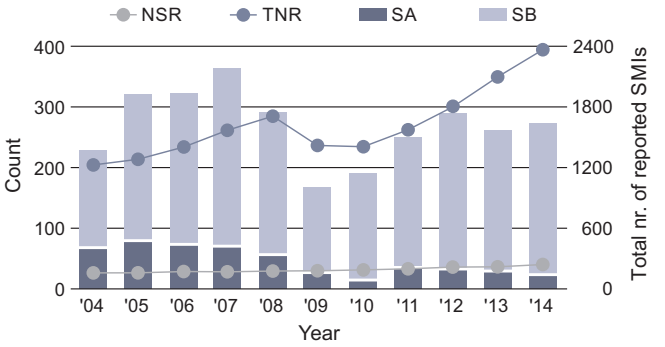


Fig. 1. Separation Minima Infringements (SMI) dataset with number of states reporting (NSR), total number of records (TNR), number of reports with severity "A" type (SA) and severity "B" type (SB).[1] Note that only TNR refers to the right-most y-axis.

Table 1
Separation Minima Infringements (SMI) distribution per year and highest severity.

	2008	2009	2010	2011	2012	2013	2014	2015
SMI severity A	56	24	16	35	29	30	23	20
SMI severity B	236	141	178	217	258	232	250	228
SMI total rep.	1711	1418	1402	1571	1796	2161	2359	2316

2.2.1. Data resampling

First method transforms real data into desired distribution with the help of expert assumptions. Typically, resampling is needed when data granularity is to be increased; even the most detailed data on safety occurrences in aviation are public only as annual figures of occurrence observations but at least distribution by month or week is needed for the deployment of advanced mathematical methods. To resample the data, expert assumptions are to be made before the resampling process starts. In general, regarding safety occurrences similar to SMI, it is true that (a) occurrence rate is higher in summer than in winter; (b) the higher the total amount of reports per year the bigger the difference between peak and trough values; (c) occurrence observations should correspond to the traffic distribution, i.e. maximum number of observations is most likely in July and minimum in January and (d) values are to be natural numbers or zero.

The assumptions are based on following facts. Occurrence rate assumption stems from the fact, that the higher the traffic saturation, the higher the probability of a conflicting situation. This is especially true for today's volumes of traffic reaching maximum capacity of existing airspaces in Europe (Lehouillier et al., 2016) and it is indicated by increasing complexity scores of Europe's ANSPs (EUROCONTROL, 2017). Traffic saturation is known to be seasonal, what can be inferred from traffic figures clearly indicating regular peak values around July and troughs around January, justifying the second assumption. Absolute difference between peak and trough values of occurrence observations during a year can hardly be constant for all safety occurrences; occurrences with hundreds of observations per year should have the difference amplified by their magnitude, causing it to increase. Occurrences with no more than 10 observations per year must remain within their limits. Last assumption relates to the format of occurrences. Any occurrence is a binary variable; either there is an occurrence or there is no occurrence. It is clear that there cannot be negative number of observations and any other than natural number or zero is not conceivable in real world. All these assumptions are general enough to be universal and valid for all safety occurrences similar to the SMI, i.e. for all occurrences on which the data are currently accessible. This is mainly due to the binary property of monitored safety occurrences and their close relation with traffic saturation, especially when reaching limits of given airspace.

Taking into account all these assumptions, following equation

provides basic solution to the problem, where the goal is to resample data into any other distribution with higher granularity:

$$N = \int_0^M k \cdot f(x)dx, \tag{1}$$

where N is annual total number of selected occurrence observations, M is scale determined by the new distribution to be produced, k is coefficient of seasonal variance, x represents time and $f(x)$ is time-dependent mathematical function capturing expert assumptions. Scale M is determined by total number of data points to be produced (e.g. $M = 12$ for data distributed by month whilst N is the total figure per year). Coefficient k may be calculated in many ways but it should be in line with provided expert assumptions. If there are no expert assumptions on the coefficient, one of the possible ways to calculate it is to use average occurrence rate N/M as a starting point because the variance typically depends on this rate: the higher the number of observations per event type, the higher the variance. For datasets by EUROCONTROL, the variance is unknown and no expert assumptions can be considered, so the problem is then shifted to the coefficient k. Based on empirical testing in MATLAB environment (MATLAB R2015b, MathWorks, Inc., Natick, MA,USA) for the purpose of this study, reasonable results with the data samples from Table 1 were achieved with $k = 0.25 \cdot N/M$ (k amplifies $f(x)$ by 25% of the average occurrence rate N/M). The coefficient may be set differently at ones discretion so that the results copy as much as possible what is supposed to be real.

With regard to the Eq. (1), new data distribution can be calculated as follows:

$$N_i = [k \cdot F(x)]_{i-1}^{i}, \quad i = 1,2,...,M, \tag{2}$$

where N_i is number of occurrences during selected time interval i and $F(x)$ is anti-derivative of the integrand (function $f(x)$). Obviously, N_i needs to be rounded in order to fulfil the last assumption about natural numbers or zero. If deemed appropriate, Eq. (2) may be complemented with white noise, which makes the resampling more realistic. The noise can be of any distribution but because Gaussian white noise is good approximation of many real-world situations (Yanushevsky, 2007), it is preferred in this study. Gaussian white noise can be generated using pseudorandom component of Gaussian distribution with mean 0 and variation equal to 1 (such pseudorandom numbers can be produced by MATLAB or similar software). The component is based on the following equation:

$$\vec{\epsilon} = p \cdot \vec{u_i}, \quad \vec{u_i} \sim N(\mu,\sigma^2), \tag{3}$$

where $\vec{\epsilon}$ is vector of final white noise components, $\vec{u_i}$ is vector of pseudorandom Gaussian distributed numbers with mean $\mu = 0$ and variance $\sigma^2 = 1$ and p is noise effect coefficient. The coefficient p amplifies the noise as needed. If the expert assumptions do not include any information about the noise, the variable p should be so that the output will be reasonable, i.e. no extreme differences between each two consecutive resampled points are achieved but on the other hand, the function $f(x)$ should not be clearly visible. In addition, the coefficient needs to be variable with the magnitude of occurrence observations, because the same noise cannot influence data with hundreds of occurrences per given time period in the same way as those with no more than ten. Therefore, p needs to be expressed rather as ratio, dependent on the average number of occurrences of given event type, multiplied by constant as follows:

$$p = r \cdot \frac{N}{M}, \tag{4}$$

where N is number of selected occurrence observations of original distribution, M is scale determined by the new distribution to be produced and r is constant to be set. Experiments performed in this study estimated the value for $r = 0.125$ to fit well the EUROCONTROL data repositories but it may be set different for other cases. The sum of all N_i may not precisely be equal to the real values of N due to rounding the results and adding the noise, but it should remain acceptably close for all cases. This also means that there should not be too much noise added, otherwise the resampling output may exceed reasonable limits.

For the particular expert assumptions introduced in this chapter, data seasonality may be modeled by sinus function:

$$N = \int_0^M k \cdot \sin\left(x \cdot \frac{2\pi}{M} - \frac{\pi}{2} - \frac{2\pi}{M}\right)dx. \tag{5}$$

The sinus uses the expression

$$x \cdot \frac{2\pi}{M} - \frac{\pi}{2} - \frac{2\pi}{M}, \tag{6}$$

to move the extreme values on the interval $\langle 0,M \rangle$ so that its maximum is achieved at the point of $7 \cdot M/12$ (July data) and the minimum at $M/12$ (January data). The sinus function is shifted upwards by constant of integration so that no values are negative. Recalculating new occurrence distribution during given year will, therefore, follow the equation:

$$N_i = \left[-k \cdot \cos\left(x \cdot \frac{2\pi}{M} - \frac{\pi}{2} - \frac{2\pi}{M}\right)\right]_{i-1}^{i}, \quad i = 1,2,...,M, \tag{7}$$

where N_i is number of selected occurrence observations during month i in selected year, M is scale determined by the new distribution to be produced, k is coefficient of seasonal variation and i is successive time step of the series from new distribution.

However, problem may arise as soon as specific requirement exists for resampled data distribution. No data distribution is assured by Eq. (7) but empirical testing showed that Gaussian and various skewed distributions are randomly obtained with the sinus function and k. Safety occurrences in aviation are assumed to follow non-Gaussian distribution (Seshadri, 1998; Wang et al., 2014) which also seems to be the case in other industries, where inverse Gaussian distribution fits incidents and lognormal distribution fits less severe but more frequent non-conformances (Love et al., 2015). Unfortunately, inverse Gaussian distribution could not be obtained from Eq. (7) and there is no general transformation function by which such distribution could be obtained e.g. from Gaussian distributed random variable (Chhikara, 1988), which is frequent product of the equation. The basic solution in Eq. (2) may produce different data distribution with different $f(x)$ and k and so has the investigator first check the distribution of the output from Eq. (2) and then add white noise with appropriate distribution in order to obtain desired distribution of the resampled data. Due to the complexity, however, this may not always be possible.

To demonstrate the resampling method as applied on aviation safety occurrences (Eq. (7)), at this point there is missing only a real figure of annual occurrences of selected event type (variable N_i) and the final decision about how many points are to be obtained from the figure (variable M). In this paper, SMI severity B recorded number of occurrences for year 2011 within the EUROCONTROL region was randomly selected ($N_i = 217$ occurrences) and this figure was resampled into monthly-distributed dataset of 12 figures ($M = 12$) for each month during 2011. The results are in shown in Section 3.

2.2.2. Data simulation

As long as there are no data available and it is important to generate some, assumptions have to additionally include what is available for resampling, i.e. occurrence observation figures. Experts to provide such assumptions are preferred to be front line personnel as they can usually estimate how frequent some occurrences are. For example, an Air Traffic Control Officer (ATCO) can estimate how many times a day or a week does he or she experience Short Term Conflict Alerts (STCA), alerting him or her to some aircraft being on collision course, whether horizontally, vertically or both. Usually, ATCO can also estimate how much does this value vary during a year, providing an estimation for variability as well.

Key principles of the simulation remain the same as for data

resampling, but this time the core lies with pseudorandom number generation. Concerning data simulation, the pseudorandom component will not simulate noise only, but the entire dataset. The distribution parameters are to be fitted to the expert or front line personnel assumptions on the occurrence. The basic solution for data simulation is then as follows:

$$E_i = ||\vec{e_i}|| = \sum_{j=1}^{D_i} e_{ij}, \quad \vec{e_i} \sim IG(\mu_i,\lambda_i) \wedge e_{ij} \in \mathbb{N}^0, \tag{8}$$

where E_i is sum of occurrence observations of event type E during time period i,$\vec{e_i}$ is vector of observations during time period i,D_i is number of data points during time period i and e_{ij} is j^{th} element from the vector $\vec{e_i}$. Vector elements are assumed to be natural numbers or zero and obeying inverse Gaussian distribution with mean μ_i and shape parameter λ_i (both variable with i). In this case, no real data exist which would restrict the simulation and so it can be based on truly inverse Gaussian distribution.

The vector $\vec{e_i}$ is to be generated using pseudorandom numbers as MATLAB or similar software can produce. Average value μ_i and its estimated variance can be provided by an expert, but shape parameter λ_i is difficult to obtain. It can only be reliably inferred from real data samples of similar occurrences. Because data in EUROCONTROL's repositories are not sufficient for such analysis, parameter λ_i will be replaced for the purposes of this study to produce single parameter inverse Gaussian distribution as follows:

$$\lambda_i = \mu_i^2. \tag{9}$$

This distribution allows overcoming the issue with unknown λ_i, but eventually it may not be so different from the distribution based on real data. For lower numbers of occurrence observations (μ_i less than approximately 25), the probability density function is similar in shape to how the distribution of aviation safety occurrences is described by Wang et al. (2014), whilst for larger numbers (μ_i more than 25) it is approaching normal (Gaussian) distribution. Mean μ_i greater than 25 can be prevented simply by utilising the pseudorandom element to simulate data "on daily basis" as it is the case in Eq. (8), where weekly or monthly data can be produced as a sum of daily simulation. This is possible due to additive property of the distribution according to which the sum of inverse Gaussian distributed random variables produces another inverse Gaussian distributed variable under given conditions (Chhikara, 1988). According to all EUROCONTROL's datasets, it is very unlikely, that there would be on average 25 or more observations per an occurrence a day. This way, the desired properties of inverse Gaussian distribution are preserved and can be used to simulate synthetic data. However, the noise induced by the omission of actual λ_i may be significant in some cases, and so should such a simulation be used only when necessary and only for testing of mathematical models, analytical tools etc. The desired noise is added by rounding the values to achieve natural numbers or zero but this may change the distribution. It is therefore highly advisable to perform tests of the produced statistics before the data are used.

To demonstrate the simulator, fictional assumptions (a) STCA is experienced on average 2 to 3 times a day; (b) the average occurrence rate during peak days is by 1 occurrence more a day, and vice versa, the average during trough day is by 1 occurrence less a day; will serve as the basis to synthesise new data.

STCA is a safety occurrence similar to SMI. In fact, it relates to SMI because it is supposed to alert ATCO to prevent SMI or similar situations in advance, but obviously there must be more STCA warnings than SMIs, because STCA under normal operational conditions precedes SMI and only after the conflict is unresolved by ATCO, SMI can emerge. Other assumptions are therefore the same as in the example with data resampling.

The assumptions are to be taken into account in similar way as for data resampling, i.e. by the means of mathematical functions, which quantify the assumptions. For the STCA assumptions, Eq. (8) was complemented with the following equations, using the same sinus function to model data seasonality:

$$\mu_i = k\cdot\sin\left(i\cdot\frac{2\pi}{M}-\frac{\pi}{2}-\frac{2\pi}{M}\right) + x_E, \quad i = 1,2,...,M, \tag{10}$$

$$k = \frac{\max(x_e)-\min(x_e)}{2}, \tag{11}$$

where μ_i is the distribution mean during time step i,k is distribution mean variation, M is scale determined by the new distribution to be produced and x_E is expert assumption on process intercept. Given the assumption on occurrence rate for STCA, the process intercept value (x_E) is 2.5 per day. Coefficient of seasonal variation k can be calculated as the difference between its maximum and minimum estimated value, as follows (by the means of Eq. (11)).

$$k = \frac{3.5-1.5}{2} = 1 \tag{12}$$

If the goal is to generate data distributed by month, D_i corresponds to number of days per each month from January to December and M is equal to 12. Likewise, many other assumptions may be included, which can set different λ_i,x_E and μ_i or even set requirement for different probability distribution of the simulated data. The simulator does not aim to provide solution for every possible scenario but rather provide key principles on how to simulate safety data by reusing the principle of data resampling from previous section.

At this point, the simulator Eqs. (8)–(11) can be used to generate synthetic data for STCA event type according to the afore-mentioned expert assumptions (a) and (b). Variable M was set to 12 as in case of data resampling, D_i included number of days of each month during average year (28 for February) and variable k was set to 1 in line with Eq. (12). The results are in shown in Section 3.

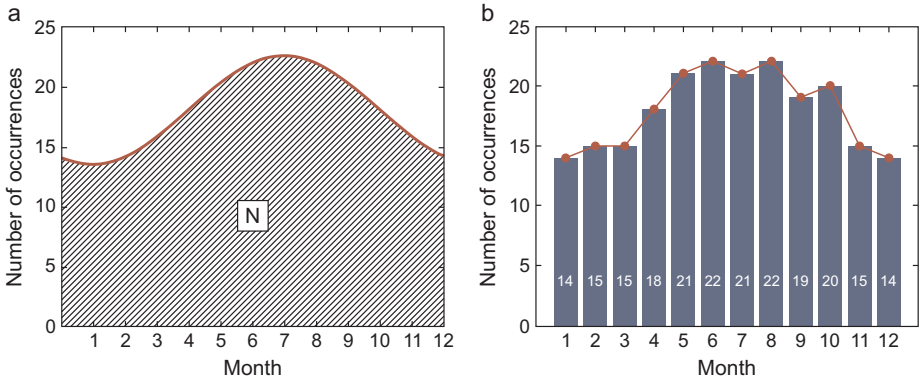


Fig. 2. Basic solution for given assumptions and SMI severity B in 2011 (a) and generated monthly-distributed data according to the basic solution for SMI severity B in 2011 (b).

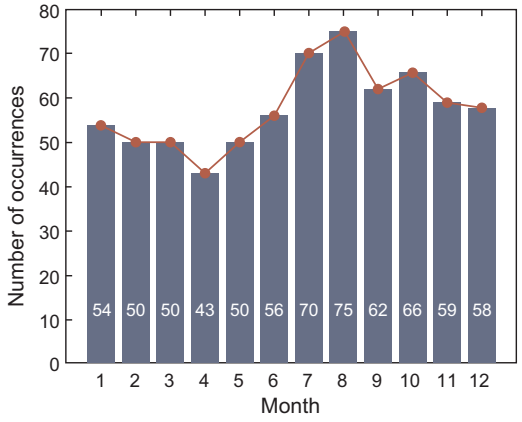


Fig. 3. Example of simulated data for STCA event type.

3. Results

The results of data resampling are depicted in Fig. 2. They are based on SMI severity B from year 2011. Fig. 2a demonstrates the sinus function behind the data resampling equations, where the area below the sinus curve and x-axis equals total number of SMI severity B observations in the year 2011. Fig. 2b depicts resampled data. Pseudorandom component (as per Eqs. (3) and (4) with $r = 0.125$) was added and so the distribution does not follow the sinus function too precisely as it is assumed to be the case during real operations. The data represent occurrence observations distributed by month of the year 2011. Data distribution remains random in this case.

The results of data simulation are on Fig. 3. The simulation is based on the fictional assumptions about STCA event type and the results are distributed by month of a fictional year. For February, 28 days are assumed in this example and the data obey inverse Gaussian distribution.

4. Discussion

The sum of all resampled occurrences on Fig. 2b is 231 which, compared to the real data of 217 occurrences in 2011, shows that the sum of the error induced by rounding and adding the noise was 6.45% thus not so significant.

Concerning data simulation, due to quite a lot of uncertainty put in the simulator (all the assumptions together), each time it runs it usually produces a notably different curve or histogram. This may not always correspond to the reality and thus shall not be preferred over data resampling, but the results make it possible to learn how to build or to trial different methodologies or advanced models where no other options exist. In any case, it is advisable to check on regular basis with experts or front line personnel how the trends evolve in order not to have the simulated data based on obsolete assumptions.

It is possible to use different or even multiple functions $f(x)$ instead of the sinus used in this study for data resampling or simulation equations. However, in such case, it is important to carefully quantify qualitative statements, which produce such need and insert them into the equations as either coefficients, constants or mathematical functions. This study does not aim to provide solutions for any possible case that may exist, but it rather outlines and exemplifies how such simulator and data resampling works, providing general solution for most common issues. On the other hand, the general nature of the proposed methods provides an option for their implementation in other transportation domains or high-risk industries.

When considering the results in terms of other research performed especially in reliability engineering, where similar problems with data unavailability appeared, the overlap with this study regards using more robust functions $f(x)$ or parameter estimation of more optimal function than sinus used in this work. Bayesian approach of integrating different data sources and expert knowledge works with probability density functions of parameters typically pertaining different variables (inputs) composing a regression model to predict future output. This study is, however, focused only on the mathematical models and their application on increasing data granularity. The core principles are also demonstrated on data simulation, but the input available in this study is very limited to allow for robust approach in producing mathematical models. If the inputs necessary to use such modelling are available, Bayesian approach and other methodologies applied to data scarcity can be used to produce more complex and precise model for generating or resampling data. Likewise, additional improvement can be achieved by robust expert elicitation, following the published frameworks suitable for particular application.

Both resampled and simulated data are suitable for applications only as entire datasets. This is because local differences between two consecutive data points may not correspond to the reality at all either due to inaccuracies in expert assumptions or due to added noise, and if only a selection of such data is used for building mathematical models, this may be completely misleading. Therefore, it is highly recommended to use entire datasets and not only their subsets.

As an example of application of the methods in this study, reconstruction of Aerospace Performance Factor (APF) according to the methodology developed by FAA (Lintner et al., 2009) will be demonstrated. Generally, the APF is one of the system-wide information, which can be produced by composing safety data into a single data point, which is intended to quantify level of system's safety performance. Concerning the data published by EUROCONTROL, the APF signal can be reconstructed for several years and in this example, it is calculated from 2008 up to 2015. According to the APF methodology, required are (a) resampled data on selected EU-wide safety occurrences into distribution by month and (b) EU-wide traffic distribution data by month in total hours flown format.

For the selected time period, data on safety occurrences from all EUROCONTROL data repositories were subjected to resampling. The real data sample comprises only 8 data points per each occurrence (distributed by year), i.e. 96 data points per each event type were achieved by the resampling process. It is to be noted here, that EUROCONTROL used for their APF calculation larger datasets concerning the safety occurrences included in the calculation (Neubauer and Lintner, 2010) whilst in this study only the occurrences provided in the public data repositories were used. The reason for omitting majority of safety occurrences used by EUROCONTROL is the complete unavailability of respective safety data. The missing data were not simulated due to that only rough assumptions could be provided. On the other hand, the most critical safety occurrences are included in the public repositories and so simulating the rest of the data could actually introduce more noise to the reconstructed signal than just omitting the data. Therefore, in this case, data resampling was preferred over data simulation. The impact of this decision can be verified through the comparison of the reconstructed signal with EUROCONTROL's output (Fig. 4), because both include year 2008.

With regard to the traffic distribution, the public repositories include annual total figures for flight hours in the EU region, but only for year 2015 the distribution by month is available. On the other hand, the same data for traffic distribution in the EU region are available using different unit, namely average daily movements, for the entire time period both as annual figures as well as figures distributed by month. The procedure to obtain distribution by month for years 2008 up to 2014 needs no resampling because the real data are there and just need to be converted into different units. Most important is to obtain the ratio between the figures as follows:

$$R_m = \frac{ADM_m}{THF_m} \tag{13}$$

where R_m is the calculated ratio, *ADM* is traffic in average IFR daily movement format, *THF* is the same figure in total flight hours format

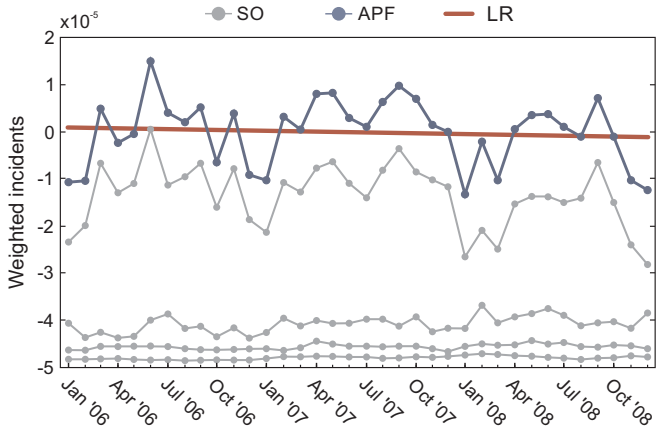


Fig. 4. APF signal based on real data from 2006 to 2008 (Lintner et al., 2009).

and m stands for respective month. Because the traffic figures in total flight hours format distributed by month are accessible for year 2015 only, the ratios R_m can be calculated using data from year 2015 only. Obtained ratios serve then as coefficients to recalculate all the years backwards using Eq. (13) to obtain monthly-distributed traffic data in total hours flown format.

At this stage, all variables are known and the APF signal can be reconstructed. Fig. 5 depicts the results. For the year 2008, reconstructed APF signal is similar to the one on Fig. 4. EUROCONTROL used relative APF figures, which are adjusted to the process mean whilst Fig. 5 demonstrates absolute APF figures, which cause shifting the scale of y-axis. Some difference can be observed, which is certainly attributable to the difference between the data behind each calculation, but comparing the outputs for the year 2008, the two signals are convincingly similar in shape and magnitude.

Last point to discuss is the new type of data on organisational factors. They are publicly available in Europe only, measured from 2012 and referring to the three EU-wide SKPIs, measured at both national and ANSP level. The data contain information on (a) Effectiveness of Safety Management; (b) Application of Just Culture and (c) Risk Analysis Tool (RAT) methodology usage.

This dataset is limited compared to the accidents and occurrences due to its novelty. It is available on the same EUROCONTROL websites together with accidents, incidents and occurrences but methodology and format of these data is obviously different from safety occurrences. To evaluate these SKPIs, artificial scores are used, represented by percentage derived from self-assessment questionnaires (see EASA). These questionnaires, however, provide certain room for bias, and so the data are not comparably accurate to the safety occurrence records. Considering this new type of safety data, no such data resampling or simulation can be used as for safety occurrences. These data are not seasonal nor do they depend on the volume of traffic etc. Their dynamicity is very low; according to the dashboards at EUROCONTROLs websites they tend to change a bit year after a year, but it is quite normal as they refer to things, which are hard to change (such as fundamentals of safety management system), and which are seasonally independent. At this point, resampling the data would more or less just follow even distribution with some linear trend during all the year thus it makes no sense to pay special attention to them. Should this change in the future and new assumptions could be drawn, then similar principles as used in the examples in this paper can be reused to build dedicated simulator for these datasets.

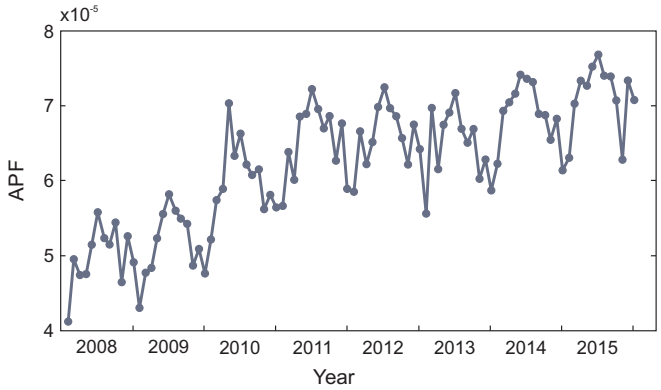


Fig. 5. APF signal based on public data repositories with applied data resampling from 2008 to 2015.

5. Conclusions

Restrictions concerning aviation safety data and their availability lead to the search for solutions, which are capable to overcome them. There are cases in which almost all safety data are accessible and just few data points need to be acquired via data resampling; in other cases there are very little or no safety data available and so they need to be simulated using expert assumptions only. The former can help to verify new methodologies or advanced modelling as they are likely to achieve comparable results with real data; the latter makes it possible to learn how to build or to trial the same methodologies or advanced models as in the former case. Both cases are usable for modern research and development activities in the domain of aviation safety but due to their general nature, they can find application in other transportation domains or high-risk industries. Because the data to be simulated or resampled in aviation are related to socio-technical system, expert assumptions are often of critical importance and are to be considered adequately.

This paper drew basic principles and solutions to the above-mentioned problems. Using basic mathematical functions, expert assumptions were transformed into sets of equations. Were real data were accessible, the equations considered them. Typical problem with such data in aviation is that it is available only annually as total figures whilst month or day distribution is desired. Introduced sets of equations were used for data resampling whilst annual total figures were obeyed. Where no data are available, the solution is based on pseudorandom number generation, such as modern computational software can generate. Mathematical functions then complement the pseudorandom number so that it produces conceivable outcome in accordance with expert assumptions.

It is clear that the synthetic data used to fill the gaps of existing limitations will never contain anything outside of what is inserted in the very equations behind the simulation. Even though they are based on expert assumptions and account for randomness, it is not possible to include all the variables, which affect the values of measured aviation safety data. The less real data and expert assumptions there are, the more inaccurate the resampled or simulated data and vice versa. It is important to note that because the aviation is a socio-technical system, it is unlikely that the system is deterministic. Therefore, there is no ultimate set of assumptions and equations, which describe the system completely and so real data should always be preferred. On the other hand, some of these limitations may be reduced by further research, applying methods from different studies dealing with data scarcity, such as Bayesian approach or Monte Carlo simulation, to refine and perfect the mathematical functions used to generate synthetic data in specific applications.

Despite the limitations, the synthesised data make it possible to implement, verify and validate advanced methodologies or analytical tools, which are highly dependent on data sample size. There are constraints stemming from the confidential nature of aviation safety data but because no aviation stakeholder is willing to share them extensively, under the risk of their misuse and with no assurance what will the benefits be, it seems unlikely that this will improve soon. On

the other hand, a chance exists to improve the situation with new technologies and inventions. At this stage, these can be pre-set up and checked using simulated data and then, if proven, used to demonstrate their capabilities to aviation stakeholders, including regulatory bodies. This may eventually resolve the general unwillingness to share and work with safety data jointly and to establish the full picture of aviation safety. As soon as some technology is proven at least on partially real data, it may eventually convince aviation stakeholders to trial it.

Acknowledgement

This work was supported by the Czech Technical University in Prague [junior research Grant No. SGS16/188/OHK2/2T/16]

References

Air Accidents Investigation Institute, 2017. Reports of accidents and incidents (September 2017). <http://www.uzpln.cz/en/reports>.

Aven, T., Guikema, S., 2011. Whose uncertainty assessments (probability distributions) does a risk assessment report: the analysts or the experts? Reliab. Eng. Syst. Saf. 96 (10), 1257–1262. http://dx.doi.org/10.1016/j.ress.2011.05.001.

Awadallah, A.G., Saad, H., Elmoustafa, A., Hassan, A., 2016. Reliability assessment of water structures subject to data scarcity using the SCS-CN model. Hydrol. Sci. J. 61 (4), 696–710. http://dx.doi.org/10.1080/02626667.2015.1027709.

Bundesstelle für Flugunfalluntersuchung, 2017. Investigation reports (September 2017). <https://www.bfu-web.de/EN/Publications/Investigation%20Report/reports_node.html>.

Carsey, T., 2014. Monte Carlo Simulation and Resampling Methods for Social Science. Sage, Los Angeles.

Chhikara, R., 1988. The Inverse Gaussian Distribution: Theory: Methodology, and Applications (Statistics: A Series of Textbooks and Monographs). CRC Press ISBN: 9780824779979.

EASA, 2016. Annual Safety Review 2016, European Aviation Safety Agency, Cologne, Germany, ISBN: 978-92-9210-202-9. doi:http://dx.doi.org/10.2822/541561. <https://www.easa.europa.eu/document-library/general-publications/annual-safety-review-2016#group-easa-downloads>.

EASA. Safety Key Performance Indicators (SKPI)/Acceptable Means of Compliance (AMC) Amendment 1/Guidance Material (GM) Amendment 1.

El-Gheriani, M., Khan, F., Chen, D., Abbassi, R., 2017. Major accident modelling using spare data. Process Saf. Environ. Prot. 106, 52–59. http://dx.doi.org/10.1016/j.psep.2016.12.004.

EUROCONTROL, 1999. ESARR 2 Guidance to ATM Safety Regulators: Severity Classification Scheme for Safety Occurrences in ATM. <https://www.eurocontrol.int/sites/default/files/article/content/documents/single-sky/src/esarr2/eam2-gui1-e1.0.pdf>.

EUROCONTROL, 2016. Annual network operations report 2015 (June 2016). <http://www.eurocontrol.int/sites/default/files/publication/performance/2015_annual/final-edition/annual_network_operations_report_2015_main_report_final.pdf>.

EUROCONTROL, 2017. Pan-European ANS Performance data repository (September 2017). <http://ansperformance.eu/data/performancearea/>.

European Commission, 2010. Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC. Text with EEA relevance. Official J. Eur. Union OJ L 264, 25–27. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:295:0035:0050:EN:PDF>.

European Commission, 2010. Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC. Text with EEA relevance. Official J. Eur. Union OJ L 264, 25–27. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:295:0035:0050:EN:PDF>.

European Commission, 2013. Commission Implementing Regulation (EU) No 390/2013 laying down a performance scheme for air navigation services and network functions. Official J. Eur. Union OJ L 128, 1–30. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:128:0001:0030:EN:PDF>.

European Commission, 2014. Regulation (EU) No 376/2014 of the European Parliament and of the Council on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007. Official J. Eur. Union OJ L 122, 18–43. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0376&from=EN>.

Federal Aviation Administration, 2015. Air Traffic Organization: 2015 Safety Report. <https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/safety/media/2015_safety_report.pdf>.

Hanakova, L., Socha, V., Socha, L., Szabo, S., Kozuba, J., Lalis, A., Vittek, P., Kraus, J., Rozenberg, R., Kalavsky, P., Novak, M., Schlenker, J., Kusmirek, S., 2017. Determining importance of physiological parameters and methods of their evaluation for classification of pilots psychophysiological condition. In: 2017 International Conference on Military Technologies (ICMT). IEEE. http://dx.doi.org/10.1109/miltechs.2017.7988810.

Hollnagel, E., 2014. Safety-I and Safety-II: The Past and Future of Safety Management. CRC Press ISBN: 978-1-4724-2305-4.

ICAO, 2013. Safety management manual (SMM), third ed., International Civil Aviation Organization, Montreal, Quebec, ISBN: 978-92-9249-214-4.

ICAO, 2013. Global Aviation Safety Plan 2014-2016, first ed., International Civil Aviation Organization, Montreal, Quebec, ISBN: 978-92-9249-355-4.

Keeney, R., von Winterfeldt, D., 1991. Eliciting probabilities from experts in complex technical problems. IEEE Trans. Eng. Manage. 38 (3), 191–201. http://dx.doi.org/10.1109/17.83752.

Klein, T., Viard, R., 2013. Process safety indicators in chemical industry – what makes it a success story and what did we learn so far? Chem. Eng. Trans. 31, 391–396. http://dx.doi.org/10.3303/CET1331066.

Lahiri, S.N., 2003. Resampling Methods for Dependent Data. Springer, New York, New York, NY.

Lehouillier, T., Soumis, F., Omer, J., Allignol, C., 2016. Measuring the interactions between air traffic control and flow management using a simulation-based framework. Comput. Indust. Eng. 99, 269–279. http://dx.doi.org/10.1016/j.cie.2016.07.025.

Lintner, T., Smith, S., Lieu, A., Cioponea, R., Stewart, S., Majumdar, A., Dupuy, M.-D., 2009. The measurement of systemwide safety performance in aviation: three case studies in the development of the aerospace performance factor (apf), vol. 2, pp. 1060–1104. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-77952276172&partnerID=40&md5=09f92af816dc732b263f9e5d7c9b1465>.

Love, P.E., Teo, P., Carey, B., Sing, C.-P., Ackermann, F., 2015. The symbiotic nature of safety and quality in construction: incidents and rework non-conformances. Saf. Sci. 79, 55–62. http://dx.doi.org/10.1016/j.ssci.2015.05.009.

Meyer, M., 2001. Eliciting and Analyzing Expert Judgment: A Practical Guide. Society for Industrial and Applied Mathematics and American Statistical Association, Philadelphia, PA.

Neubauer, K., Lintner, T., 2010. The APF: Using the aerospace performance factor to measure safety performance, pp. 319–372. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-77958496643&partnerID=40&md5=5405cab56d6cfd2caf2db2bde762a891>.

Niu, D.X., Song, Z.Y., 2013. Research on nuclear power plant operational safety performance based on confidence level and fussy evaluation model. Appl. Mech. Mater. (AMM) 475–476, 1721–1724. http://dx.doi.org/10.4028/www.scientific.net/amm.475-476.1721.

Reason, J., 2000. Safety paradoxes and safety culture. Inj. Control Saf. Promot. 7 (1), 3–14. http://dx.doi.org/10.1076/1566-0974(200003)7:1;1-v;ft003.

Safety Regulation Commission, 2016. Src document 55: Annual safety report 2015 (January 2016). <https://www.eurocontrol.int/sites/default/files/article/content/documents/single-sky/src/src-docs/src-doc-55-e1.0.pdf>.

Seshadri, V., 1998. The Inverse Gaussian Distribution: Statistical Theory and Applications (Lecture Notes in Statistics). Springer ISBN: 978-0-387-98618-0.

Socha, V., Socha, L., Szabo, S., Nemec, V., accidents, Air, 2014. their investigation and prevention. eXclusive e-J. 1–9. <http://www.exclusiveejournal.sk/files/4-2014/1-socha-socha-szabo-nemec.pdf>.

Wang, C., Drees, L., Holzapfel, F., 2014. Incident prediction using subset simulation. In: Proc. of ICAS 2014 29th Congress of the International Council of the Aeronautical Sciences, International Council of the Aeronautical Sciences, pp. 1–8, ISBN: 3-932182-80-4.

Wen, Z.H., Zhou, J., Jia, M.X., 2011. Study on relation of structural reliability calculation and fuzzy mathematics. Adv. Mater. Res. 243–249, 5739–5744. http://dx.doi.org/10.4028/www.scientific.net/amr.243-249.5739.

Yanushevsky, R., 2007. Modern Missile Guidance. CRC Press ISBN: 9781420062267.

Yu, H., Khan, F., Veitch, B., 2017. A flexible hierarchical bayesian modeling technique for risk analysis of major accidents. Risk Anal. 37 (9), 1668–1682. http://dx.doi.org/10.1111/risa.12736.

Appendix C

LALIŠ, Andrej, Vladimír SOCHA, Jakub KRAUS, Ivan NAGY and Antonio LICU. Conditional and unconditional safety performance forecasts for aviation predictive risk management. In: *2018 IEEE Aerospace Conference*. IEEE, 2018, pp. 1-8. DOI: 10.1109/ AERO.2018.8396648. ISBN 978-1-5386-2014-4.

Conditional and Unconditional Safety Performance Forecasts for Aviation Predictive Risk Management

Andrej Lališ, Vladimír Socha, Jakub Kraus
Department of Air Tansport
Czech Technical University in Prague
Horská 3, 128 03 Prague 2, Czech Republic
+420-224-359-185
(lalisand, sochavla, kraus)@fd.cvut.cz

Ivan Nagy
Department of Applied Mathematics
Czech Technical University in Prague
Na Florenci 25, 110 00 Prague 1, Czech Republic
+420-224-358-448
nagyivan@fd.cvut.cz

Antonio Licu
Network Operations Management Division
The European Organisation for the Safety of Air Navigation
96 Rue de la Fusée, B - 1130 Brussels
+32-2-729-3480
antonio.licu@eurocontrol.int

Abstract*—This paper deals with safety performance predictions in the aviation, which address the long-term global efforts to achieve predictive risk management by the year 2028. Predictive risk management regards timely and accurate detection of risk, well before some incident or accident takes place so that effective control actions can be provided. To assure achieving such diagnosis, it is necessary that mathematically well-founded predictions will become part of existing safety management systems with the capability to predict key performance indicators. From current safety metrics and with respect to the data available in the aviation, overall safety performance was selected as suitable candidate for predictions. To obtain the performance signal, Aerospace Performance Factor methodology was utilized. Due to confidentiality restrictions with regard to aviation safety data, this study relies on public data sets from the domain of European Air Traffic Management. Dedicated resampling method was used to fill in the gaps of real data sets by transforming expert knowledge into mathematical functions. This enabled the possibility to build and test mathematical models for predicting safety performance. Because the identified data sources included some data, which are not necessary for computing safety performance but relevant in its context, conditional forecasts were made possible. With respect to this, the goal of this paper was to research and evaluate possibilities for both conditional and unconditional forecasts in the context of future risk management. Time-series analysis of the computed safety performance was conducted using ordinary least squares and maximum likelihood estimation. Each of the methodology led to different mathematical model and different predictions. Specific aspects of each methodology were identified. Among others, the conclusions confirm possibility of predicting safety performance for establishing predictive risk management, highlighting great potential of conditional forecast and favouring systemic models of safety.

TABLE OF CONTENTS

978-1-5386-2014-4/18/$31.00

1. INTRODUCTION

Modern trends in the aviation show that the industry strives to adopt new technologies, despite of some constraints to the process. In the domain of aviation safety, there are more these because of general sensitivity of safety issues, which may compromise market position of respective aviation organization, if unveiled. This is understandable to certain extent and even though it provides no excuse for unwillingness to innovate or improve in safety, the resulting drivers for shifting the maturity of safety solutions are enforced by top-down approach, i.e. by aviation regulators and authorities. It may appear odd when regarded to some of the high-risk industries, where the aviation certainly belongs to, but the industry stakeholders deal with other concerns in the first place. This is attributable to the industry complexity [1], market competition and lack of clear relationship between safety and operational costs, which is often estimated as negative by aviation management, i.e. as to increasing the costs with no or little benefit in return.

The vision for safety is provided by International Civil Aviation Organization (ICAO) [2] and to date, it emphasizes effective safety oversight, implementation of vision and action plans to manage hazards and risks, formulated in state safety programs, and finally the ultimate goal of predictive risk management. The predictive risk management, as defined by ICAO, assumes implementation of predictions into the present safety management systems in the aviation, including continuous exchange of safety-critical information in real time, to facilitate decision-making process and to prioritize tasks of greater concern with regard to achieved safety performance [3]. Whilst this is certainly challenging and feasible goal in the context of modern technology, there are many issues that need to be addressed before any predictions may accurately serve safety management.

The first major problem is, that ICAO intends to motivate predictions of risk, but risk is hard to measure. It is a generally accepted solution that risk matrices [4] are used to this end, but their variations and inconsistent approach to determining acceptable level of risk in particular operations suggest that this measure of safety is to substantial extent biased and subjective [5]. When discussing the issue of their predictions, the afore-mentioned rises questions about usefulness of predictions in the context of such severely biased variable to be predicted. It appears much more reasonable to shift the focus to better quantifiable variables, allowing

for more reasonable predictions. For this purpose, one of suitable candidates are safety performance indicators [6] and the methodology dealing with their aggregations - Aerospace Performance Factor (APF) [7].

The second major problem regards general unavailability of aviation safety data, which would meet the requirements of predictive mathematical methods. If the predictions are to be sound, they must be based on proper modeling and make the maximum use of available scientific methods. This requires precise data on safety occurrences and various safety issues, recorded throughout longer time periods. Even though no personal information is needed and anonymized context of the data is sufficient, aviation organization are reluctant to provide their data for research and development purposes. The issue is amplified by the fact that effective safety management requires data sharing among multiple organization in order to establish clear picture of the domain [6], and so the predictions are likely to be distorted if only a single aviation organization participates. However, the situation improved recently when some aviation safety data sets were made public for recent years by some aviation authorities. The most advantageous are data sets published in the European Union (EU) concerning Air Traffic Management (ATM)[2][3][4], because they comprise data from all EUROCONTROL[5] member states for several years and with good level of detail. It was likely the fact that the aviation organizations providing ATM services are mostly monopolies and state enterprises, which contributed to the decision to share some of their data publicly. Other available databases regard the Aviation Safety Reporting System (ASRS)[6] in the U.S. or ATSB[7] National Aviation Occurrence Database[8] in Australia, but they are not comparably processed as in the case of EU ATM data.

With regard to the mentioned issue of predictive risk management, this paper takes the opportunity of the newly emerged data sets in the EU and the APF methodology to evaluate the possibility of using standard mathematical modeling and predictions in the context of civil aviation. The core of the performed research is the idea of predicting safety performance, i.e. safety achievement as defined by safety performance indicators [6]. Even though the idea is not new as there already were attempts to provide safety performance predictions in the ATM [8], these were specific for Italian environment and based on predicting of safety occurrences, which is an arguable concept. This study shifts the focus to predict state of the system (the safety performance) rather than occurrence of specific event types and elaborates the idea using pool of data from 28 countries.

The goal was to check the possibility of providing the predictions in the context of future predictive risk management in the aviation and so to contribute both the the domain of aviation safety as well as to encourage aviation organization to trial the predictions for their needs.

[2]http://ansperformance.eu/
[3]http://www.eurocontrol.int/prudata/dashboard/eur_view_2014.html
[4]http://www.eurocontrol.int/prudata/dashboard/rp2_2015.html
[5]The European Organisation for the Safety of Air Navigation
[6]https://asrs.arc.nasa.gov/
[7]Australian Transport Safety Bureau
[8]https://www.atsb.gov.au/avdata/

2. METHODOLOGY

This section details the steps taken to collect and process aviation safety data, including brief description of applied mathematics to model relationships among variables present in the collected data in order to enable safety performance predictions in the aviation.

ATM Safety Data

The most valuable sources of aviation safety data, with respect to the goal of this paper, are the safety data from ATM published at the EU level, as already described in the previous section. They were used as the primary source for this paper. Apart from these, additional data can be collected from annual reports published by civil aviation authorities (such as [9] and [10]). Some EU-level publications by EUROCONTROL were used to fill the gaps of the data published at the mentioned performance monitoring websites.

Additionally, Air Accident and Incident Investigation Branches (AAIB) and some amateur web pages collect and publish results of the investigated air accidents and incidents, however, these represent only small fraction of safety occurrences in the aviation. It is generally known that safety cannot be effectively measured nor controlled with data solely from accidents and, also, due to practical reasons, these were not included in this research.

Apart the EU-region, aviation safety data of sufficient quality can be collected from other world regions, namely from the U.S. and Australia, as indicated in the previous section. However, these data are gathered in different way than the European data (due to different legislative framework behind the data collection process) and they comprise less details, e.g. there is no distribution per occurrence severity, information about effectiveness of safety management, historical trends throughout several years and others, available in regions other than Europe. It was eventually the different content and high granularity of European data that set the limitations of this work to the EU region.

The final set of EU-level aviation safety data identified as suitable for modeling aviation safety performance comprised the following:

- Data on en-route induced delays (average delay per flight)
- Data on airport induced delays (average delay per flight)
- Data on complexity scores (per country, computed according to published methodology [11])
- Data on Effectiveness of Safety Management (EoSM), both at national and Air Navigation Service Provider (ANSP) level (relative score according to published methodology [12])
- Data on Just Culture (JC) application, both at national and ANSP level (relative score according to published methodology [12])
- Data on selected safety occurrences (number of observations), namely Separation Minima Infringements (SMI), Unauthorized Penetrations of Airspace (UPA), Runway Incursions (RI) and ATM Specific Occurrences, distributed by severity
- Data on traffic volume (per country in total movements)

All data were collected throughout the years 2008 to 2016. However, only traffic volume and data on selected occurrences were available throughout the entire time period. Other data sets start from later years: en-route delays start from 2011, airport delays, EoSM and JC start from 2012 and complexity scores are available first from year 2014.

In addition, the data set progressively captured more EUROCONTROL member states as they joined the reporting scheme. To keep the modeling consistent, only those states, which reported through the entire time period, were accounted for in the analysis (28 in total). Luxembourg had to be excluded because for some years and in some data sets, the member state data are missing, resulting in the final count of 27 members from which data were processed. All these fact imposed limitations which had to be respected when selecting proper modeling technique.

Data Resampling

Despite the quality and extent of European ATM safety data, there is one major limitation to address separately, namely uneven distribution of data in time. Whilst majority of data sets are distributed monthly, data on selected safety occurrences are available only as total number of observations per year. This may be resolved by either reducing granularity of more detailed data or by increasing granularity of less detailed data. Because mathematical modeling does not allow modeling of time-series with very few data points (in the former case there would be less than 10), the latter solution was to be selected.

To resample the data (increase granularity), expert knowledge on the safety occurrences was formalized by means of mathematical functions and used to resample the occurrence data sets. Expert was selected from academic staff at the Czech Technical University in Prague, with ATM background (both education and practice). For this particular research, sinus function, amplified and shifted in time to fit expert assumptions, was used to model data seasonality to decompose one data point into twelve new points (from distribution by year to distribution by month), using the same equation and principles as in the previous study (for details see [13]):

$$N = \int_0^M k \cdot sin\left(x \cdot \frac{2\pi}{M} - \frac{\pi}{2} - \frac{2\pi}{M}\right) dx \qquad (1)$$

where N is number of selected safety occurrence observations, M is scale determined by the new occurrence distribution to be produced (in this case twelve, to break N down into twelve new figures), k is coefficient of seasonal difference and x is time. Coefficient k was set upon empirical testing or expert assumptions on specific safety occurrence to amplify the sinus function, proportionately to order of magnitude of given safety occurrence. For the purpose of both this and the previous study, desirable results were achieved with k = 0.25*N/M, where k amplifies sinus by 25% of the average monthly occurrence rate N/M. By the means of equation 1, all collected data on safety occurrences were resampled into higher granularity.

As a conseuqence, resampling the data, even though using real data sets and domain expert knowledge, introduced some bias to the further calculations. Synthetic data, whether entirely or just partially, almost never reproduce real world scenarios as they do not account for anything outside the equations behind them. In case of this research, however, only data on safety occurrences were resampled from real datasets thus the introduced bias to the next computations is unlikely to be severe, but it certainly must be emphasized with regard to the results of this study.

Computing the Safety Performance

With all the data filtered (some EUROCONTROL member states were removed as described before) and resampled to achieve common granularity and data consistency, it was possible to compute the overall safety performance. In the aviation, there is currently only one methodology to compute the performance from safety performance indicators - the APF [7]. The methodology requires establishing set of safety performance indicators, their evaluation by subject matter experts using pairwise comparison and/or Analytical Hierarchy Process (AHP) [14] and subsequent indicators measurement. Additionally, normalization variable is needed.

For the purpose of this study, the set of indicators was achieved by reducing the EUROCONTROL set established in the published methodology [7], where the key indicators (of each cluster, as in the methodology) were the same, namely the SMI, UPA, RI and ATM specific occurrences. This made it possible to reuse the EUROCONTROL evaluation of the indicators (their weights). On the other hand, some of the lower level indicators (comprising the clusters of EUROCONTROL APF) were not included in this research, because no data were made public on these indicators. Even though this certainly introduced some additional bias (together with occurrence resampling) to the computed time-series, decision was made to rather omit data on missing indicators than simulate entirely synthetic data for the purpose, because the latter could introduce more significant noise to the response signal than just omitting the data. The decision was also supported by the fact, that none of the missing indicators were key (of significant severity, compared to the indicators with data made available) in terms of any cluster of the EUROCONTROL APF. Traffic volume data were use as the normalization variable. The computed safety performance time-series is depicted in Figure 1.

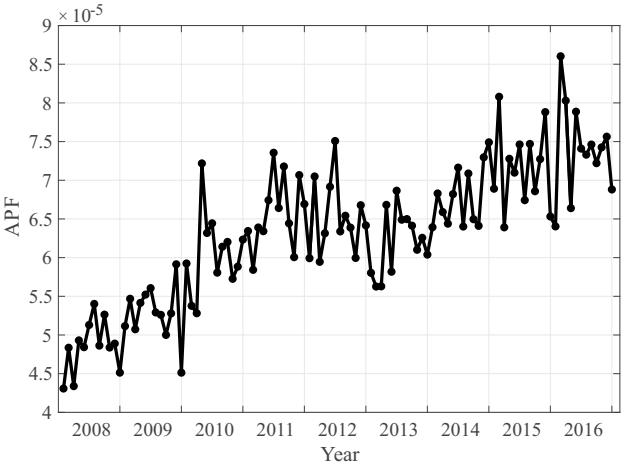


Figure 1. **Computed safety performance.**

Stochastic Models

With respect to the collected data, their characteristics and the methodology used to compute safety performance time-series, it became clear that any elaboration of the series predictions must be based on models capable of dealing with signal noise and seasonality (due to bias and seasonality present both in safety occurrence data and normalization

variable). Whilst there are multiple forecasting tools provided by the mathematics, this study preferred methods proved from econometrics, namely linear regression modeling based on Ordinary Least Squares (OLS) [15] and Autoregressive Moving Average (ARMA) based on Maximum Likelihood Estimation (MLE) [16].

These methods proved their capabilities to model behavior of noise affected time-series, such as GDP [17] or inflation rate [18], and to forecast the signal response. Safety performance is similar in its nature, even though it is not directly measurable (it is only computed as a system state from other measured variables). The attempt to use the same methods as for GDP or inflation rate forecasts to predict safety performance leads to an interesting parallel and it may be of benefit to other applications in the domain of safety.

The selected methodologies were used to establishing two distinct models: linear regression model allowing conditional forecasts (exogenous predictors are used to predict the response) and ARMA model of unconditional forecasts (the series is autoregressive, i.e. using historical values of response and noise innovations only). With regard to the concept of each of those methodologies, linear regression was preferred to avoid using moving average (MA) component, whilst this was considered in the ARMA model. The reason to put emphasis whether the MA component is present or not stems from the very principle of how the component is calculated:

$$\epsilon_t = y_t - \overline{y}_t \tag{2}$$

where ϵ_t is the estimated noise at time t and $\overline{y}_t$ is the response forecast from time t-1 of the actual response y_t. This principle is probably the only way how to estimate noise, but it is arguable whether such estimation is accurate and if it doesn't add some additional bias to the model. ARMA models can also be produced with exogenous variables to provide conditional forecasts as well, but due to limited size of data sets used in this study, the number of both response and predictor observations was insufficient to produce stable ARMA model of these properties.

Data Processing and Checks

As a first step, holdout sample of 6 data points (second half of the year 2016) was excluded from all other model-building related processes. The size was selected to account for seasonality present in the data. Half of the season was selected to capture the seasonality and, at the same time, to not limit the model-building process by significantly reducing already limited samples.

Before the model-building process started, data sets were checked for strong interactions (correlation), both within and among all sets. To check the correlation, Pearson's and Spearman's correlation coefficient [19] (depending on data distribution determined by the means of Jarque-Bera test [20]) were used. All the testing of strong interactions was performed with level of significance α=0.05.

Throughout the process of testing individual sets, it was discovered that complexity scores data set is highly correlated between its member states, with an average R=0.71. This is reasonable output of the testing because the number of conflicting situations to be resolved by air traffic control depends on volume of traffic, which is distributed proportionally among the neighboring member states and not limited to some specific airspace. As a result, complexity scores were used as averaged figures from all 27 member states. Other data sets did not exhibit strong correlations among members states and so they passed the testing unchanged.

Results from correlation testing among different data sets indicated strong correlations among JC data and EoSM data (R oscillating around 0.7). Because correlation between JC data sets was stronger than between EoSM data sets, it was concluded that EoSM data sets include much of the information from JC data sets. This is also reasonable output, because both EoSM and JC data sets are based on EU legislative framework, motivating members states and ANSPs to constantly improve and achieve targets set for year 2019 [21]. This motivation is present in the data and, as a result, JC data sets were dropped from the model building process. EoSM data remained unchanged. Apart from that, moderate correlation was identified among both delay data and complexity scores data (R oscillating around 0.55). This is also realistic indication because delays are induced typically when airspace gets congested with higher volumes of traffic. However, because it was not possible to conclude the correlation as strong, none of the data were dropped at this stage.

Further, stepwise regression (testing up and testing down) was used to confirm relevance of the remaining predictors with regard to the response (safety performance). The testing was done with level of significance α=0.15 to account for some predictors, which could be dropped due to smaller sample size (especially complexity scores). To cross-check the results of stepwise regression, test models with different predictors were additionally evaluated by the means of model selection criteria, namely Akaike's Information Criterion (AIC), Schwarz' Bayesian Criterion (SBC) [15], Sum of Squared Errors (SSE)[22], [23], Error Mean Square (MSE), R^2 and adjusted R^2 [15]. The testing, confirmed by the evaluation from calculated model selection criteria, dropped both delays and ANSP-level EoSM data sets as not relevant enough with regard to the response.

As the last step, all data were checked for possible non-linear nature of their relationship with the response. To this end, various interactions, quadratic, pure quadratic and higher-order polynomial (up to order of five) models were evaluated to check possible non-linear relations between respective predictor and the response. To evaluate different models, the same model selection criteria were used as before. The testing confirmed previous results and dropped both delays and ANSP-level EoSM data as not significant with regard to the response (according to their t-statistic and overall model F-statistic, with level of significance α=0.05). However, the testing revealed that both the state-level EoSM and complexity scores better match the response in quadratic form (EoSM^2 and CS^2) and product of their interaction (EoSM·CS) is also significant.

Model Building Process

Building the linear regression followed published methodology in [15]. The model-building process violated classical linear regression assumptions [24] due to the necessity of adding dynamic terms (lagged response, both seasonal and non-seasonal). As a result, the model became no longer strictly exogenous. To remedy the negative effects, Jackknife bias reduction [25] was applied (both moving blocks and non-overlapping partitions). However, according to [26], when

the sample size used to build a model is from around 25 to 100 data points, OLS estimators may surpass even the estimators specifically designed to address autocorrelation issues, such as the Jackknife bias reduction. The sample size used to build the linear regression model in this research consisted of 66 data points (years 2011 to mid-2016) thus exactly fitting the mentioned size. The results from Jackknife confirmed that the supposedly biased estimators were better performing than their Jackknife-based counterparts. At the end, model residuals were checked for effects of autocorrelation, heteroskedasticity and normality by means of Ljung-Box Q-test [27], Engle's ARCH test [28] and one sample t-test respectively. First two tests were executed to assure model stableness and one sample t-test to assure that prediction confidence intervals can be carried out by standard techniques [24].

ARMA model was build according to Box-Jenkins methodology [16]. Both seasonal and non-seasonal differencing was applied to achieve stationary time-series. The series stationarity was tested by Kwiatkowski-Phillips-Schmidt-Shin (KPSS) test [29] for a unit root. To detect the need for autocorrelation (AR) or moving average (MA) terms, whether seasonal or non seasonal, the autocorrelation and partial autocorrelation functions were computed and plotted. Different models of various combinations including AR and MA terms up to degree six, including their seasonal counterparts up to degree three, where computed and evaluated by the same model selection criteria as used for stepwise regression before.

3. Results

This sections demonstrates the results of the performed research. Equation 3 shows the computed linear regression model:

$$\begin{aligned} y_{t+1} = c + \beta_1 y_t + \beta_2 y_{t-1} + \beta_3 y_{t-2} + \beta_4 y_{t-3} + \beta_5 y_{t-4} + \\ + \beta_6 y_{t-5} + \epsilon_t + B_1 y_{t-12} + B_2 y_{t-24} + B_3 y_{t-36} + \\ + \beta_E EoSM^2 + \beta_C CS^2 + \beta_{EC} EoSM \cdot CS + \epsilon_t, \end{aligned} \tag{3}$$

where y is the response series, c is model intercept, β are non-seasonal regression coefficients, B are seasonal regression coefficients, $EoSM$ and CS represent predictor variables, t stands for discrete time step and ϵ_t is noise innovation. Estimated coefficients of the model are listed in Table 1, including their stableness assessment. Relative change shows how much the estimates vary by comparing those from entire data sets and those produced without data from holdout sample.

In Figure 2, there are depicted one step predictions using the linear regression model, where the response series (safety performance) is limited to the last three years. The computed confidence intervals correspond to level of significance α=0.05.

Equation 4 shows the resulting form of ARMA model:

$$y_{t+1} = c + \beta_1 y_t + \beta_2 y_{t-1} + \epsilon_t + \gamma \epsilon_{t-1}, \tag{4}$$

where y is the response series, c is model intercept, β are non-seasonal regression coefficients, ϵ_t represents noise innovation and γ is the moving average coefficient. Estimated coefficients of the model are listed in Table 2 with their stableness assessment.

Table 1. Estimated coefficients for linear regression model

coeffic. estimate	without holdout []	with holdout []	relative change [%]
C	2.34E-05	4.30E-05	83.67
B_1	0.128	0.248	94.01
B_2	0.192	0.009	95.09
B_3	-0.056	-0.012	77.64
β_1	-0.197	-0.266	-35.12
β_2	-0.246	-0.246	-0.00003
β_3	0.092	0.101	8.95
β_4	0.192	0.213	10.73
β_5	0.124	0.101	-18.27
β_6	0.497	0.277	-44.20
β_E	2.14E-09	1.49E-09	-30.12
β_C	-2.61E-06	-1.02E-06	60.98
β_{EC}	-7.50E-08	-1.11E-07	-47.59

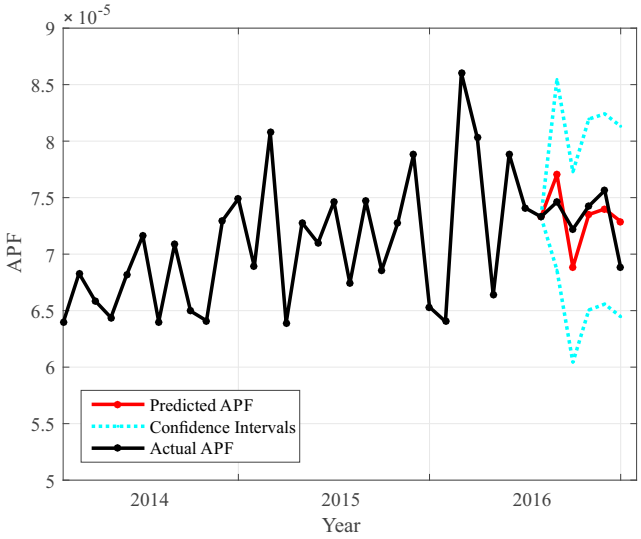


Figure 2. **Predictions with the computed linear regression model.**

Similarly to the linear regression model, Figure 3 depicts one step predictions with the model. Confidence intervals correspond to level of significance α=0.05.

4. Discussion

The results show that both models produced reasonable forecasts and that both correctly anticipated the presence of future data points (none of them departed out of the light blue dashed lines). However, visual examination of both forecasts shows that linear regression model outperformed ARMA model because it estimated more closely the magnitude of signal change as well as the course of change for all points. ARMA model mistakenly forecasted decrease in safety performance for third data point and likewise the increase for the

Table 2. Estimated coefficients for ARMA model

coef. estimate []	without holdout []	with holdout []	relative change [%]
C	3,01E-07	2,10E-07	-30,28
β_1	-0,441	0,027	-6,25
β_2	-0,336	0,017	-5,09
γ	-0,398	0,033	8,52

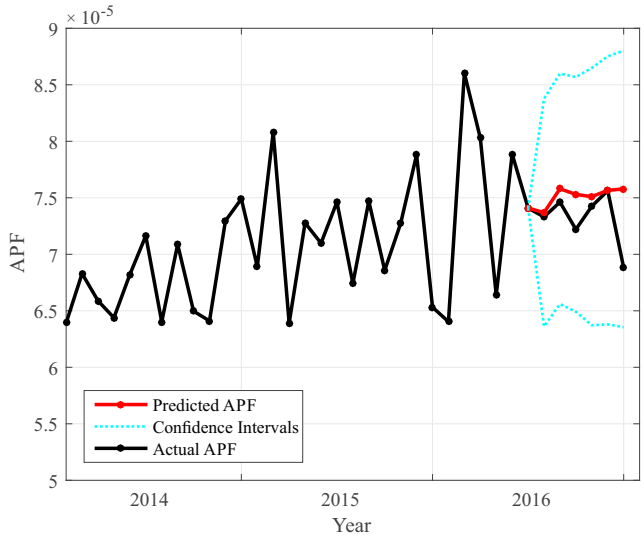


Figure 3. **Predictions with the computed ARMA model.**

last data point. Model variance indicated by the confidence intervals suggests that the linear regression model is more certain about the future output.

To proceed with the validation of both models, their predictive performance was checked using Prediction Sum of Squares (PRESS) criterion [15], where each of the models was compared together and with the so-called constant model - a model consisting only of an intercept equal to the last observed data point (at all times), i.e. model with no predictors. For constant model, the computed PRESS was 6.0184e-11. Linear regression model, as per equation 3, achieved PRESS equal to 3.6979e-11, thus clearly outperforming the constant model. On the other hand, estimated ARMA model achieved PRESS equal to 6.0408e-11, performing slightly worse than the constant model and significantly worse than the linear regression model. According to PRESS criterion, only the linear regression model proved as valid.

With regard to coefficient stability, ARMA model performs better then linear regression model. However, the model is of high variance and does not allow for significant changes, including the response. The model structure is more parsimonious, making it easier to stabilize. It is questionable, whether the stability was achieved because the safety performance is heavily biased and the actual core of the process was captured by ARMA, or the model was simply unable to identify behavioral patters in the response. This is hard to decide and it can only be ascertained with more robust study, by increasing the level of detail. On the contrary, not even the changes in linear regression model are of extreme values and they may be caused by limited data samples, where each new data point still notably affects the entire model. From the standpoint of coefficient stability, no conclusive statements can be made apart from that ARMA model was already stabilized throughout this study.

At this point, it is important to realize, that the results of this study are certainly affected by the limited sample size. Moreover, the effect was supported by introducing additional bias from data resampling and omitting some safety performance indicators. For safety performance, there were 108 data points in total (from 2008 until 2016), but predictor data started from 2011 to 2014, inhibiting the possibility to compute ARMA model with exogenous predictors. In fact, this is the reality of safety data; even though there may be thousands of record of safety performance indicators at regional level, as soon as system-wide information is to be produced, such as safety performance, they all aggregate and reduce in size. Even if there would be all predictor data available for all the years, there would be about 100 data points only, which is still quite limited sample for thorough time-series analysis. This supports the need for alternative safety performance evaluation, if standard time-series modeling techniques are to be used effectively.

The results of this work point also to another interesting point. They indicate that safety performance as such may not be easily predictable without accurate data on predictors, i.e. unconditionally. ARMA model, despite of the longest possible data set collected in this study (108) was unable to provide valid predictions. High model variation confirms that the process mean is likely deranged in time. This conclusion is in line with the newest discoveries in safety, namely systemic models of safety, where system-theory based approach is proposed instead of analytical reduction or standard probabilistic approach [30]. This result supports the notion that systemic approach to predicting safety may be of greater benefit to modern safety management, including the vision of predictive risk management as its integral component.

With regard to the very techniques to predict time-series, whether conditionally or unconditionally, this study cannot conclude whether OLS or MLE are more effective for the purpose of predicting safety performance. It is probably the case that both of the methods can be used but MLE proved to be more data demanding than standard OLS. With respect to this, OLS may be more appropriate for cases such as in this paper.

5. Conclusion

This paper aimed to identify possible ways of supporting the development towards achieving predictive risk management in the aviation, as stipulated by civil aviation authorities, and to give directions for further research. Because measurement of risk is hard and severely biased, this goal appears rather as not feasible if the risk evaluation methodologies are to be maintained. With respect to that, this paper shifted the focus on better measurable variables from the domain of aviation safety, namely the safety performance and its indicators.

Even though safety performance cannot be measured directly today, there is sound method for its indirect computation from set of performance indicators, named Aerospace Performance Factor. This methodology was selected as the best candidate to provide the desired input for research of possible introduction of predictions into the aviation, which would serve the risk management afterwards. As a next step, this study searched and identified available sources of aviation safety

data to compute the safety performance. Additional data sources were identified that served eventually as predictors concerning the safety performance. The most suitable data were identified at the EU level, namely from the domain of Air Traffic Management, and their characteristics, together with the specifics of the computed safety performance, determined the ways of mathematical modeling used to establish safety performance predictions.

Linear regression model using Ordinary Least Squares was used to produce model capable of conditionally (using predictor data) forecasting the safety performance. Autoregressive Moving Average (ARMA) model based on Maximum Likelihood Estimation was used to produce model of unconditional forecasts. At the end, the linear regression model was pronounced valid, whilst ARMA was not. This result is attributable to limited data samples which did not allow computation of effective ARMA model (with regard to the available data), but it also suggests that safety performance likely cannot be predicted unconditionally due to unstable process mean. By contrast, conditional forecasts proved as better performing due to predictor data, which explained part of the performance behavior. Because aviation safety data are limited in sample size, linear regression model and Ordinary Least Squares are considered as more suitable for safety performance predictions.

These results give directions for further process in achieving predictive risk management. They favor systemic approach and accurate measurement of key variables of the controlled safety system. Linear regression may provide help in modeling safety behavior, including its predictions, given real time data.

Limitations of this work lie with the fact, that even though various contextual data and data on specific safety occurrences were collected from 27 EUROCONTROL member states and used to research possible safety performance predictions, these data comprise just the tip of the safety data iceberg and there is much more to discover if robust data on less severe safety occurrences are used for such analysis. Another limitation was the fact, that some safety occurrence data were missing entirely, and some distributed by year only, whilst all other available data were distributed by month. Consequently, safety occurrence data were to be resampled, adding some new bias to the analysis.

Future work certainly needs to focus on better data sharing, so that more data are available to similar research as from this paper. It is important to work with the full picture and not just with fractions of safety data. As already indicated, precise predictions require precise measurement thus more accurate methods for risk evaluation and measurement. Combination of both quality data sharing and deployment of advanced methods for measuring safety variables is the key to achieve predictive risk management of the future.

ACKNOWLEDGMENTS

This work was supported by the Czech Technical University in Prague, junior research grant No. SGS16/188/OHK2/2T/16.

REFERENCES

[1] S. Eriksson and H. Steenhuis, *The global commercial aviation industry.* London and New York: Routledge, 2016.

[2] International Civil Aviation Organization (ICAO), *Doc. 10004 Global Aviation Safety Plan*, 2nd ed. Montral, Quebec: ICAO, 2016.

[3] C. Janicak, *Safety Metrics: Tools and Techniques for Measuring Safety Performance.* Lanham, MD: Government Institutes, 2010.

[4] L. Cox, *Risk Analysis of Complex and Uncertain Systems.* New York, N.Y.: Springer, 2010.

[5] L. Anthony Tony Cox, "What's Wrong with Risk Matrices?", *Risk Analysis*, Vol. 28, No. 2, pp. 497-512, 2008.

[6] International Civil Aviation Organization (ICAO), *Safety Management Manual (SMM).* Montral, Quebec: ICAO, 2013.

[7] European Organisation for the Safety of Air Navigation (EUROCONTROL), *The Aerospace Performance Factor (APF): Developing the EUROCONTROL ESARR 2 APF.* Brussels: EUROCONTROL, 2009.

[8] G. Di Gravio, M. Mancini, R. Patriarca and F. Costantino, "Overall safety performance of Air Traffic Management system: Forecasting and monitoring", *Safety Science*, Vol. 72, pp. 351-362, 2015.

[9] European Aviation Safety Agency (EASA), *Annual Safety Review 2016.* Cologne, Germany: EASA, 2016.

[10] European Organisation for the Safety of Air Navigation (EUROCONTROL), *Safety Regulation Commission Document 56: Annual Safety Report 2016.* Brussels: EUROCONTROL, 2017.

[11] European Organisation for the Safety of Air Navigation (EUROCONTROL), *Performance Review Commission: Complexity Metrics for ANSP Benchmarking Analysis.* Brussels: EUROCONTROL, 2006.

[12] European Aviation Safety Agency (EASA), *Annex to ED Decision 2011/017/R: Acceptable Means of Compliance and Guidance Material for the implementation and measurement of Safety Key Performance Indicators (SKPIs) (ATM performance IR).* Cologne, Germany: EASA, 2011.

[13] A. Lalis, V. Socha, P. Vittek, and S. Stojic, Predicting safety performance to control risk in military systems. *2017 International Conference on Military Technologies (ICMT),* 2017.

[14] T. Saaty, *Fundamentals of Decision Making and Priority Theory With the Analytic Hierarchy Process.* Pittsburgh, Pa.: RWS Publications, 2006.

[15] M. Kutner, *Applied linear statistical models.* Boston: McGraw-Hill Irwin, 2005.

[16] G. Box, G. Jenkins, G. Reinsel and G. Ljung, *Time Series Analysis: Forecasting and Control.* John Wiley & Sons, Inc, Hoboken, New Jersey, 2015.

[17] R. Golinelli and G. Parigi, "Real-time squared: A real-time data set for real-time GDP forecasting", *International Journal of Forecasting*, Vol. 24, No. 3, pp. 368-385, 2008.

[18] I. Baciu, "Stochastic Models for Forecasting Inflation Rate. Empirical Evidence from Romania", *Procedia Economics and Finance*, Vol. 20, pp. 44-52, 2015.

[19] P. Chen and P. Popovich, *Correlation: Parametric and Nonparametric Measures.* Thousand Oaks, Calif: SAGE Publications, 2006.

[20] C. Jarque and A. Bera, "Efficient tests for normality,

homoscedasticity and serial independence of regression residuals", *Economics Letters*, Vol. 6, No. 3, pp. 255-259, 1980.

[21] European Parliament. Commission Implementing Decision 2014/132/EU setting the Union-wide performance targets for the air traffic management network and alert thresholds for the second reference period 2015-19. *Offcial Journal of the European Union*, L71(20), 2014.

[22] N. Draper and H. Smith, *Applied Regression Analysis.* New York, NY: John Wiley & Sons, 2014.

[23] M. Gacula, *Design and Analysis of Sensory Optimization.* Trumbull, Conn., USA: Food & Nutrition Press, 2005.

[24] P. Kennedy, *A Guide to Econometrics.* Malden, MA.: Blackwell, 2013.

[25] M. Chambers, "Jackknife estimation of stationary autoregressive models", *Journal of Econometrics*, Vol. 172, No. 1, pp. 142-157, 2013.

[26] A. Maeshiro, "Teaching Regressions with a Lagged Dependent Variable and Autocorrelated Disturbances", *The Journal of Economic Education*, Vol. 27, No. 1, pp 72, 1996.

[27] G. Ljung and G. Box, "On a measure of lack of fit in time series models", *Biometrika*, Vol. 65, No. 2, pp. 297-303, 1978.

[28] R. Engle, "Autoregressive conditional heteroscedasticity with estimates of the variance of united kingdom in ation", *Econometrica: Journal of the Econometric Society,*, Vol. 50, No. 4, pp. 987-1008, 1982.

[29] D. Kwiatkowski, P. Phillips, P. Schmidt and Y. Shin, "Testing the null hypothesis of stationarity against the alternative of a unit root: How sure are we that economic time series have a unit root?", *Journal of econometrics,*, Vol. 54, No. 1-3, pp. 159-178, 1992.

[30] N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety.* Cambridge, Mass: The MIT Press, 2012.

BIOGRAPHY

Andrej Lališ *received his M.S. and Ph.D. degree in Air Traffic Management and Control. He currently works as lecturer, researcher and head of Laboratory of Aviation Safety and Security. His research interests include safety engineering, signal processing, air traffic control and management and human factors in the aviation.*

Vladimír Socha *recived his M.S. degree in the field of biomedical and clinical technology at the Czech Technical University in Prague, and Ph.D. degree in transportation at Technical University of Košice. He is lecturer, researcher and head of the Laboratory of Human Factors and Automation in Aviation at the Department of Air Transport. His research interests include signal processing and human factors in the aviation.*

Jakub Kraus *received his M.S. and Ph.D. degree in Air Traffic Management and Control. He is currently head of the Department of Air Transport at the Czech Technical University in Prague. His research interests include air transport operation, aviation safety, air traffic management and communication, navigation and surveillance.*

Ivan Nagy *received his M.S. degree in the field of technical cybernetics at Czech Technical University in Prague and Ph.D. degree in hybrid adaptive control at Czech Academy of Science. Currently, he works as associate profesor in mathematics at the Faculty of Transportation Sciences, Czech Technical University in Prague. His research interests include bayesian modeling, estimation, prediction and control of random dynamic systems and their application in transport.*

Antonio Licu *received his M.S. degree in avionics at University Politehnica of Bucharest. He works in EUROCONTROL, as Head of Safety Unit at the Network Manager Directorate, Bruxelles. He leads the deployment of safety management and human factors programmes of EUROCONTROL and he has extensive Air Traffic Control operational and engineering background. His research interests include ATM, safety and performance.*

Appendix D

LALIŠ, Andrej, Vladimír SOCHA, Peter VITTEK and Slobodan STOJIĆ. Predicting safety performance to control risk in military systems. In: *2017 International Conference on Military Technologies (ICMT)*. IEEE, 2017, pp. 392-396. DOI: 10.1109/MILTECHS.2017.7988791. ISBN 978-1-5090-5666-8.

2017 International Conference on Military Technologies (ICMT)
May 31 – June 2, 2017, Brno, Czech Republic

Predicting Safety Performance to Control Risk in Military Systems

Andrej Liališ*, Vladimír Socha†, Peter Vittek‡ and Slobodan Stojić§
*Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Prague, Czech Republic, e-mail: *lalisand@fd.cvut.cz*
†Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Prague, Czech Republic, e-mail: *sochavla@fd.cvut.cz*
‡Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Prague, Czech Republic, e-mail: *vittek@fd.cvut.cz*
§Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Prague, Czech Republic, e-mail: *stojislo@fd.cvut.cz*

***Abstract*— This paper deals with research of safety performance predictions to allow improved risk control in military. Safety performance is identified as appropriate tool to establish system-wide information on safety which can serve the decision making process on how to manage safety. The information contributes to better understanding of behavioural patterns in the controlled system and the ability to foresee short-term future can provide key elements for justification of remedial measures. Aviation safety data served the research due to confidentiality restrictions in military. Data deficiencies were addressed by the means of developed simulator. Suitable mathematical models were identified and autoregressive model was selected and applied to predict computed safety performance. At the end, it was possible to validate the model. Remarks on its potential application into real military environment conclude this work.**

***Keywords*– aerospace safety; autoregressive processes; regression analysis; risk analysis; stochastic system; system performance**

I. Introduction

Modern safety management in high-risk industries demands advanced information technologies to achieve its goals. Whilst understanding key principles of safety behaviour reached certain maturity over recent years, their application to real environment still implies many challenges. Individual pieces of technology can usually be considered safe today, but as soon as they aggregate into one operating system located in some environment, many opportunities for unacceptable risk emerge. Challenge is the ”soft” nature of how safety works because application of hardware sensors for tracking safety is very limited. System component interactions, interfaces between different systems, human factor or human-machine interface point to the inherent complexity of robust operations, which is typical for modern systems such as used for military purposes or in civil aviation [1]. These are hard to control in safety [2].

Friendly fire accident in Iraq from April 1994, where two U.S. Air Force F-15's shot down two U.S. Army helicopters, killing all people aboard, is a good example, which contributed to the discussion of necessity to develop new tools and solutions for managing risks. According to the known facts and system-theory based investigation [3], process complexity and numerous deviations, from how the operations were originally designed to work, were the key players in this accident.

One of the recently introduced tools for managing risks is safety performance [4]. It uses safety performance indicators to evaluate the overall performance in order to identify weak points in the context of system-wide information. Whilst some issues may appear negligible when assessed separately, the opposite may be the case as soon as they are combined with other, normally also insignificant issues. Good practice is not to allow the system deviate too far from how it was designed or redesign it appropriately. To identify the deviations timely and adequately, selective datasets, which are practical to measure, shall be gathered and evaluated either in real time or within some acceptable time interval. These may comprise hardware-based data recorded during operations as well as soft data originating from safety reports, audits, investigations etc.

At present, the only successful methodology for safety performance computation is Aerospace Performance Factor (APF) [5], developed by U.S. Naval Safety Centre, easyJet airlines and Imperial College of London. The methodology computes the performance as a non-dimensional aggregated figure based on number of safety occurrences (deviations from designed system behaviour), assessed for severity by domain experts, and normalization data, such as traffic or volume of operations. The methodology allows quantitative evaluation of safety performance, producing a time series thus enabling safety management to get an insight of how the deviations add up to the overall system behaviour.

This article works with unique idea to predict computed safety performance. There are no accepted safety performance predictions available to date and in civil aviation and military environment, mathematical modelling is normally used for hardware sensors data only. By contrast, predictions using ”soft” sensors data became successful in econometric applications (such as [6] or [7]), which were

good starting point for this research. Safety performance itself can be very powerful tool, but the ability to predict it implies to understand and quantify basic dependencies, such as seasonality, dynamic relations or the influence of specific actions. This can affect safety management decisions, as it provides sound basis for justification of their measures, finally leading to better targeted safety oversight, saving costs or human lives.

II. Methodology

Due to confidentiality restrictions of military safety data, the data for research of safety performance predictions were taken from the domain of civil aviation. As already mentioned, modern safety solutions are similar due to commonalities among safety issues in high-risk industries such as military or civil aviation [3]. Apart from that, military and civil aviation overlap in the technology used because civil aviation frequently adopts technology developed originally for military purposes. Further, the idea of similarity is supported by [8] or [9].

In civil aviation, data of the highest quality are regularly published by EUROCONRTOL in the EU and associated countries, either in various annual safety reports or in dedicated websites. Advantage of this approach is that safety occurrences evaluation by domain experts (safety KPIs weights), which is needed for APF computation, was also published by EUROCONTROL when trialling the computation of APF in civil aviation [10].

Data on safety occurrences in aviation are likely similar to those, which could be gathered from military. In fact, various systems and industries, where safety is managed, seem to exhibit common patterns in terms of how safety occurrences emerge. Specific probability distributions can be derived from safety data [11], [12], commonly indicating skewed distributions to fit them regardless where they originate from. This is in line with the fact that safety solutions are similar in their foundations regardless of industry where they apply.

The goal was to compute APF for a period of few years to allow thorough quantitative analysis of the series. As soon as the signal was computed, selection of appropriate mathematical modelling followed. Model validation process concludes the work, which depends on selected mathematical modelling. Following subchapters provide more details on each step.

A. Computing APF

As a first step, all applicable data sources were identified. These include namely:

- Safety Regulation Commission (EUROCONTROL) Annual Safety Reports.
- Performance Review Commission (EUROCONTROL) Performance Review Reports.
- Performance Review Unit (EUROCONTROL) ANS performance monitoring website [13].
- Performance Review Unit (EUROCONTROL) RP1 [14] and RP2 [15] dashboards.
- EUROCONTROL Annual Network Operations Reports.

The data were collected for period 2008 to 2015. For normalization, traffic distribution data were used as was the case of APF computation by EUROCONTROL. However, first problems emerged already at this stage; whilst safety occurrence data are available as annual figures, traffic distribution is available monthly for all the period. This limited APF computation to eight points only, because it was not possible to identify data on safety occurrences with higher granularity. Another issue is that, over the period, the list of reporting member states to EUROCONTROL progressively extended from 29 to 40 and it was not possible to determine the contribution of each newly joined state. The problem lies with the fact, that safety occurrences are collected jointly from all states, whilst traffic distribution figures were available only for the former 29 member states, except for year 2015 where traffic distribution is available for the newly joined states as well.

To address the issue of different data granularity, dedicated simulator was developed. It is based on real data and aviation domain expert assumptions modelled by mathematical functions. The simulator was used to resample existing safety occurrence data into higher granularity, namely distribution by month. It is based on the following expert assumptions:

- Occurrence rate is higher in summer than in winter.
- Occurrence values correspond to the traffic distribution, i.e. maximum value is most likely in July and minimum in January.
- The higher the total amount of reports per year, the bigger the difference between peak and trough values.
- Values are to be natural numbers or zero.

Data resampling was then based on the following equation:

$$N = \int_0^M k \cdot sin\left(x \cdot \frac{2\pi}{M} - \frac{\pi}{2} - \frac{2\pi}{M}\right) dx \qquad (1)$$

where N is number of selected occurrence observations of original distribution, M is scale determined by the new distribution to be produced (in this case 12, as one annual figure N is to be broken down into 12 new figures), k is coefficient of seasonal difference and x is time. Coefficient k is to be set upon empirical testing or expert assumptions on specific safety occurrence, if provided, so that it reasonably amplifies the sinus function, proportionately to order of magnitude of respective safety occurrence. For the purpose of this research, reasonable results were achieved with $k = 0.25*N/M$, where k amplifies sinus by 25% of the average monthly occurrence rate N/M. Sinus function itself is used to model seasonality. Expression in the sinus function shifts its maximum and minimum as per expert assumptions above. By the means of simulator based on (1), all publicly available safety occurrence data were resampled into dataset with higher granularity.

With regard to the inconsistent number of reporting states, it was possible to determine, which 11 countries/units joined the reporting: Albania, Armenia, Croa-

tia, Georgia, Maastricht, Macedonia, Moldavia, Montenegro, Serbia, Turkey and Ukraine. According to the traffic distribution data available for year 2015, it is clear that only Maastricht, Turkey and Ukraine might be able to influence the APF because their traffic distribution in total exhibits some significance compared to the total EU-wide figures. On the other hand, the crucial majority of 29 EU member states includes the biggest players for all the data. Taking this into account, the error caused by omission of the difference in occurrence observations, caused by newly joined 11 members, may slightly change the trend of the computed APF towards the year 2015, but it is unlikely to affect the core of APF, which is based weighted safety occurrences.

With the resampled data on safety occurrences, it was possible to compute the APF for years 2008 up to 2015 (Fig. 1). It is a dimensionless variable.

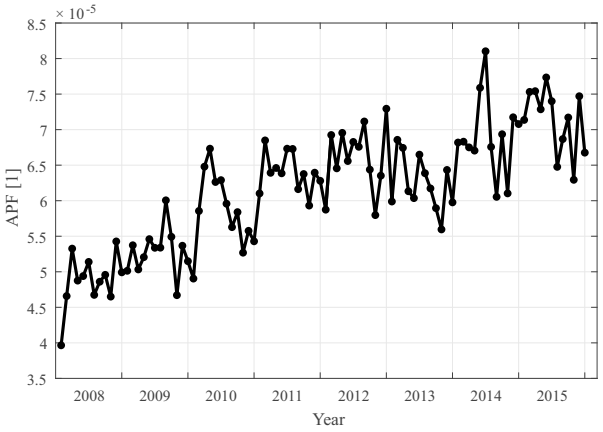


Figure 1. Computed APF signal for period 2008 - 2015.

B. Selection of suitable mathematical model

In general, there are several ways of analysing signals to allow predictions of univariate time-series [16]. It is possible to use linear trend and mean (constant) model, random walk models, averaging and smoothing models, linear regression model and ARMA models with their variations. The decision which to choose depends on qualitative properties of the time-series, such as trend patterns, correlations among variables, seasonality etc. In theory, the elementary decision process to follow was already defined some time ago [17].

Main characteristic of the computed APF signal is a clear presence of seasonal element because traffic distribution, normalizing the signal, exhibits regular peaks and troughs. This is also supported by the fact that demand in aviation is variable and dependent on season of a year, causing the denominator of APF to periodically change. Another feature is that the signal is most likely influenced in a dynamic way, i.e. a perturbation resonates it for one or more steps in a sample. This assumption stems from the fact that aviation is a complex socio-technical system and as soon as APF captures some non-random perturbation, the complexity very likely requires some time for the system to absorb it.

According to the signal features and with regard to the goal to be achieved, ARMA model with its variations fits the need to further predict the APF. It is typically based on Maximum Likelihood Estimation [18], capable of producing unconditional predictions and dealing with signal dynamicity.

C. Model application

Before the model-building process commenced, a hold-out sample consisting of last six data points of the computed APF was created. These were put on hold for model validation and excluded from model-building.

To build an ARMA, Box-Jenkins methodology [19] was to be followed. The methodology requires transformation of the time series into stationary series. This was achieved by differencing the series and by testing the differenced data by the means of Kwiatkowski-Phillips-Schmidt-Shin (KPSS) test for a unit root [20] and by verification using sample autocorrelation and partial autocorrelation functions (ACF and PACF). Desired series properties were achieved by first order of differencing, both seasonal and non-seasonal. ACF and PACF, however, indicated overdifferencing but addition of autoregressive and moving average terms sorted out the problem. To make sure, that the most suitable ARMA is selected, multiple models with different orders of autoregressive and moving average terms, both seasonal and non-seasonal, were computed and compared by the means of model selection criteria, namely Akaike's Information Criterion (AIC), Schwarz' Bayesian Criterion (SBC) and Prediction sum of squares criterion (PRESS) [21]. The best candidate was selected as an optimum trade-off between all three model selection criteria, which was achieved by multiplicative ARIMA$(5,1,1)(2,1,0)_{12}$. Model coefficients are shown in Tab. I, and the model in lag operator notation is following:

$$\begin{aligned}&\left(1-\beta_1 L-\beta_2 L^2-\beta_3 L^3-\beta_4 L^4-\beta_5 L^5\right)\\&\left(1-B_1 L^{12}-B_2 L^{24}\right)\left(1-L-L^{12}+L^{13}\right) y_t\\&=c+\epsilon_t+\gamma\epsilon_{t-1},\end{aligned} \tag{2}$$

TABLE I
ESTIMATED COEFFICIENTS FOR MODEL BASED ON (2).

c	β_1	β_2	β_3	β_4
9.1237e-09	-0.59367	-0.52600	-0.33499	-0.01210

β_5	B_1	B_2	γ	
0.00162	0.38970	0.23932	-1	

D. Model validation

As a last step, the model was subjected to validation process. First check of prediction performance was done via calculating PRESS criterion. The criterion was then used to compute performance of constant model with no predictors, where the constant was the last observed response value, before the prediction starts. For single step

forecast, the achieved PRESS is 1.102e-10 and for multi-step forecast, it is 7.300e-11. Both models outperformed constant model with PRESS equal to 1.696e-10 by capturing some of the information from response signal.

The last step in the validation process was to check the stableness of model coefficients. To do so, the same model was reestimated with the entire response dataset, including holdout sample. Reestimated coefficients with relative change are shown in Tab. II. The table indicates stableness for majority of model coefficients, where only β_4 and β_5 appear non-stable, likely affecting the stableness of model intercept c. On the other hand, the concerned coefficients relate to the largest AR lags of low magnitude, having small impact on the model itself and so they may be considered for omission. However, their variability does not substantially influence model performance. Therefore, it was possible to pronounce the computed ARMA model valid.

TABLE II

REESTIMATED COEFFICIENTS WITH HOLDOUT SAMPLE FOR MODEL BASED ON (2).

	c	β_1	β_2	β_3	β_4	β_5
value	6.86e-06	-0.194	-0.009	-0.029	0.372	-0.018
change	+659%	-51%	+93%	-302%	-15%	+90%

	β_6	β_7	β_8	β_9	β_{10}	β_{11}
value	0.256	0.392	0.274	-2.78e-08	-2.18e-06	-1.38e-05
change	+8%	+29%	-61%	-1622%	+21%	-315%

III. RESULTS

The result of mathematical modelling is a multiplicative ARMA model specified in (2) and Tab. I. The model was used to predict last six data points of computed APF signal by single and multi-step forecast. The results of the forecasting are on Fig. 2 and 3.

IV. DISCUSSION

Both figures show that the model correctly captured magnitude of all APF values because none departed out of the blue 95% confidence bounds. Single step forecast mistakenly anticipates downward and upward trend for second and last data point, but the predicted APF is tolerable. Multi-step forecast incorrectly assumed only downward trend for second data point and the actual prediction is also tolerable. Both figures support model validity.

From the perspective of mathematical modelling, it is clear that various patterns can be identified and used for future predictions. Application of the modelling using aviation safety data, despite the fact that they were partly synthetized, support this claim. ARMA models provide acceptable solution for cases, where data contain noise and behavioural pattern is often obscured. This is typical for soft data application, where limited amount or no hardware sensors can be applied. It is also an effective solution for cases where the predicted series cannot be measured directly, as is the case of safety performance.

Unconditional forecasts of safety performance allow to draw short-term future, assuming that the system won't be intervened. As soon as the system is changed by some targeted remedial measures, actual safety performance may be compared to the predicted, what allows retrospective evaluation of the measures. Another advantage is that results of such quantitative analysis provide key input to decision-making process, which is at present based rather on implicit mental models than on explicit control algorithms.

Important aspect is that the modelling cannot be used to predict actual events. In this study, the data used were aggregated from all available safety occurrences. The model then simply computes system-wide dependencies, which are not visible from raw data. Therefore, data to be used for such predictions should be sets of safety-related occurrences or various deviations, which have relevance to particular system interfaces between several components or complex systems as a whole. Safety occurrences, incidents, accidents, different failures or malfunctions, regardless of the technology concerned, are great candidates for suitable data, which are then to be aggregated by APF or similar methodology into system-wide figure or figures. Predictions using larger parts or whole systems enable brand-new view on how particular system works. They eliminate unnecessary concerns about truly random events and attract attention to actual risk increase.

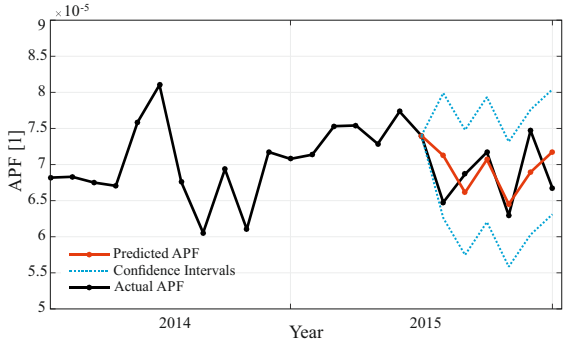


Figure 2. APF single step prediction by the means of ARMA model calculated as per (2).

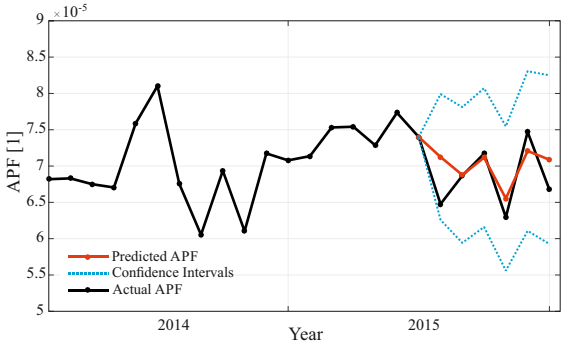


Figure 3. APF multi-step prediction by the means of ARMA model calculated as per (2).

V. Conclusion

This paper demonstrated elementary idea to allow better risk control in military systems. Military is a high-risk industry which needs to effectively control risks but it is quite complex and so it demands more advanced solutions. One of the solutions is to use safety performance as a tool to understand system-wide behaviour. Its predictions are one of the key features, which contribute to improved risk control. The research in this paper suggests that predicting such indicators, as safety performance, is possible and it may be of great benefit for safety managers.

Because of confidentiality restrictions in military, aviation safety data were selected as substitute to test the idea of predicting safety performance. It is certainly a limitation of this work but on the other hand, safety is based on the same essential solutions regardless of which high-risk industry is considered. Additionally, similarities in the technology used by civil and military aviation and commonalities in regulatory approach to their operations suggest that civil aviation safety solutions can be at least partly reused for military application.

Another limitation is the fact, that real data were not available to the extent, which would allow computing real safety performance. Part of the data had to be resampled by dedicated simulator. Even though this made it possible to evaluate advanced quantitative methods, the synthetic part of the data will never contain more than what was inserted into the equation of the resampling mechanism.

Deploying the predictions into real military environment requires adequate safety performance measurement. Aerospace Performance Factor offers an option but it is important to realize, that the data are to be robust and not relevant only to one or very few deviations or incidents. The system of predictions should never be set up for predicting individual events as this may lead to completely misleading assumptions. By contrast, best is to apply it for assessing the entire operations of complex system with many interacting components, because it is possible to understand and reasonably predict system-wide behaviour. Safety performance predictions should serve decision-making process regarding the overall system operations to help identify undesired deviations.

In military, there is still lot of room to develop robust solutions for ”online” monitoring and evaluation of safety performance. This is includes proper set up of safety performance indicators and adequate measurement of safety performance. One of the potential features for future is to introduce conditional forecasts by the means of explanatory variables, which could enter the model. On the other hand, this would require proper selection of such variables, which are in fact actuators, over which safety management has full control. Another potential exists regarding utilization of explanatory variables with limited or no control to assess their true effect on safety performance. This would allow quantitative analysis of deeper behavioural patterns in military safety. Developing such robust solutions may be painstaking process, but it is great opportunity to shift safety management into next evolutionary stage.

Acknowledgment

This work was supported by the Czech Technical University in Prague, junior research grant No. SGS16/188/OHK2/2T/16.

References

[1] J. Kraus, P. Vittek and V. Plos, “Comprehensive emergency management for airport operator documentation,” in *Proc. of International Conference on Engineering Science and Production Management (ESPM 2015)* , Slovakia: Tatranska Strba, 2015, pp. 139–144.

[2] P. Fuchs et al., “The assessment of critical infrastructure in the Czech Republic,” in *Proc. of 19th International Scientific Conference on Transport Means*, LT: Kaunas, 2015, pp. 418–424.

[3] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety.* Cambridge, MA: MIT Press, 2012.

[4] International Civil Aviation Organization, *Safety management manual (SMM),* 3rd ed. Montreal, Quebec: International Civil Aviation Organization, 2013.

[5] T. M. Lintner, et al., *The measurement of system-wide safety performance in aviation: Three case studies in the development of the aerospace performance factor (APF).* 2009.

[6] R. Golinelli and G. Parigi. "Real-time squared: A real-time data set for real-time GDP forecasting," *International Journal of Forecasting*, Vol. 24, Iss. 3, pp. 368-385, 2008.

[7] I.-C. Baciu. "Stochastic models for forecasting ination rate. Empirical evidence from Romania." *Procedia Economics and Finance*, Vol. 20, pp. 44-52, 2015.

[8] European Organisation for the Safety of Air Navigation. *White paper on performance-based certification of military airborne systems to meet civil ATM/CNS requirements: Civil-military ATM coordination division Communications-Navigation-Surveillance unit.* EUROCONTROL, 2013.

[9] J. Soeters and P. Boer, "Culture and Flight Safety in Military Aviation", *The International Journal of Aviation Psychology,* vol., 10, Iss. 2, pp. 111-133, 2000.

[10] European Organisation for the Safety of Air Navigation. *The Aerospace Performance Factor (APF): Developing the EUROCONTROL ESARR2 APF.* EUROCONTROL, 2009.

[11] C. Wang, L. Drees and F. Holzapfel, ”Incident prediction using subset simulation”, in *Proc. of ICAS 2014 29th Congress of the International Council of the Aeronautical Sciences,* International Council of the Aeronautical Sciences, pp. 1-8, Sep. 2014.

[12] P. E. D. Love, P. Teo, B. Carey, C. P. Sing and F. Ackermann, "The symbiotic nature of safety and quality in construction: Incidents and rework non-conformances," *Safety Science,* vol. 79, pp. 55-62, Nov. 2015.

[13] "Performance Review Unit (PRU) Portal," PRU. [Online]. Available: http://ansperformance.eu/

[14] "2014 - EU wide level - ANS performance monitoring," 2015. [Online]. Available: http://www.eurocontrol.int/prudata/dashboard/eur_view_2014.html

[15] "ANS performance monitoring (RP2, 2015)," 2015. [Online]. Available: http://www.eurocontrol.int/prudata/dashboard/rp2_2015.html

[16] R. F. Nau, "Statistical forecasting: Notes on regression and time series analysis,". [Online]. Available: http://people.duke.edu/~rnau/411home.htm

[17] J. C. Chambers, S. K. Mullick and D.D. Smith, “How to choose the right forecasting technique”. *Harvard Business Review*, 49, p. 45-71. 1971.

[18] R. B. Millar, *Maximum likelihood estimation and inference: With examples in R, SAS, and ADMB.* United States: Wiley, John & Sons, 2011.

[19] E. P. Box, G. M. Jenkins and G. C. Reinsel, *Time series analysis: Forecasting and control,* 4th ed. United States: John Wiley & Sons, 2008.

[20] D. Kwiatkowski, P. C. B. Phillips, P. Schmidt and Y. Shin, "Testing the null hypothesis of stationarity against the alternative of a unit root," *Journal of Econometrics,* vol. 54, no. 1-3, pp. 159-178, Oct. 1992.

[21] M. H. Kutner, C. J. Nachtsheim, W. Li, and J. Neter, *Applied linear statistical models,* 5th ed. Boston: McGraw-Hill Inc.,US, 2004.

Appendix E

LALIŠ, Andrej, Peter VITTEK and Jakub KRAUS. Process modelling as the means of establishing semi-automated safety management. In: *Proceedings of 20th International Scientific Conference*. Transport Means 2016.

Proceedings of 20th International Scientific Conference. Transport Means. 2016.

Process modelling as the means of establishing semi-automated safety management

A. Lališ*, P. Vittek, J. Kraus*****

**Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Horská 3, 128 03 Praha 2, Czech Republic, E-mail: lalisand@fd.cvut.cz*
***Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Horská 3, 128 03 Praha 2, Czech Republic, E-mail: vittek@fd.cvut.cz*
***Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Horská 3, 128 03 Praha 2, Czech Republic, E-mail: kraus@fd.cvut.cz*

Abstract

This paper introduces process modelling with regard to its potential to establish semi-automation of decision-making within safety management. High-risk industries are facing intangible nature of their safety-related issues, commonly involving human and system component interactions. To date, they typically utilize mental models to understand the processes, which they aim to control. This paper deals with the transition from mental models to the hybrid form of mixed mental and automated parts where the latter stem from partial formalisation of the existing process models. Issues with variables and their quantification are described and addressed accordingly within proposed solutions. These solutions are capable of formalising mental models and providing basis for automated elements that can reduce the burden of human controller. Interpretation and aggregation issues are outlined and links to both the control algorithms and sensors used by safety management are introduced. Aviation industry application is used to demonstrate the solutions.
KEY WORDS: *Process modelling, safety management, safety performance indicators, aviation safety*

1. Introduction

High-risk industries are to various extent concerned about intangible system properties which are to be handled in order to not allow accidents to take place. The extent depends on the industry; some are already well automated and most of the issues can be tracked using sensory data, others involve greater variety in terms of system components and interactions among themselves or with the environment. Normally, hardware systems with predefined behaviour patterns, regardless of the amount of system components, are relatively simple when it comes to tracking undesired behaviour or resolving its occurrence in the future. On the other hand, there is special attention dedicated to humans, which are the most hard-to-predict elements in any system as far as their performance is concerned [1], and so they are still subject of an intensive research in high-risk industries (such as [2], [3] or [4]). The more the industry contains such hardly predictable elements or complex interactions, the more difficult it is to establish effective safety management system and the more mature the solutions have to be.

This article focuses especially on presence of intangibility, where currently the most room for improvements exists. Intangibility means that the controlled process cannot be tracked with any hardware sensors, but needs to be observed by human personnel, whether through oversight activities (such as audits) or through direct reporting from line personnel which may recognise deficiencies during their work performance. These types of sensors are sometimes called as “soft” sensors and are well-known for their likely increased bias and distortion for various motivations and goals of the humans involved [5].

To facilitate effective establishment of soft sensors where these are needed, many international and industry-wide efforts already exist. Especially within nuclear power, chemical or aviation industry, remarkable progress has been achieved recently ([6], [7] and [8]). However, the cognitive process, which has to follow to interpret the data obtained and to support effective control algorithms to be implemented, still exhibits immaturity. It is owing to the fact that the cognitive and control algorithms remain mental, entirely dependent on respective human controller (e.g. safety manager) and therefore also very unique at the time. This is one of the contributory factors to the controlling inadequacies. Nevertheless, the increasing maturity of the soft sensors provides progressively more and more opportunities to formalise objective knowledge and understanding, making it possible to reduce the room for human control inadequacies by the introduction of automation elements.

2. Process model and its automation

Process model is typically comprised of set of variables and their values [9]. These variables should capture all system-critical properties in terms of given management criterion (in this case safety) in a consistent way. Incompleteness or incorrectness of the model lead to incomplete or incorrect picture of what is happening in the

controlled process and subsequent confusion about inadequate or ineffective control actions. Automation may be included to take over part of the cognitive process by using mathematical equations, which process the information from sensors and provide the controller with additional layer of information or guidance. From theoretical standpoint, the system with automation would follow the scheme depicted on figure 1.

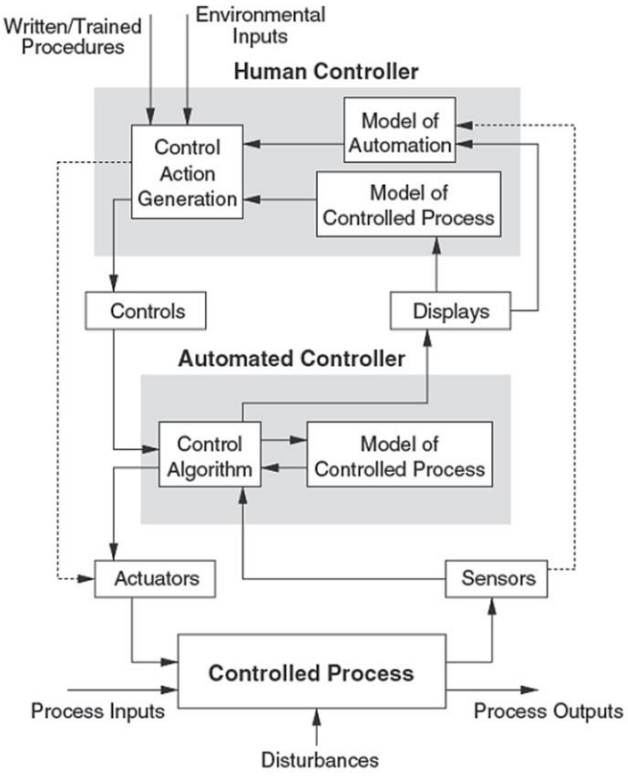


Fig.1 Automation and process model [10]

Normally, the human controller needs to supervise both the controlled process and the automation and therefore may often be in need of direct access to the physical actuators and sensors in case the automation fails or acts inadequately. This is the case for safety management as the soft sensors are likely to be biased and certainly need strict supervision. The formalised model of controlled process, that the automation will be based upon, should be known to the human controller so he or she understands why the automation acts as it does. Besides that, the controller needs to establish his own model of the controlled process, which should complement the automation process model but also be capable of correcting it, if necessary.

The system depicted on figure 1 shows typical hardware solutions where human supervision exists. In aviation, this model is becoming widely spread for instance concerning aircraft technology, where today's pilots are flying semi-automated airplanes, most of the flight time only supervising the automation. Further application of this system to soft sensors and complex socio-technical systems could provide safety management with similar benefits.

3. Variables and their interpretation

Process model variables are gathered via sensors application on the controlled process output. As already mentioned, socio-technical systems in many cases have no applicable hardware sensors and so the sensors are naturally soft, based on occurrence and investigation reports or audit findings. Where possible, hardware sensory data may complement the picture, but usually they are not sufficient to effectively control safety of operations. The issue is that soft sensors need to be well-defined to have explanatory value for further processing.

Soft sensors gather information about conditions and events. These are related then to the recorded undesired output of the controlled process in form of contributory factors. Sometimes, negative potential of some conditions and events is recognised only after an incident or accident what makes proper setting of the sensors more difficult. Also, technology and the environment dynamically change and new challenges emerge so as the old disappear continuously. The ultimate goal is to have complete list of the so-called safety performance indicators (SPIs) at all times and up to date. Surely, this process needs to be coordinated within particular industry between its stakeholders, otherwise the stakeholders may struggle to keep the pace with the industry evolution.

SPIs are measuring the output using normalised sum of each indicator's observations [11]. In other words, each identified contributory factor should be considered to be measured as SPI, where number of its observations will be normalised as follows:

$$SPI_i = \frac{N_i}{appropriate\ denominator} \quad (1)$$

where N_i is the number of observations of the SPI during time interval i. Denominator is deemed appropriate when it reflects the exposure to the risk, e.g. duration of operations, amount of delivered services or products etc.

Other types of SPIs may be aimed at assessing the degree of safety management system maturity or application of certain principles, where the principles on how to operate correctly such management systems are confronted with the observation of the existing system [12]. These SPIs are being measured using questionnaires so that the evaluator gets some level (alphabetical A to E or numerical 1-5 or similar) or percentage at the end of the evaluation process. The variables may need to be transformed in order to make it possible to process them. Best is to select some numerical scale, for example between 0 and 1, and distribute the conceivable results on that scale. Some SPIs' quantification may be tricky, but even if it is not done properly, there is still the opportunity to refine the shortages within the automation process model. The core of automation technology can determine the most suitable solution for quantification solution, but the only way to assure reasonable accuracy is to use industry subject matter experts jointly with experts on system modelling.

Finally yet importantly, some SPIs may be identified on the controlled process input. These can be divided into those, which we can control (such as allocation of resources, training schedule, safety promotion activities etc.), and those we can only measure (such as market conditions, demand, year season etc.).

All in all, the complete list of SPIs should include as much as possible of the variables that have significant potential to influence the controlled process, numerically expressed. Certainly, the identification of such variables may be time-consuming task and may involve interdepartmental and even interorganisational cooperation. The more complex the system, the higher the potential of automation to facilitate the cognitive process and subsequent decision-making.

4. Aspects to consider

From the system theory, there are some aspects to consider for any solution [10]:

- The data from sensors may be missing, delayed or inadequate
- The process model may be inconsistent, incorrect or incomplete

Each of these aspects needs to be addressed. Certainly, particular application depends on the environment where the process model and its automation is to be established, but these aspects remain invariable. Subject matter experts must consider them when the automation is being designed, otherwise the system will need to be redesigned if the non-addressed aspects result in an incident or accident.

Establishing complete, timely and adequate sensors requires experts from all the departments or even from other organisations or regulatory bodies in the industry. Involving professionals from all key areas in the design process will reduce the likelihood of any flaws in the sensors' design. Parameters such as management's reaction time, information infrastructure specifications or typical background of the controlling personnel must be considered, so that the information gathered is unambiguous and can be delivered to the automation controller and processed whilst still providing enough time for human controller to make decision.

The automation process model is critically dependent on the sensors and its inconsistency or incompleteness may be in some cases entirely dependent on them. Inadequate sensors lead to inconsistent process model and missing sensors for tracking critical system properties lead to its incompleteness. On the other hand, the process model for automation must ensure utilization of adequate processing mechanisms, so that no information is lost, misinterpreted or inconsistent in terms of describing the controlled process. There are various ways, how to approach these aspects but it is, usually, the core of the automation technology which determines what and how is to be processed. For example, one of the solutions for core of automation is deployment of state-space model, which follows denotation [13]:

$$x_{t+1} = Mx_t + Nu_t + w_t \quad (2)$$

$$y_t = Ax_t + Bu_t + v_t \quad (3)$$

where $w_t \approx \mathbb{N}_w(0,\, r_x)$ and $v_t \approx \mathbb{N}_v(0,\, r_y)$ representing white innovation noise at the discretely running time t. The innovation noise aims to capture random disturbances, y_t is the measured output, x_t is the state and u_t represents measured input. A, B, M and N are matrices or vectors of parameters. State x_t is something that cannot be directly measured but it varies in time. Usually, it is comprised of all variables, including those which can be calculated indirectly only. Measured output y_t is obtained directly. This solution is similar to those in use for hardware automation, but for socio-technical systems it will be much more biased through the white innovation noises. Only proper selection of the variables and their quantification can provide the desired effect.

Because of the restrictions of the state-space model and given the intentions to apply it for automation, not only does the model influence the sensors and way to quantify them, but it also lays down principles on how to make consistent, complete and correct model itself [13]. When obeyed, the mathematical methods assessing consistency and efficiency of the model assure its desired properties for any practical application.

5. Embedding the system into aviation

Aviation industry is now focused on SPIs and their correct implementation as well as quality of safety data gathered [14]. The more is the industry mature on safety management, the more there is the space for application of the automation. Some efforts already addressed SPIs aggregation where, as a result, a safety performance signal was received [15]. This aggregation provides even more room for the automation, as the signal received resembles usual hardware signals received from hard sensors and so it may be processed and analysed in similar way, although taking into account the inherent soft nature of the sensors.

Applying the space-state model from previous chapter, all the aviation best practice SPIs can be processed. The industry has its regulations and there are numerous safety documents available, which are aimed at understanding aviation safety issues and formalising contributing factors (such as [16], [17] or [18]). Apart from the regulatory required SPIs, these documents provide sound basis for SPIs implementation. Some of the regulatory SPIs need transformation of their values from letters to numbers, some other SPIs may need scale adjustment, but in general there is no SPI in aviation which cannot be processed via state-space model. For the input matrices, besides regulatory SPIs such as Effectiveness of Safety Management or Just Culture, contextual information can be used such as year season, local GDP or any other indicator that influences the operations of aviation in terms of safety. Significance of each of these variables will be captured within the parameter matrices or vectors in equations 2 and 3. Parameter estimation will stem the data available in the industry and where needed, it may even alter the way the data is gathered.

The appropriate denominator from equation 1 is in aviation usually number of flights or number of sectors flown. All the SPIs can be directly measured (despite serious bias present in the measurement); the only indirectly measured variable is safety performance, which would then appear as the state in the state-space equation. Its value is measured indirectly from all the other SPIs via published methodology. Whilst there still exists potential to improve the methodology to provide more accurate aggregation, such as via Analytical Network Process application instead of Analytical Hierarchy Process or simple pair-wise comparison, for the purpose of initial automation deployment it is sufficient.

Another feature that the automation may use is safety performance prediction. It has the potential to facilitate the decision-making process and to validate the state-space model. With regard to the state-space model itself, the prediction is based upon the principles of predicting with linear regression models or ARIMA models [13]. The automation process model can then be integrated per aviation organisation type and per regulatory body, formalising the available knowledge and providing understanding of following:

- what has more impact on the aviation and what less impact,
- if the system is intervened, what will most likely happen
- what is normal in the system and what can be considered as undesired deviation

The performance predictions would provide a whole new level of understanding the controlled process. Automating its parts where such formalisation of knowledge can be introduced can finally provide more room for better and more adequate actions by the human controller. Certainly, such automation should in no way have direct access to the system actuators because of the mentioned bias, but it should only provide the human controller with the knowledge that he or she simply cannot observe directly from the sensors. The controller will still need to establish some mental process model where knowledge formalisation is not possible, but the room for bias will be considerably reduced by the automation, eventually improving safety of operations.

6. Conclusions

Formalisation of the existing safety management knowledge and its subsequent use for establishing partial automation of safety management processes has potential to replace parts of the mental models used to control safety processes to date. By doing so, not only will be some of the burden taken away from safety management and its human controllers, but it will also provide additional information, which cannot be observed directly from the safety performance indicators. This additional information shall improve adequacy and accuracy of safety management's control actions and may even provide the management with justifications for the actions, investments etc. With the increasing maturity of soft sensors, application of automation is becoming similar to hardware technology application despite the noise present in the safety data. When addressed accordingly, the noise can be reduced to an acceptable level what makes it possible to process or aggregate and properly analyse the data gathered. Due to the generalised nature of the solutions, this technology advance can reduce the number of incidents or accidents in the future regardless of the domain of its application.

Acknowledgement

This paper was supported by the Grant Agency of the Czech Technical University in Prague, grant No. SGS16/188/OHK2/2T/16.

References

1. **U.S. Department of Energy.** Human Performance Improvement Handbook: Volume 1: Concepts and Principles. DOE-HDBK-1028-2009. Washington, D.C. 20585. 2009.
2. **Novák, L., Němec, V. and Soušek, R.** Effect of Normobaric Hypoxia on Psychomotor Pilot Performance. In The 18th World Multi-Conference on Systemics, Cybernetics and Informatics. Orlando, Florida: International Institute of Informatics and Systemics, vol. II, p. 246-250. 2014. ISBN 978-1-941763-05-6.
3. **Socha, V. - Szabo, S. - Socha, L. - Kutílek, P. - Němec, V.** Evaluation of the Variability of Respiratory Rate as a Marker of Stress Changes. In TRANSPORT MEANS 2014. Kaunas: Kauno technologijos universitetas, 2014, p. 339-342. ISSN 1822-296X.
4. **International Atomic Energy Agency (IAEA)**. Managing Human Performance to Improve Nuclear Facility. Vienna: Intl Atomic Energy Agency, 2014. ISBN 978–92–0–144610–7.
5. **Fortuna, L., Graziani, S., Rizzo, A., Xibilia, M.G.** Soft sensors for monitoring and control of industrial processes. London: Springer, c2007. ISBN 978-1-84628-480-9.
6. **International Atomic Energy Agency (IAEA)**. Operational safety performance indicators for nuclear power plants: IAEA-TECDOC-1141. Vienna, 2000. ISSN 1011-4289.
7. **Organisation for Economic Co-operation and Development (OECD).** Guidance on Developing Safety Performance Indicators related to Chemical Accident Prevention, Preparedness and Response, No. 18. Second edition. Paris, 2008.
8. **International Civil Aviation Organization (ICAO).** Safety management manual (SMM). Third edition. Montreal, Quebec: International Civil Aviation Organization, 2013. ISBN 978-92-9249-214-4.
9. **Hangos, K. M., Cameron, I. T.** Process modelling and model analysis. San Diego: Academic Press, c2001. ISBN 978-0121569310.
10. **Leveson, N.** Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, c2011. Engineering systems. ISBN 978-0262016629.
11. **Verstraeten, J.G., Roelen, A.L.C., Speijker, L.J.P. (NLR).** Safety performance indicators for system of organizations in aviation. 2014, 28 p. Available from Internet: https://www.ascosproject.eu/downloads/ascos_paper_verstraeten.pdf
12. **European Aviation Safety Agency (EASA).** Annex to ED Decision 2014/035/R: Acceptable Means of Compliance and Guidance Material for the implementation and measurement of Safety (Key) Performance Indicators (S(KP)Is) (ATM performance IR). Issue 2. Cologne, Germany. 2014.
13. **Harvey, A. C., Koopman, S. J., Shephard, N.** State space and unobserved component models: theory and applications. Cambridge: Cambridge University Press, c2004. ISBN 0-521-83595-X.
14. **European Aviation Safety Agency (EASA).** Annual Safety Review 2014. Luxembourg, 2015. ISBN 978-92-9210-195-4.
15. **European Organisation for the Safety of Air Navigation (EUROCONTROL).** The Aerospace Performance Factor (APF): Developing the EUROCONTROL ESARR 2 APF. Brussels, Belgium, 2009. Available from Internet: http://aloftaviationconsulting.com/publications/ECTL APF Implementation Plan.pdf
16. **European Organisation for the Safety of Air Navigation (EUROCONTROL).** Operational Safety Study: Conflict detection with adjacent sectors. Edition 1.0. Brussels, 2015. Available from Internet: https://www.eurocontrol.int/sites/default/files/publication/files/top-5-safety-n4-study-conflict-detection-adjacent-sectors.pdf
17. **International Civil Aviation Organization (ICAO).** Doc 9870: Manual on the Prevention of Runway Incursions. Montréal, Quebec, Canada, 2007. Available from Internet: http://www.icao.int/safety/runwaysafety/documents%20and%20toolkits/icao_manual_prev_ri.pdf
18. **NLR Air Transport Safety Institute, G.W.H. van Es.** Study of Runway Excursions from a European Perspective. Report no. NLR-CR-2010-259. Amsterdam, 2010. Available from Internet: http://www.nlr-atsi.nl/downloads/a-study-of-runway-excursions-from-a-european-p.pdf

Appendix F

KŘEMEN, Petr, Bogdan KOSTOV, Miroslav BLAŠKO, Jana AHMAD, Vladimír PLOS, Andrej LALIŠ, Slobodan STOJIĆ. Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems. *Journal of Aerospace Information Systems*, 2017, 14(5), pp. 1-14. DOI: 10.2514/1.I010441.

JOURNAL OF AEROSPACE INFORMATION SYSTEMS
Vol. 14, No. 5, May 2017

Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems

Petr Křemen,* Bogdan Kostov,* Miroslav Blaško,* Jana Ahmad,* Vladimír Plos,† Andrej Lališ,†
Slobodan Stojić,† and Peter Vittek†
Czech Technical University in Prague, 16627 Prague, Czech Republic

DOI: 10.2514/1.I010441

The European Coordination Centre for Accident and Incident Reporting Systems develops an information system for reporting aviation occurrences on the European scale. The system makes use of various taxonomies, like the taxonomy of event types, or a taxonomy of descriptive factors. However, the European Coordination Centre for Accident and Incident Reporting Systems data model and associated taxonomies are complex and difficult to understand, which reduces interpretability of the records. In this paper, the problems European Coordination Centre for Accident and Incident Reporting Systems users face during occurrence reporting are discussed, as well as subsequent searches in reported occurrences. Next, it is shown how proper conceptual modeling with ontological foundations could leverage the quality of occurrence categorization, and thus better exploitability of the European Coordination Centre for Accident and Incident Reporting Systems system. The ontological model is demonstrated on the Aviation Vocabulary Explorer, which is a new prototypical tool for exploring European Coordination Centre for Accident and Incident Reporting Systems.

I. Introduction

THE system used in Europe to record aviation safety occurrences on the corporate, national, as well as European levels is difficult to use, both by those who wish to record incidents and those who wish to use the reported data. We propose here an ontology-based approach that helps to simplify the reporting process, and thus improve the quality of the collected data.

Reporting safety occurrences in the aviation domain at the European level is an important and steadily growing requirement of the European Aviation Safety Agency (EASA). The EASA enforces use of the European Coordination Centre for Accident and Incident Reporting System (ECCAIRS) [1] for occurrence reporting on the national and European levels. The system uses large terminologies and taxonomies containing thousands of terms related to occurrences, events, their factors, as well as other data attributes like aircraft categories or event phases. These terms are connected by a single type of relation that is used in different meanings (see Sec. III.B.3), and thus negatively influences both reporting (a term is difficult to find) and data analyses (the term is difficult to interpret), which try to use the reported data as a basis for safety issues and safety performance indicators. For example, one of the options the EASA provides for reporting occurrences is a Web form [2] that contains approximately 100 different attributes together with more than 3000 possible attribute values. As a result, the system is too complex for reporters [3] who, as a consequence, fail to fill all relevant data or (even worse) fill in incorrect/imprecise data.

We analyze here the problems and offer the aviation ontology, which is an ontology-based approach for improving the ECCAIRS knowledge structure to be more compact and intuitive to use. One of the key benefits of this approach is disambiguation of terminology definitions, thus improving its manageability. From the reporter's point of view, the ontology improves explorability of the ECCAIRS terminology by using a smaller number (reduction from a few thousand terms to a few hundred) of simpler terms. Another benefit is the disambiguation of the data-driven safety indicators, and thus better interpretation of their results. Thus, the primary users of the ontological knowledge (and applications built on its top) are reporters, safety managers, and safety officers of aviation organizations. In the future, the aviation ontology can help in ECCAIRS evolution to redesign and simplify its structure.

The paper is organized as follows. Section II discusses work related to ours. In Sec. III, we introduce the ECCAIRS data model and explain its current issues. Next, in Sec. IV, we introduce formal ontologies as a technique for disambiguation of diverse and dynamic data. In Sec. V, the aviation ontology is introduced together with main design decisions made during its design. To see the ontology in action, we show the Aviation Vocabulary Explorer, which is a prototypical tool for exploring ECCAIRS in Sec. VI. The paper is concluded in Sec. VIII, discussing the overall reporting scenario and future directions.

II. Related Work

Besides ECCAIRS (described in detail in the next section), many aviation safety taxonomies [4] have evolved. Although mandatory occurrence reporting in Europe is managed by the EASA, EUROCONTROL (which is a European organization providing air traffic management coordination) uses the e-Toolkit for ATM Occurrence Investigation (TOKAI) Web application [5] to collect occurrence risks reported by national air navigation services providers. To evaluate the occurrence risk, e-TOKAI supports the creation of an occurrence report compliant with ECCAIRS. Additionally, e-TOKAI uses the Harmonization of European Incident Definitions Initiative for Air Traffic Management (HEIDI) taxonomy [6] for describing specific safety-related terminology for air traffic management (ATM), including event types (like air–air collision), their descriptive factors (like phraseology), and explanatory factors (readback error). HEIDI has similar problems as the ECCAIRS Taxonomy (see Sec. III), like the terms redundancy and ambiguity (e.g., descriptive factor "Documentation/charts" vs explanatory factor "Documentation"). The Commercial Aviation Safety Team/International Civil Aviation Organization Common Taxonomy Team (CICTT) [7] creates taxonomies for occurrence reporting that involve, e.g., hazards, humans factors, system/component malfunctions, or occurrence categories. The latter is reused in the ECCAIRS occurrence category taxonomy.

Received 1 December 2015; revision received 8 February 2017; accepted for publication 24 February 2017; published online 6 April 2017.

*Researcher, Department of Cybernetics, Faculty of Electrical Engineering, Technická 2.
†Researcher, Department of Air Transport, Faculty of Transportation Sciences, Technická 2.

EUROCONTROL also offers the ATM Lexicon [8], providing comprehensive ATM-related terminology equipped with mutual links (e.g., the runway incursion term is related through the related entries link to the runway excursion term). The ATM Lexicon is meant as a general reference vocabulary, it is not part of any reporting tool. Another general vocabulary is provided by the aforementioned CICTT initiative [9].

The Human Factors Analysis and Classification System (HFACS) [10] is a vocabulary for describing human and organizational causes of accidents in aviation domain. Although one of ECCAIRS taxonomies (explanatory factors) deals with human and organizational causes of occurrences, no information is available on any harmonization efforts between the HFACS and the ECCAIRS.

The design process and history of these vocabularies/taxonomies are not described explicitly by their authors. Furthermore, with the exception of CICTT occurrence taxonomy, no harmonization between the ECCAIRS and other mentioned vocabularies/taxonomies exists: also because of the difficulty of finding the proper semantic relationship between terms in different taxonomies. The sound ontological analysis shown in this paper addresses this issue.

In the field of aircraft structure/design, the air transport association (ATA) [11] and the Joint Aircraft System/Component Code (JASC) [12] are well-known and established taxonomies used by the Federal Aviation Administration. The ATA classification is used in the ECCAIRS system for referencing occurrence factors related to aircraft components. An ontology for aircraft design was introduced in [13].[‡] It provides a coarse taxonomy of the essential parts of an aircraft. However, it does not specify relationships to standard vocabularies like the ATA and JASC.

Ontological descriptions of air campaigns were already studied in the 1990s [14]. An ontological approach for modeling aeronautical domain was introduced in [15]. An ontology-based learning system for air traffic control was introduced in [16]. These ontologies were backed by sound ontological analysis, but they are not applicable for aviation safety, as they lack the fundamental notions for occurrence reporting and event modeling.

Knowledge support for safety management has been studied for decades in various high-risk environments, like transportation (including aviation and space) or industrial environments (including powerplants), resulting in various models focusing different parts of safety, like in [17] or [18]. The latter used Ishikawa diagrams to model causes and effects of safety events, which was similar to the ECCAIRS (and thus aviation ontology) notion of factors. Some knowledge structures also involve ontologies, like [19,20], or [21]. However, none of these knowledge structures were tailored to aviation safety reporting in terms of vocabulary and appropriate event/occurrence modeling.

The mentioned taxonomies, vocabularies and ontologies are only supplementary to the ECCAIRS, which remains the first choice for aviation safety reporting in Europe. The aviation ontology proposed in this paper leverages the usability of the ECCAIRS by providing an ontologically sound model of aviation safety situations resulting in more intuitive and simpler ECCAIRS navigation, as well as integration of the ECCAIRS with other taxonomies. Contrary to the generic safety management ontologies mentioned previously, our aviation ontology is an event-centric ontology designed on top of aviation vocabulary.

III. ECCAIRS Overview

The ECCAIRS system has been developed since the 1990s [22] by the Joint Research Centre of the European Commission, and it is currently available in its fifth edition (ECCAIRS 5). The system is aimed at safety reporting in various high-risk industries (domains), with each represented by a separate data model ("taxonomy" in ECCAIRS wording). The ECCAIRS aviation taxonomy, Version 3.4.0.2, is compliant with the ECCAIRS 5 system and is publicly accessible at the ECCAIRS portal [1] for EASA-approved users (e.g., national authorities).

On the European Union (EU) level, the ECCAIRS has been provided by the EASA to the national authorities for the purpose of mandatory reporting on the national level for several years. In November 2015, the new EU regulation 376/2014 [23] came in action, complementing EU regulation 1018/2015 [24], together specifying which event types, as well as attributes, needed to be collected from aviation organizations during safety reporting. Both regulations are harmonized with the ECCAIRS taxonomies, and the EASA enforces these regulations through the ECCAIRS system. The national civil aviation authorities in the EU are obliged to use the ECCAIRS for mandatory safety reporting. Each national authority runs its own ECCAIRS server, which is configured to send reports to the European Central Repository maintained by the EASA. On the national level, aviation organizations do not use the ECCAIRS. Instead, they report occurrences using predefined forms [2] (approximately half of the EU states use a form defined by the EASA, whereas the other half use ad-hoc-designed national forms). In summary, the ECCAIRS is mandatory at the EU level and its complexity is propagated to the reporting aviation organizations by means of the occurrence forms provided by national authorities.

The ECCAIRS aviation taxonomies evolved from the Accident/Incident Data Reporting (ADREP) system [25], which is a data structure maintained by the International Civil Aviation Organization (ICAO) since the 1970s. In 2004, the ICAO adopted the ECCAIRS for occurrence data collection [26]. Today, no clear distinction between the ECCAIRS and ADREP can be tracked. For example, the ICAO released a set of documents [27] in 2013, referenced as "ADREP Taxonomy," as well as the "ECCAIRS Aviation 1.3.0.12 Data Definition Standard"[§] on the ICAO Web pages. The EASA evolves its own line of aviation taxonomies to be used in the ECCAIRS system. Most of them are taken from the original ADREP taxonomies, and some of them are new (like the CICTT taxonomies). We will consistently refer to all these taxonomies as "ECCAIRS aviation taxonomies." ECCAIRS aviation taxonomies describe occurrences, events, their factors, as well as other data attributes, like aircraft categories or event phases. The evolution of the ECCAIRS aviation taxonomies has resulted in thousands of terms in the aforementioned Version 3.4.0.2, which is currently used by the EASA.

The ECCAIRS data model consists of entities, attributes, and values. The ECCAIRS distinguishes several dozen entities (which vary across different ECCAIRS versions) interconnected by means of a single relation. For example, an *Aircraft* entity has as its children one or more *Event* entities and one or more *Engine* entities. Additionally, an entity is equipped with attributes that denote particular properties of the entity. For example, an *Aircraft* entity has attributes of *Fatal* and *Cabin Crew* (denoting the number of deaths for cabin crew), as well as an attribute *Aircraft* category (classifying the aircraft as an airplane, helicopter, glider, free balloon, etc.). Although the former changes from occurrence to occurrence for the particular aircraft, the latter remains the same; this distinction is not captured by the ECCAIRS data model. Some ECCAIRS attributes have predefined lists/trees of values (value lists), whereas others are filled manually. Each report filling method is discussed in the following:

1) Manual entries are filled manually. These involve identification of the aircraft and aerodrome, as well as the operated airspace and responsible air traffic service unit, together with their properties, like injuries, history of flight, maintenance records, and others. Most of these entities and their attributes define the state of the involved objects. ECCAIRS Taxonomy Version 3.4.0.2 contains 370 such attributes.

2) Predefined value lists are filled by selecting an appropriate value from a predefined list. There are 455 such attributes in ECCAIRS Taxonomy Version 3.4.0.2. The largest-value lists are flat lists of worldwide data, like ICAO locations (e.g., LKPR), reporting entities (like civil aviation

[‡]Data available online at https://github.com/astbhltum/Aircraft-Ontology [retrieved 2017].

[§]Data available online at http://www.icao.int/safety/airnavigation/AIG/Documents/ADREP%20Taxonomy/ECCAIRS%20Aviation%201.3.0.12%20(Entities%20and%20Attributes).en.id.pdf.

Table 1 Number of terms in the largest value lists relevant to occurrence classification (Desc., descriptive; Expl., explanatory)

Value list	Count of terms
Occurrence category	36
Event type	2617
Phase	309
Desc. factor subject	2061
Expl. factor subject	555
Desc./expl. factor modifier	720

authority of the Czech Republic), operators (like Germanwings), and others. From the perspective of safety reporting and safety investigation result modeling, taxonomies of events/descriptive factors/explanatory factors are fundamental, as shown in Table 1.

Core ECCAIRS entities and attributes relevant to occurrence classification are depicted in Fig. 1. The figure shows that each occurrence is described using a chain of events. Each event in this chain can be assigned to various entities connected to the occurrence, e.g., an aircraft or an aerodrome. The size of the value lists of the respective attributes is depicted in Table 1. Each value list needs to be explored by the reporter to select the appropriate category/categories.

Let us review the basic concepts taken from the ECCAIRS 3.4.0.2 definitions:

1) *Occurrence* is defined as an *accident or incident* throughout this taxonomy. Generally, accidents and incidents differ only in the degree of injury sustained by the persons involved or in the damage sustained to the aircraft. Each *(Occurrence category) has* a unique name and identifier to permit common coding in accident/incident systems, a text definition, and usage notes to further clarify the category and aid in coding occurrences . . . , e.g., "AMAN: Abrupt Maneuvre," or "CFIT: Controlled Flight into or toward Terrain."

2) The *event type* is defined as "The type of event, i.e., aircraft/system/component, consequential, air navigation services, aerodrome and ground aids, CAA, other or unknown [1]."

3) The *phase* is defined as "The phase of flight that relates to the event," e.g., "Approach" or "Post-Impact."

4) The *descriptive factor subject* is "The subject of a descriptive factor. Descriptive factors are a combination of a subject, e.g., aircraft/operations, air traffic management, aerodrome, meteorological or terrain, and at least one modifiers. The subjects provide information on the subject area described and the modifiers indicate the nature of the involvement of the subject," e.g., "Takeoff clearance," "Runway," "Propeller," etc.

5) The *explanatory factor subject* is "The area of concern or subject described in the explanatory factor," e.g., "Liveware (human)", "Human vs procedures," etc.

6) The *descriptive/explanatory factor modifier* is described as follows: "Modifiers provide information on the nature of the involvement of the subject to which they relate," e.g., "Correct," "Wrong," or "High."

In the next sections, we will introduce the flaws of the ECCAIRS that we identified during analysis. These problems complicate ECCAIRS usage during reporting or exploitation of the terms during data analysis.

A. ECCAIRS Data Model Aspects

1. *Insufficient Link Between Attributive and Classification Data*

Both types of data introduced in the previous section are strongly connected. Take event type 2200102 "Runway incursion by a Vehicle/Equipment" as an example. Whenever an event is classified to be of this type (taxonomy class is assigned), there are numerous basic data (attributes) to be collected. For example, for the case of the selected event type, the required data involve 1) the information about the particular location of the event, 2) which vehicle was incorrectly present on the runway, 3) whether the vehicle was cleared to use the runway or not, 4) whether there was conflicting traffic and its identification, and 5) whether the conflicting traffic was cleared to use the runway or not.

Schematically, an example representation of such an occurrence in the ECCAIRS is shown in Fig. 2.

However, when constructing such a report, the reporter has no information about which ECCAIRS attributes are relevant for which event types. As a result, the ECCAIRS cannot guide the reporter through the relevant data collection. Reporting a single event, classifying it into a flight phase, and assigning a single descriptive factor, and a single explanatory factor forces the reporter to decide over more than 5500 ECCAIRS Aviation 3.4.0.2 classes. Even though the user interface might help to organize the terms for the reporter, the final responsibility of exploring and deciding on these options is on the reporter. In our opinion, this cannot be responsibly and reliably done, forcing reporters to select too-general terms, wrong terms, or no terms at all. This negatively influences the quality and completeness of the collected data.

2. *Data Model Ambiguity*

The distinction between event types, descriptive factors, and explanatory factors is not clear. Some situations can be modeled as a chain of events, as an event with assigned descriptive factors, or as an event with assigned descriptive factors and explanatory factors. For example, the distinction between event type 4010203 "Provision of air navigation services (ANS) weather information" and descriptive factor 24010500 "Air traffic control provision of weather information" is not clear. In the case where an occurrence involves wrong information provided by air traffic

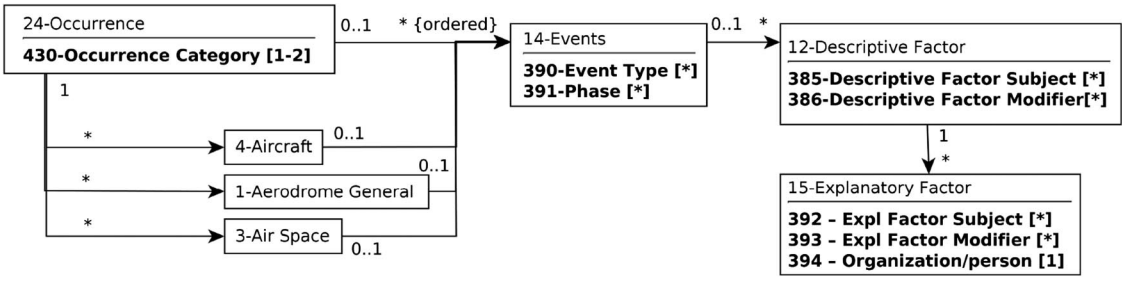


Fig. 1 Core of ECCAIRS data model classifying events and its factors (Expl, explanatory).

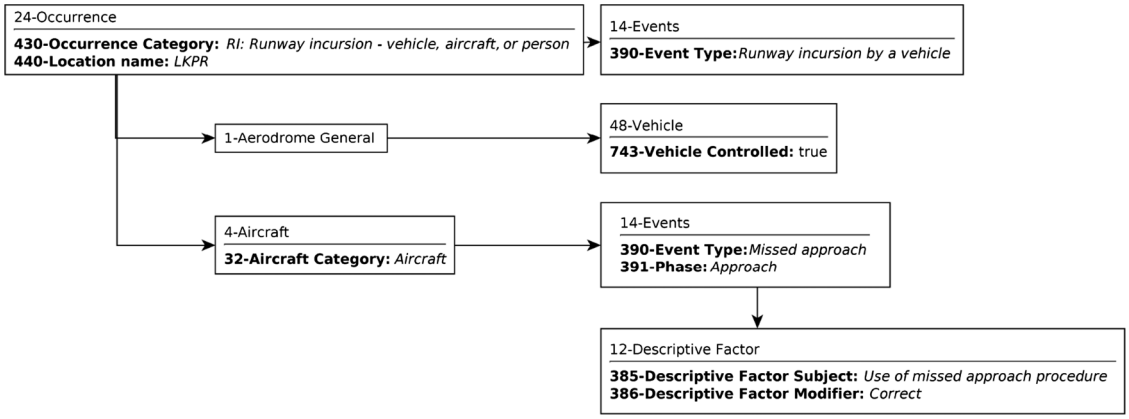


Fig. 2 Schematic data model of an example report.

control, the reporter might decide to assign either a new event (4010203) into the event chain or assign a new descriptive factor (24010500) to an existing event type, or both. Whenever existing safety events where the provision of ANS weather information was a factor need to be found, the respective query has to search the event type, the descriptive factor, and the combination thereof to be sure of correctly locating all such occurrences.

B. ECCAIRS Taxonomy Aspects

1. ECCAIRS Term Ambiguity

Many terms lack definitions. One such term is, for example, the descriptive factor 42030000 "Aerodrome/heliport hazard warning/notification," which might be interpreted as a warning being correctly issued, a warning being wrongly issued, or even a problem with warning functionality. Using different meanings for one term in two reports limits the future-occurrence search relevance.

2. ECCAIRS Term Names not Unified

Similarly, some terms do not follow the same naming policy, making it difficult to find them using the full-text search. For example, the word airspace is typed differently in event 4040000 "Airspace management-related event," descriptive factor 24030000 "AirSpace management's provision of service," and descriptive factor 4070400 "Air space capacity reduction."

3. ECCAIRS Taxonomy Ambiguity

The hierarchy in ADREP taxonomies is used for representing different meanings. For example, descriptive factor 100000018 "Door system wiring (ATA Code:5297)" is a subterm of 11520000 "Fuselage doors (ATA Code:5200)," representing a part-of relation between an object (door) and its part (wiring). On the other hand, 5010101 "Instrument landing-system-related event" is a subterm of 5010100 "Aerodrome approach systems-related event," representing an "is-a" relation between an event (approach system related) and a specific event (instrument landing system related).

IV. Ontological Modeling

The fundamental contribution of this paper lies in the ontological model for aviation safety. The key difference with a taxonomy is that an ontology describes the meaning of the terms used in the data model in terms of existing top-level ontologies, uses a rich set of relationship types (whereas taxonomy only provides one relationship), and (in order to be processable automatically) binds terms together by means of various logical axioms.

A. Simple Example

For example, using the ECCAIRS Taxonomy, one could create the data structure depicted in Fig. 2. Interpretation of its nodes is ambiguous (e.g., *Aircraft* mixes information about an enduring object with information about the object's participation in a given occurrence. The former is represented (for example) by attributes 232 "Propulsion type" or 32 "Aircraft category," whereas the latter is represented by attribute 292 "Airspeed," denoting the actual air speed during occurrence. A proper ontological analysis of the occurrence underlying Fig. 2 would need to distinguish, for example, the following:

1. Entities Changing in Time

Entities changing in time, or "endurants," can be like an aerodrome (LKPR), an aircraft (unknown serial number), a vehicle, a runway, or an approach procedure.

2. Entities Not Changing in Time

Entities not changing in time, or "perdurants," can be like an observation made by the reporter (occurrence), a flight, a flight phase (approach), or events (runway incursion, missed approach, or correct use of missed approach procedure).

3. Nature of Their Mutual Relationships

The nature of their mutual relationships can be like when an aircraft participates in the missed approach event. If needed, detailed information about the nature of the participation is also used (for example, an aircraft might participate in a runway incursion event in two roles, e.g., taxiing aircraft on ground or an approaching aircraft). Other examples of relationships involve that correct use of the missed approach procedure caused the missed approach or that the approach (flight phase) was part of the flight, etc.

4. Nature of Endurants

The nature of the endurants can be like when both the aircraft and the vehicle are physical objects used for transportation, and thus can move at some time instant with some speed. Thus, the property speed is related to some participation of a transportation object in an event. Another example is that the runway is a physical part of the aerodrome, and thus shares its spatial location. In this case, the runway is part of the aerodrome continuously (across multiple events).

This example only shows what sort of analysis proper ontological engineering can do. The notions of endurants, perdurants, events, participations, etc., are taken from the Unified Foundational Ontology (UFO) [28] (see Sec. IV.C), but similar notions exist in other top-level ontologies as well. Let us go deeper and introduce basic notions of ontologies in more detail.

B. Ontological Background

The Information Technology perspective of ontology as a philosophical discipline has already been studied for a few decades. The best known definition of ontology has been provided by Gruber [29], and further extended by Studer et al. in [30], as follows:

An ontology is a formal, explicit specification of a shared conceptualization.

Although revised many times (e.g., [31]) since its publication, the crucial points remain. An ontology 1) is explicit, i.e., declarative knowledge that is easily updatable and not a precompiled computational artifact; 2) is formal, i.e., machine processable with well-founded (typically logic-based) semantics; 3) is shared, i.e., it should capture the common understanding of the domain; and 4) is a conceptualization, i.e., a definition of meanings and not only of terms describing these meanings.

A knowledge structure with these properties, known as an ontology, can be used for knowledge sharing among experts, often using a software application.

For building a knowledge structure with these properties, different methodologies covering various parts of ontology design, evaluation, or maintenance exist. The portfolio of methodologies ranges from standard heavyweight bottom-up techniques, like Methontology [31] or the DILIGENT methodology [31], over agile methods [32] to collaborative ontology engineering methods [33]. Our approach is similar to the agile ontology engineering method introduced in [32], building the ontological knowledge bottom-up and identifying fundamental domain concepts under the supervision of a top-level ontology. Before introducing details on aviation ontology design in Sec. V, we review the fundamental instruments that we use in ontology design.

C. Unified Foundational Ontology

Starting with a discussion of top-level ontologies, a top-level ontology (or upper-level ontology) describes general concepts that are common to multiple domains. Many top-level ontologies have been developed during the past decades, involving descriptive ontology for linguistic and cognitive Engineering [34], basic formal ontology [35], suggested upper merged ontology [36], and many others [31].

1. Unified Foundational Ontology Basics

Our ontological analysis of the ECCAIRS is based on a recent approach that integrates ideas from multiple top-level ontologies into a single coherent top-level ontology, as introduced by Guizzardi in [28]. His proposal involved a unified foundational ontology as well as OntoUML,

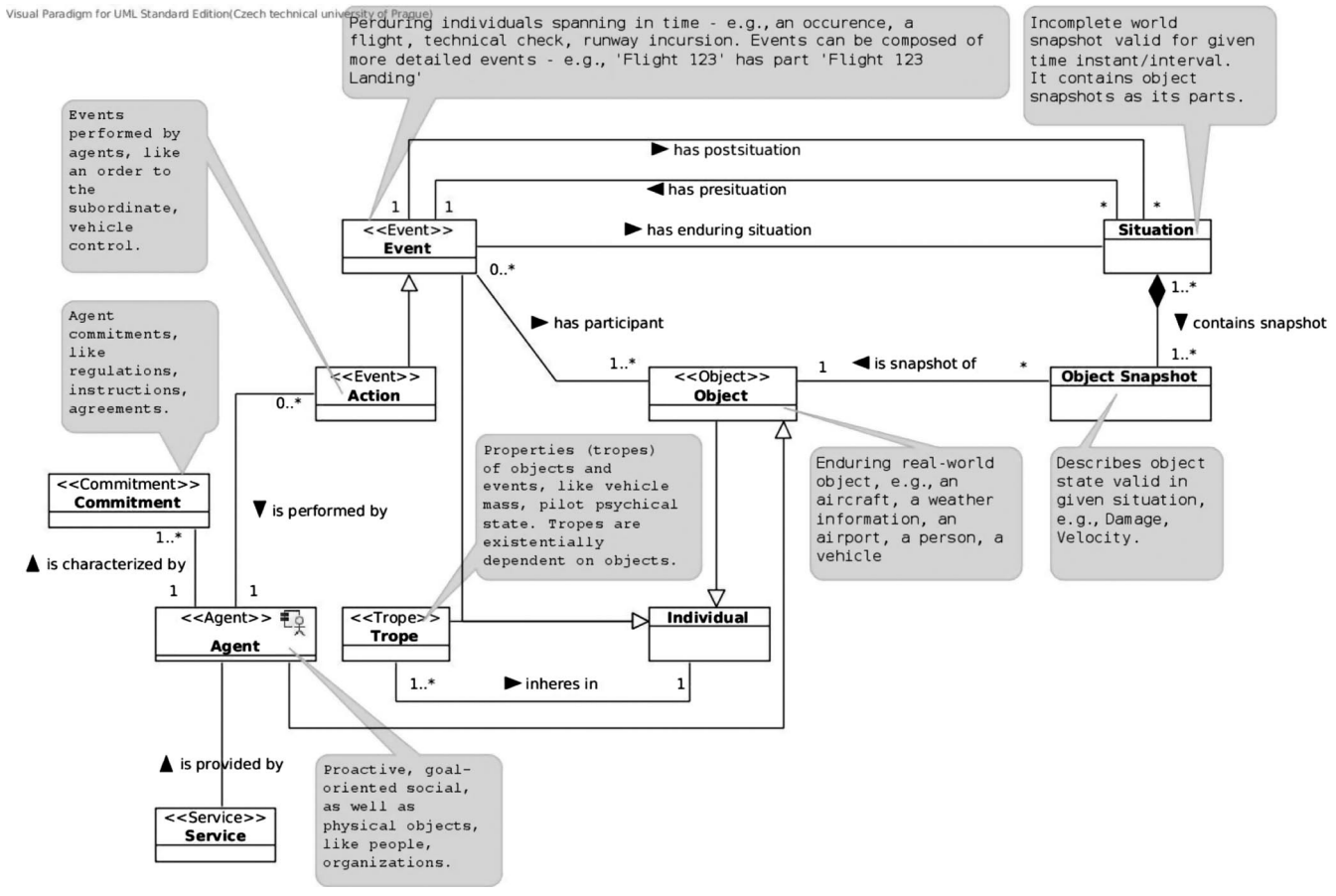


Fig. 3 Fundamental concepts and relations of UFO.

which is an ontology modeling language. The main parts of the UFO ontology that are fundamental for the purpose of this paper are depicted in Fig. 3.

UFO is built from several components, described in detail in [28–39]. It introduces several fundamental ontological categories, like individuals (e.g., a single particular aircraft) and universals (e.g., an aircraft type), representing sets of individuals. The next fundamental distinction on individuals is between endurants (e.g., an aircraft with properties fixed over the time, like category, serial number, etc.) and perdurants (e.g., an aircraft with properties for a particular time instant, like maximum speed during one particular flight). Endurants can be observed as complete concepts in a given time snapshot, whereas perdurants only partially exist in a given time snapshot. Endurants can be objects (an aircraft) or its tropes (e.g., a length of an aircraft) that exist as long as an object they inhere in exists. That is, the length of an aircraft cannot exist without the aircraft itself.

The next part of the UFO introduces the notion of an event, a perdurant, spanning some time interval or occurring in a time instant and having participants and parts (subevents). The events themselves can be temporally related (i.e. one happening before another, during another, etc.), as specified by Allen's temporal algebra [40]. A situation, on the other hand, can be understood as a bag of snapshots of object states and their relationship at one particular instant in time. Consequently, an event has its presituation (composed of object snapshots valid just before the event started) and a postsituation (composed of object snapshots valid just after the event ended). Such a framework is suitable for representing temporal and causal relationships between events, as well as for simulation scenarios [37].

Additionally, UFO introduces the notion of agents (i.e., proactive objects with an intention, e.g., a person or a company), their intentions, the commitments and actions they perform, and services.

The top-level ontology UFO is can be understood as a "high-level model of the world," i.e., it is applicable to multiple domains. To design the ontology, we also needed a modeling language to formalize our aviation safety concepts with respect to UFO. Fortunately, UFO comes with one: the OntoUML language.

2. *OntoUML*

OntoUML is a language provided on top of UFO for the purpose of conceptual modeling. The language was introduced in [28], is built on top of the Unified Modeling Language (UML) Version 2.0 [41], and refines it to allow proper ontological analysis. The UFO constructs are included into the UML mainly in the form of class/association stereotypes defining proper ontological semantics to the corresponding classes/associations. Here, we only review the most important constructs necessary for the purpose of this paper.

a. Sortal vs Mixin. A sortal is any universal carrying a principle of identity [e.g., *Aircraft* universal (identifiable by serial number)], which is contrary to a mixin universal (e.g., *Object* universal having different principles of identity given by its subtypes: person, car, aircraft, etc.).

b. Rigid vs Antirigid. Rigid is any universal for which all its instances (individuals) belong to the universal for the whole time of their existence, e. g., *Person* sortal universal. Antirigid universal is any universal for which all its instances will not be in the future or were not in the past instances of the universal, e.g., *Airborne aircraft* sortal universal.

c. Kinds and Subkinds. A kind is any rigid sortal that provides a principle of identity (e.g., *Person* kind) contrary to a subkind, of which any rigid sortal principle of identity is inherited from its ancestor kind, e.g., *Man* subkind inherits its identity from the *Person* kind.

d. Role Sortals. Role sortals are antirigid sortals for which the relation with another individual makes the particular individual an instance of that antirigid sortal, e.g., being a military aircraft depends on the type of operation for which the aircraft is registered.

e. Relators. A relator reifies a relation among several individuals, e.g., *Flight* (as a relation between a passenger, an aircraft, a company, etc., existing during the *Flight* event in a given timeframe).

f. Power Types. A power type is a type of types introduced and analyzed in [42] used for product-type modeling (like aircraft category) or social role modeling (like air traffic controller type).

Using OntoUML, the designer ends up with a properly designed model that helps in sharing the meaning of domain terminology among people. To make it interpretable by a computer, one needs to equip the designed ontology with the declarative semantics. For this purpose, we use a semantic Web standard Web Ontology Language (OWL 2) [43], which is a description logic-based [44] declarative calculus.

D. Formal Ontologies

Formalization of ontologies is needed for their use by software applications, including automated reasoning. Currently, the Web ontology language OWL 2 is considered a standard for representing formal ontologies on the Web. Together with the related technologies of the Semantic Web Rule Language (SWRL) [45] and expressive ontology queries like SPARQL [46], OWL 2 offers a powerful and semantically well-founded language for representing ontologies.

Specifically, OWL 2-DL, which is a decidable subset of OWL 2, is often used. OWL 2-DL is a syntactic variant of an expressive description logic that is, in turn, a fragment of first-order predicate calculus. OWL 2-DL ontologies accept a so-called open-world assumption, stating that everything is considered to be possible unless a negative statement is known. This makes OWL 2-DL an ideal choice for representing ontological knowledge in a distributed world.

In our case, the open-world assumption allows easy integration of the aviation ontology with existing, as well as newly emerging, ontologies in other domains. The aviation ontology described next was designed using OntoUML and translated into OWL 2 using a simple transformation defined in [47].

V. Aviation Ontology

The ECCAIRS data model and taxonomy flaws mentioned in Sec. III make the safety reporting process tedious and error prone. The aspects mentioned in Secs. III.A.1 and III.B.2 make it difficult for the reporter to find all relevant categories, thus resulting in incomplete reports. Additionally, aspects mentioned in Secs. III.A.2 and III.B.1 make resulting reports difficult to interpret.

To support search and exploration scenarios, we started to investigate ontological foundations of events and factors, as defined by the ECCAIRS and other aviation taxonomies, as shown in Sec. II.

Putting these ideas into the language of ontological engineering [31], the scope of the ontology can be delimited as safety occurrence modeling in aviation. The described problems also motivated the construction of competency questions that defined expectations of ontology users (reporters, safety managers, and safety officers of aviation organizations):

Q1) What are the parts of an aircraft?
Q2) Which people necessarily participate in a particular event (e.g., a runway incursion)?
Q3) Which safety events happen at the runway?
Q4) What comprises the condition of an aerodrome surface area?
Q5) Which safety events happen during a particular flight phase (e.g., takeoff)?
Q6) Which safety events have air traffic controller/pilot/ground service personnel as their participants?

These competency questions show two basic use cases for the ontology regarding the aviation occurrence investigation and reporting: get all the events with some properties (Q3, Q5, and Q6), get the properties of an event (Q2), or object (Q1 and Q4). The questions have been designed based on the ECCAIRS reporting scenario. Domain experts analyzed public investigation reports of the Czech Air Accidents Investigation Institute [48] and tried to model them using the ECCAIRS. During the reporting process, they logged the obstacles during the ECCAIRS taxonomies exploration that resulted in the competency questions. For example, after creating an occurrence (entity 24 "Occurrence") and filling in information about an aircraft (entity 4 "Entity") and the phase it was in during the occurrence (attribute 121 "Flight phase"), a reporter wanted to assign events to the aircraft according to the ECCAIRS model. He was offered a full list of event types (approximately 700) by the ECCAIRS system. Thus, he provided the reporting context and formulated competency question Q5. It ensured that the reporter received a filtered list of event types relevant to the actual flight phase (e.g., runway excursion event type cannot happen during an approach phase). More information about the scenario is discussed in Sec. VIII.

Aviation ontology details are presented in the appendices in order to not drive the reader's attention away from the ECCAIRS at this point. Please refer to the appendices for more detailed description of the aviation ontology while reading the following sections.

A. ECCAIRS Mapping

Based on the aviation ontology, we decomposed the ECCAIRS data model and taxonomies and restructured them using the generic ontological categories as exemplified in the next sections.

1. *ECCAIRS Entities and Attributes*

Modeling of the general structure of the ECCAIRS in terms of aviation ontology is rather straightforward. The ECCAIRS data model consists of several interconnected entities (e.g. aerodrome, aircraft, air traffic services unit, etc.) consisting of various attributes. Basically, most entities describe objects (e.g., an aircraft) but contain attributes of different levels of object identification:

1) The first level includes immutable object tropes, like aircraft make or ATS unit name. The values of these attributes do not change over the lifespan of the object.

2) The second level includes mutable object tropes, like aircraft speed or number of sectors opened in the ATS unit. The values of these attributes change over the lifespan of the object, and they relate to the particular participation of the object in the event.

3) The third level includes the tropes of an object part, like heads-up display installed for an aircraft or short-term conflict alert active for an ATS unit. In the former case, the display is a part of an aircraft and the heads-up installation position is a trope of the display. In the latter case, the short-term conflict alert is a function of an ATS unit. The "function being active" is a trope of the short-term conflict alert function.

2. *ECCAIRS Events*

Events, as used in the ECCAIRS, have a narrower meaning than those of UFO. The former can be understood as UFO events with some safety impact. To capture this distinction, a new class, *SafetyEvent*, which is a subclass of UFO *Event*, has been defined to capture the ECCAIRS meaning.

An example of the ECCAIRS event taxonomy restructuring can be seen on the taxonomy rooted in node 2200000 "Incursions generally." This node contains 12 bottom-level descendants (e.g., 2200101 "Runway incursion by an aircraft"). Two pieces of information are described in these categories: 1) where the incursion took place (runway/taxiway/apron), and 2) who made the incursion (aircraft/vehicle/person/animal).

These two pieces of information are hidden in the textual description of the event type and are not bound in any way to the ECCAIRS representation of respective entities (e.g., runway, aircraft, vehicle). Using aviation ontology, all types of incursion are captured as OWL axioms of the following form:

```
Safety_event
  and Incorrect_presence
  and has_location some ***
  and is_performed_by some ***
```

where $***$ denotes the particular parameter. Thus, aviation ontology only needs to replace four valid options for entities (aircraft, person, vehicle, animal), as well as three valid option locations (runway, taxiway, and apron) to cover 12 possible event types in the ECCAIRS (all possible combinations of entities and locations). Another example shows various parts of information that are often present in the ECCAIRS event types: ECCAIRS event 2020505 "Take-Off Clearance Deviation" can be modeled in terms of the aviation ontology as follows:

```
Safety_event
  and Regulation_violation
  and is_violation_of some Takeoff_clearance
  and is_performed_by some Flight_crew
  and has_location some Aerodrome
  and is_part_of some Flight
```

Such formal descriptions of the ECCAIRS events using the aviation ontology together with the definition of the aviation ontology itself as introduced in the appendices are used during the ECCAIRS category search by means of the expressive ontological query evaluation presented in Sec. VI.

3. *ECCAIRS Descriptive and Explanatory Factors*

The notion of a factor is used very frequently in safety reports, as well as in investigation reports of safety incidents. Examples of factors include 12141500 "Taxi speed," 100000021 "Use of the towing system," or 11210000 "Air conditioning system (ATA Code:2100)." Looking at the

ontological nature of these terms, the first denotes a value of a trope (speed) of an object (aircraft) during an event (taxiing), the second an event (using) and its participant (towing system), and the latter just an object snapshot (air-conditioning system).

An analysis of the ECCAIRS descriptive and explanatory factors revealed that these examples were typical: factors denote objects (or object snapshots), tropes (or trope values), or events. To unify the event description, we define the notion of a context event as an event spanning the time during which object snapshot/trope values do not change.

An adequate way to model the notion of a factor is through a relation *has factor* between an event and another context event. For example, although *Unstabilized approach* (a context event) is not a factor on its own, a particular *Runway excursion* (an event) might have the previous *Unstabilized approach* as its factor. In this sense, the *has factor* relation is a form of causal relationship between events. Whenever event A has event B as its factor, it is the case that event B partially causes (and thus starts before) event A.

Thus, the ECCAIRS descriptive factors, as well as explanatory factors, can be understood as types of context events that happen to be the typical factors of a safety event. This simplifies and unifies the description of safety events, avoiding the ECCAIRS data model ambiguity described in Sec. III.A.2.

As an example, let us take the formal definition of several factors showing up their different natures. The descriptive factor 42140100 "Vehicle/equipment speed" is described using the aviation ontology as follows:

```
Speed and inheres_in some Vehicle
```

Ontologically, this descriptive factor is a trope (speed) that inheres in an object (vehicle) or, more precisely, its value at some given situation (object temporal snapshots). Whenever the descriptive factor is a factor of a safety event, ontologically, it means that there exists a context event related to the vehicle speed (e.g., the car was moving too fast) that preceded the safety event and was one of its causes.

Other ontological entities that can be found in the ECCAIRS descriptive factors are objects. For example, the descriptive factor

```
Ramp_service_vehicle and Towing_and_parking_device
  and is_used_for some (Towing and has_location some Aerodrome)
  and is_operated_by some Ramp_service_agent
```

The vehicle is related to an operation it is used for (towing) and who operates the vehicle (ramp service agent).

The ECCAIRS descriptive and explanatory factors also involve events (in the ontological sense). For example, 27020000 "Air traffic control team briefing" is described as follows:

```
Briefing
  and has_location some Operations_room
  and has_participant some Air_traffic_controller
  and has_participant min 2
```

The descriptive factor denotes an event (briefing) and its participants (air traffic controllers).

4. *ECCAIRS Occurrence Categories*

Occurrence categories are event types in the ontological sense. Their instances have temporal and spatial extent. As an example, let us take the occurrence category 102 "Collision with obstacle(s), during take-off or landing whilst airborne." This category has its ontological representation as follows:

```
Safety_event
  and has_participant some (Obstacle and Ground_object)
  and has_participant some (Aircraft and Airborne_object)
  and during some (Landing or Takeoff)
```

The description captures the participants of the collision (an airborne aircraft and a ground obstacle). Furthermore, it says that the safety event occurred during a landing or takeoff.

5. *Summary*

Considering the ECCAIRS taxonomies that contain almost 5000 terms and our aviation ontology that contains approximately 1500 terms, we claim that the vocabulary simplification and disambiguation are significant. This directly improves data quality (as the reporter has fewer options to select, and thus is less prone to errors and misuse). Additionally, proper ontological distinctions lower syntactic overhead of the ECCAIRS descriptions. For example, event type 4010203 "Provision of ANS weather information" and descriptive factor 24010500 "Air traffic control provision of weather information" are modeled in the ontology as the same events:

```
Provision
  and is_provision_of some Weather_information
  and is_performed_by some Air_traffic_controller
```

In this way, both ECCAIRS event types provide the same contribution to the safety data and influence subsequent analysis in the same way.

The example formal descriptions mentioned in this section show how the ontological knowledge can be used as follows:

1) The ontological knowledge can be used to generate an event-specific form for high-quality data acquisition. Considering the runway incursion event type, the relevant data to be gathered include the location at which the object was incorrectly placed (e.g., incorrect presence) and identification of the object (vehicle or aircraft or person) causing the incursion

2) The ontological knowledge can be used to recognize an event type, considering any event for which the location is on the runway and having a vehicle as a participant; it is possible to suggest the runway incursion as an event type.

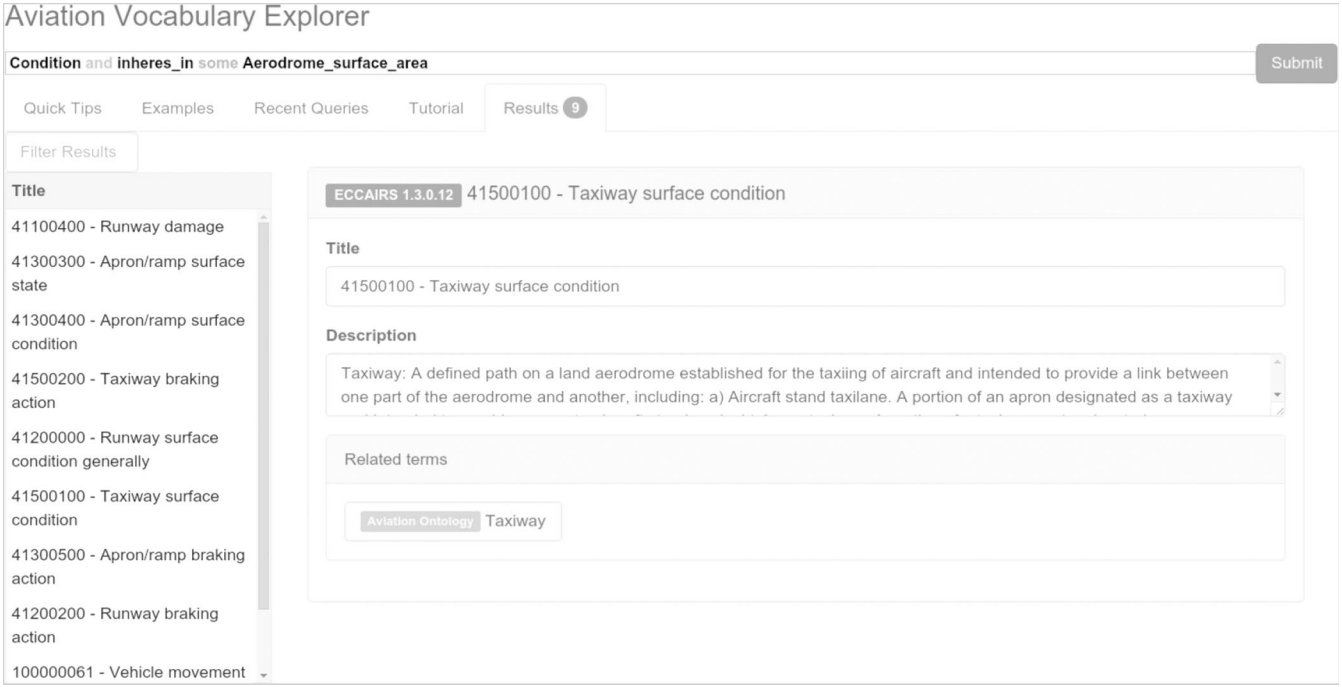


Fig. 4 Example of search results in the Aviation Vocabulary Explorer.

VI. Aviation Vocabulary Explorer

To explore capabilities of the aviation ontology, we developed an Aviation Vocabulary Explorer, see Fig. 4. The tool is a Web application, available on the INBAS project portal [49] and allowing us to look up terms from the ECCAIRS taxonomies, the ATM Lexicon, as well as the ICAO vocabulary based on a structured query posed in the aviation ontology.

The application is a rewritten version of the OntoQuery engine [50]. The queries have the form of OWL-class descriptions in Manchester syntax. Several query examples involve the following:

1) `Collision and has_participant some Airborne_object` looks up all collisions (events) in which airborne objects participate (e.g., airborne aircraft, birds, etc.). Evaluating this query with respect to ECCAIRS 3.4.0.2 results in 11 results: an ECCAIRS occurrence category 102 (see Sec. V.A.4), as well as 10 ECCAIRS event types of 2050101, 2050102, 2050200, 2050201, 2050202, 2050300, 2050301, 2050302, 2050303, and 2050304. For example, the latest event type is 2050304 "Aircraft collision with parachutist in the air."

2) `Object and is_part_of some Aerodrome` fetches all objects that are part of an aerodrome. Evaluating this query with respect to ECCAIRS 3.4.0.2 results in 149 results, with all of them being ECCAIRS descriptive factors: for example, 100000062 "Blast fence."

3) `Condition and inheres_in some Aerodrome_surface_area` fetches all types of condition (tropes) that inhere in an aerodrome surface area. This query returns nine results for ECCAIRS 3.4.0.2: 100000061, 41100400, 41200000, 41200200, 41300300, 41300400, 41300500, 41500100, and 41500200. For example, the latest descriptive factor is 41500100 "Taxiway surface condition."

VII. Evaluation

Due to the size of the ECCAIRS, the ontology has been evaluated only partially. Basically, two evaluations have been performed. First, we wanted to find out whether the ontology was expressive enough to model most frequent safety issues and event types. To obtain these, we took safety issues identified by the EASA in the "European Aviation Safety Plan 2013–2016" [51]. Safety issues can be modeled as occurrence categories in the ECCAIRS. In addition to the most frequent safety issues, we also successfully reconstructed models of all 36 ECCAIRS occurrence categories. A few ontological models of ECCAIRS occurrence categories are shown in Table 2.

Gradually, each query in the table can be decomposed to more atomic terms, e.g., `Ground_operation` can be modeled as an `Operation and has_location some Ground`, depending on how the reporter is familiar with the vocabulary.

Similarly, we evaluated whether the ontology is expressive enough to model the ECCAIRS event types. Due to the huge amount of ECCAIRS event types (there are more than 700 of them), we were not able to reconstruct all of them. Instead, we took those ECCAIRS event types that are frequently present in the aviation Czech investigation reports[¶] mentioned in Sec. V. These involve `Bird strike`, `Loss of Separation`, and `Deviation from Air Traffic Control Clearance`. Details on event type models are listed online at the Aviation Vocabulary Explorer page[**] as predefined queries to the explorer.

Although the previous evaluation was done in-house, for the second evaluation, we involved experts from the Air Navigation Services of the Czech Republic. We wanted to find out whether the competency questions were correctly answered by the ontology. The evaluation was performed by means of the Aviation Vocabulary Explorer tool. Experts were asked to go through the competency questions formalized as ontological queries and to validate the results. Although the experts found the results always correct, they found them incomplete in some cases. The correctness was a result of the ontological modeling (comparing to statistical analysis). The incompleteness was caused by missing constraints in the ontology (e.g., the location of an event type was not defined), which were easy to fill, and partly by the fact that the ontology was designed to have only a limited number of aviation safety vocabularies as an input (ADREP/ECCAIRS, ATM Lexicon, HFACS, and HEIDI). This experience also showed that testing completeness was difficult, namely, in such large knowledge structures as the ECCAIRS.

[¶]Data available online at http://www.uzpln.cz/en/ln_incident [retrieved 29 March 2017].

[**]Data available online at https://www.inbas.cz/aviation-vocabulary-explorer [retrieved 29 March 2017].

Table 2 Selected occurrence category modeling

ECCAIRS occurrence category	Ontological query to fetch the ECCAIRS occurrence category
Runway excursion	`Incorrect_presence and has_location some Runway and is_performed_by some Aircraft`
Midair collision	`Collision and has_location some Airspace and has_participant some Aircraft`
Controlled flight into terrain	`Event and has_participant some Aircraft and is_performed_by some Flight_crew`
Loss of control in flight	`Event and is_part_of some Flight and has_location some Airspace`
Runway incursion	`Incorrect_presence and has_location some Runway`
Safety of ground operations	`Event and is_part of some Ground_operation`

Next, the experts were asked to construct new queries. This part took much longer than expected (several weeks compared to the expectation of several days). The reason was the query language. Although providing many query examples, and although the Manchester query syntax was limited to two OWL class constructs only [the existential restriction (keyword `some`) and conjunction (keyword `and`)], the language turned out to be difficult for domain experts. For example, the distinction between `Event and has_participant some (Aircraft and Person)` and `Event and has_participant some Aircraft and has_participant some Person)` was difficult to grasp. The former expression describes an event that has an aircraft (which is a person at the same time) as a participant. The latter expression describes an event that has an aircraft as well as a person as its participants. The former query necessarily gives empty results, which was misunderstood by the evaluating experts. Although the experts were able to get familiar with the syntax within a few weeks, it was clear that special attention had to be paid to the query language. This problem will be dealt with in our next work.

One more requirement was identified during evaluation: the distinction between the necessary knowledge and the possible knowledge. For example, the runway incursion event necessarily has at least one participant that is located on the runway. On the other hand, other properties about runway incursion cannot be extracted from the event type itself because they are specific for each particular event. This involves particular factors causing the event (e.g., wrong clearance issued by air traffic control or deviation of clearance by pilot). The aviation ontology only focuses on a formal description of those resultant and regularity properties of events, objects, and tropes that can be extracted directly from the particular object/trope/event type.

VIII. Conclusions

This paper introduced an ontology describing typical safety occurrences, their factors, participants, and temporal and location characteristics, based on the analysis of existing aviation taxonomies (with the focus on the ECCAIRS). One of its uses is the following scenario: based on the formal description of the event characteristic (its location, temporal characteristics, participants, and their tropes), a set of matching event types can be offered to the safety occurrence reporter. This scenario is shown in the description of The Aviation Vocabulary Explorer in Sec. VI.

But, the opposite direction can be used as well. An event type prescribes its possible participants, time, and location characteristics that can be offered to the user in order to fill the preliminary occurrence report or the investigation report. For example, a runway incursion prescribes its location (runway border/protected area), participants (a vehicle, person, or an aircraft), as well as flight phase in case the participant was an aircraft (taxiing, landing, or takeoff).

Within the INBAS project, a solution, combining both approaches, is being worked on that represents the current vision for safety occurrence reporting and investigation. First, the reporter writes an occurrence narrative. Next, the description is analyzed and relevant ontology categories are automatically extracted. Based on the extracted categories (e.g., Prague airport, Flight OK123, air traffic controller, left wing, etc.), an ontological query is constructed (e.g., schematically) as follows:

```
Event and has_participant value Prague_airport
  and during value OK123
  and has_participant some Air_traffic_controller
  and has_participant some Left_wing,
```

and a list of relevant partially matching event types is fetched (first scenario). Then, the user selects one or more event types, and a list of attributes that need to be reported for the event types will be generated (second scenario).

This overall scenario complements the two future research directions previously mentioned in Sec. VII: easy to use query language and representation of the possible knowledge. The aviation ontology is used within two national projects for catalyzing the report understandability between the aviation organizations themselves, as well as between the organizations and the Civil Aviation Authority of the Czech Republic.

Appendix A: Technical Systems and Agents

The appendices offer details on the aviation ontology description. The foundations of the aviation ontology are based on UFO; see Sec. IV.C.

References to technical systems appear in the ECCAIRS taxonomies frequently, including physical technical systems, like an aircraft, vehicle, or equipment, as well as software systems, like a radar data-processing system. Their ontological foundation is rather straightforward to capture using standard ontological categories of endurants and objects, as modeled using UFO-A, a subset of UFO describing endurants.

Another important construct (taken from UFO-C, a subset of UFO defining social relationships) is the construct of an *Agent*. Safety event classification requires describing participating agents, including organizations (authorities, airline operators, aerodrome companies, etc.), as well as particular people (air traffic controller, vehicle driver, pilot, etc.).

Fundamental parts of the interaction between technical systems, agents, and functions are depicted in Fig. A1. The dashed line denotes the general relationships from an example taken from the respective taxonomies, e.g., an air traffic controller (a role of a person) operates a headset (a piece of equipment) that provides a communication function for the air traffic controller. Each of the core classes, technical system and function, is specialized in respective taxonomies. Technical systems provide functions that are used by agents to achieve their goals. Technical systems can be composed of other technical systems.

Many technical system types, as well as the social roles of agents, have the nature of power types [42]. An example power type might be an aircraft category distinguishing physical and functional structures of an aircraft, like fixed wing, helicopter, glider, etc. A power type collects general information about the type itself, see Fig. A2 in terms of the following:

1) Resultant properties involve summary or statistical information about all instances of the particular type. For an aircraft category of power type, the number of registered aircraft might be an example of a resultant property, having different values for a fixed-wing aircraft type (i.e., number of all registered fixed-wing aircraft) and a helicopter type (i.e., number of all registered helicopters).

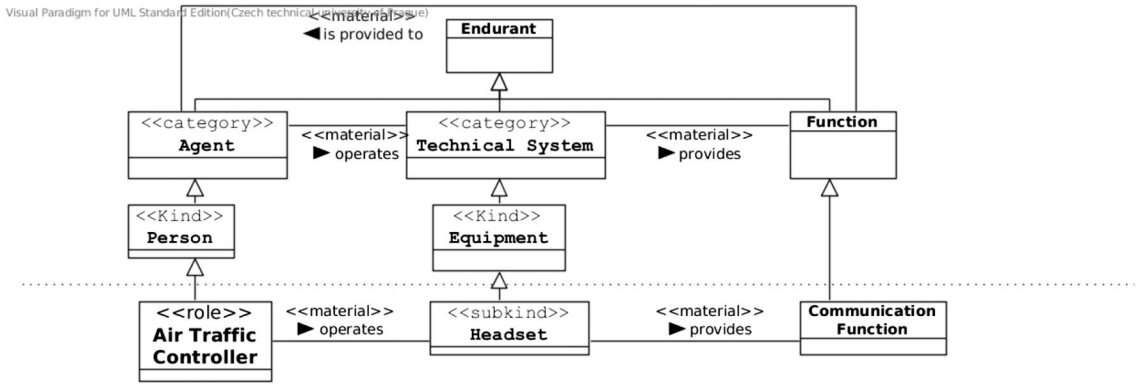


Fig. A1 Modeling of technical system types.

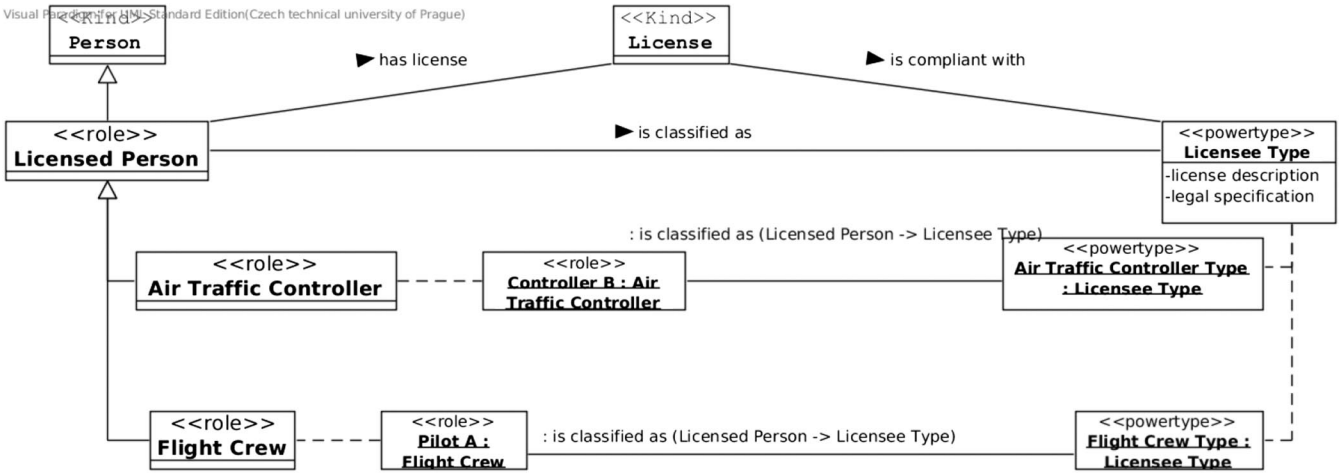


Fig. A2 Modeling of licensed person types.

2) Regularity properties involve the property of every single instance of the particular type. For an aircraft category of power type if the type of landing area, having a value of runway strip for a fixed-wing aircraft type (and thus for each particular fixed wing aircraft) and a value of heliport for a helicopter type (and thus for each particular helicopter).

3) Direct properties involve properties of the type itself, having no connection to the particular instances. For example, quadcopters were first created in the 1930s [52], giving rise to the quadcopter type at that time.

To capture agent commitments, stemming from the legislation in the aviation industry, the concept of service is heavily used in the domain. Examples include air traffic control service or ramp service. The concept of service is very broad, referring to various meanings, depending on context, e.g., an agent (person/organization who provides the service) or an agreement (a set of obligations/promises comprising the service).

Appendix B: Events

Events are fundamental and can be understood as the basic instrument for safety incident reconstruction and investigation. As the main input, we took events, descriptive factors, and explanatory factors from the ECCAIRS taxonomies and remodeled them using principles from UFO-B, a subset of UFO modeling events and situations. Events are perdurant entities that occur in time (i.e., with temporal extension). Let us describe prominent event types first, and then let us discuss relationships between events. The fundamental notions are depicted in Fig. B1. The dashed line denotes the general relationships from an example taken from the respective taxonomies. For example, a runway incursion is a safety event, *Use* is an action and *Takeoff* is part of some flight.

B1. Event Types

The concept of an event used in ECCAIRS has the meaning of a safety event, which is an event with safety impact. Typical examples include incorrect presence, which describes events during which an object is on another place than expected (like runway/taxiway/apron incursions, excursions, intrusion, unauthorized entry, etc.); collision or near collision (like aircraft/vehicle/equipment airborne/ground near/collision); regulation violation (like security events such as bomb threats, sabotage, jamming); or air traffic control instruction/clearance deviation, etc..

Events are decomposable into smaller events that are part of their parent. Typical examples include takeoff (or another flight stage) as a part of a flight (event), or hear-back as a part of some communication (event). Mereological relations on events are frequent and are typically well defined, as most processes in the aviation industry are defined by formal procedures.

Events can be actively performed by agents; such events are called actions. Examples of typical actions include *Use* (an agent uses some object to achieve its goals), *Provision* (an agent provides some service to another agent), or *Planning* (an agent plans some action).

B2. Event Relations

Another important part of an event description is its relation to other events. One of these relationships, *part-of relation*, was already described in Sec. VIII.B.1.

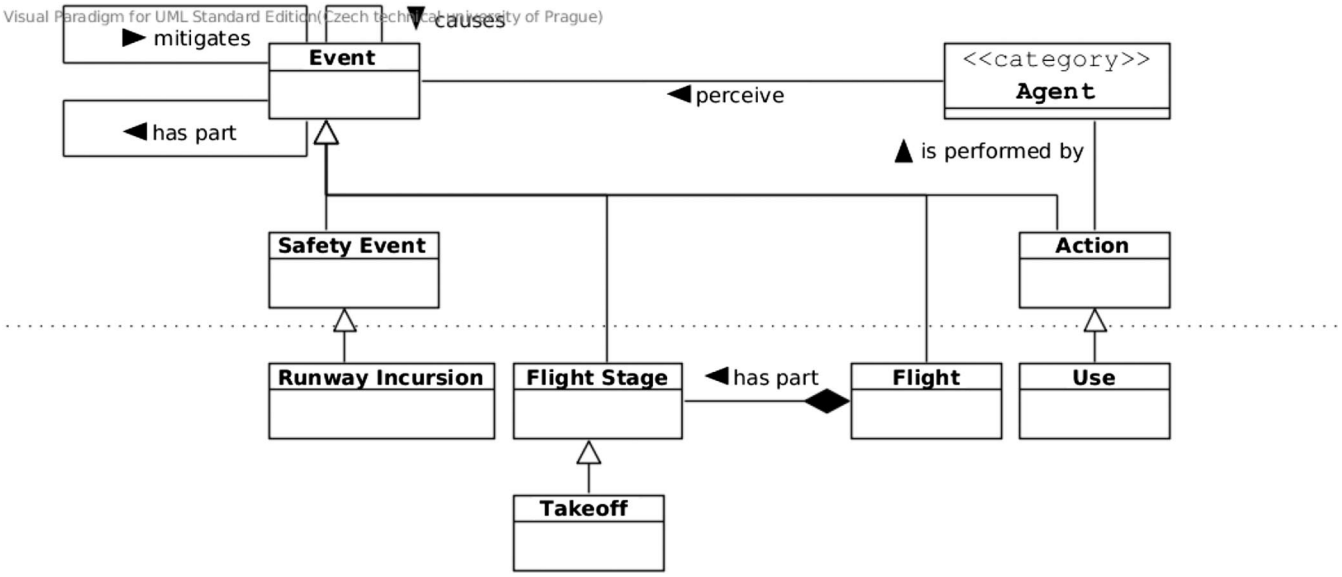


Fig. B1 Modeling of event types.

An important aspect is the causality of events. One event might cause another event (e.g., a deviation from air traffic control instruction might cause a runway incursion, or presence of a foreign object debris on a runway might cause a tire defect), or it might prevent another event to occur (e.g., a go-around/missed approach might prevent runway incursion from happening). The causality of events is a typical outcome of occurrence investigation.

Appendix C: Spatial and Temporal Characteristics

Fundamental information that is important for safety reporting includes spatial and temporal references. Events happen in some spatial region, during some time interval (or temporal entity in general). The spatial and temporal information is crucial and should be part of the occurrence report. In many cases, the particular type of event that occurred prescribes the spatial and temporal characteristics of the event.

For example, a runway incursion can only happen on an aerodrome at some runway border, loss of separation can only happen in an airspace, and a decompression always happens in an aircraft; wherever it is present at a given time, a hard landing is part of some particular flight, and thus is limited by the flight time span, etc.

C1. Temporal Characteristics

The temporal characteristic of an event can be defined absolutely, using standard ontological means for representation of time entities (time points and intervals) and their exact specification in terms of a time stamp/date.

From the perspective of safety occurrence analysis and investigation, it is often more useful to mutually relate events in time instead of providing absolute time stamp. For example, if there is a landing gear failure, the information that it happened during an approach is more relevant than stating that it happened at 1345 hrs. An ontologically well-founded proposal has been introduced by Allen [40]. Allen's algebra provides a complete set of temporal relations between time entities, like *overlaps*, *meets*, *during*, or *startsWith*. These basic temporal characteristics together with temporal relations are formalized, e.g., in the time ontology [53].

We introduced two constructs for relating events: the constructs of temporal relations and the constructs of *part-of* relations. It might be tempting to consider the temporal relation *during* as a special type of the *part-of* relation. Ontologically, the latter is a stronger notion; whenever an event is part of another, it also happens during the latter (e.g., a takeoff is part of a flight, and thus happens during it), but not vice versa (e.g., a landing gear failure might occur during an approach but is not its part).

C2. Spatial Characteristics

Spatial information has similar aspects to the temporal kind: absolute spatial locations of events are frequent in many cases, like for runway incursion or airspace infringement. In both cases, an exact location is relevant for safety analysis and easily obtained. On the other hand (e.g., in case of blocked communication), the location is related to the agents performing the communication, and the exact location (where the aircraft was) is less important than the information in which the aircraft was the blocked communication encountered.

There exists the dimensionally extended nine-intersection model [54] model aimed at representing spatial relations. A set of nine relations, like *contains* or *crosses*, is defined. Similarly to the time axis, the *part-of* relation is a stronger notion than the *contains* relation on spatial regions; whereas an aircraft could be contained in an airspace sector at given time, it is not part of the airspace region in the mereological sense. On the other hand, a runway is a (logical, physical and essential) part of an aerodrome. These basic spatial entities and their characteristics are formalized, e.g., in the WGS84 vocabulary [55].

Appendix D: Formalization

The previous sections showed the most important aspects of the designed aviation ontology. The ontology is formalized using the Web Ontology Language (OWL 2) and SWRL and is available online with a short description and documentation.[††] During formalization, we avoided nominals (an OWL construct to define an OWL class by enumeration) to keep the expressiveness of the ontology as low as $\mathcal{SHIQ}(\mathcal{D})$ in order to

[††]Data available online at http://www.inbas.cz/ontologie [retrieved 2017].

allow efficient reasoner optimizations [56]. The current version of the aviation ontology contains more than 1500 classes, more than 100 (object and data) properties, and approximately 18 SWRL rules.

As an example of OWL representation, let us show the formalization of the runway incursion event (using Manchester syntax [57]:

```
Safety_event
  and Incorrect_presence
  and has_location some Runway
  and is_performed_by some (Vehicle or Aircraft or Person)
```

This description describes the necessary knowledge related to the runway incursion, namely, its nature (incorrect presence), location restriction (runway), and type of performer (vehicle, aircraft, or person). Although runway, vehicle, aircraft, and person are terms well understood in the domain, incorrect presence is a generic event type that is domain independent and describes those events in which an object is present at some location it is not expected to be.

Acknowledgment

This work was supported by grant no. TA04030465 "Research and Development of Progressive Methods for Measuring Aviation Organizations Safety Performance" of the Technology Agency of the Czech Republic.

References

[1] *ECCAIRS Community Portal* [online database], http://eccairsportal.jrc.ec.europa.eu [retrieved 5 Nov. 2016].
[2] EuropeanAviationSafetyAgency, *Aviation Safety Reporting*, http://www.aviationreporting.eu/index.php?id=196 [retrieved 5 Nov. 2016].
[3] Stolzer, A. J., and Goglia, J. J., *Safety Management Systems in Aviation*, Taylor and Francis, Philadelphia, PA, 2016, p. 189.
[4] Stojić, S., Vittek, P., Plos, V., and Lališ, A., "Taxonomies and Their Role in the Aviation Safety Management Systems," *eXclusive e-JOURNAL*, No. 1, 2015, http://exclusiveejournal.sk/issue-1-2015.html [retrieved 29 March 2017].
[5] E-TOKAI Web Page, http://www.e-tokai.net [retrieved 5 Nov. 2016].
[6] HEIDI Taxonomy, 2004, http://www.eurocontrol.int/articles/esarr-2-reporting-and-assessment-safety-occurrences-atm [retrieved 10 July 2016].
[7] The Commercial Aviation Safety Team/ICAO Common Taxonomy Team (CICTT), http://www.intlaviationstandards.org/ [retrieved 30 Nov. 2016].
[8] ATM Lexicon, http://www.eurocontrol.int/lexicon/lexicon/en/index.php/Main_Page [retrieved 3 Aug. 2015].
[9] ICAO Glossary, http://www.intlaviationstandards.org/apex/f?p=240:1:15338757287208::NO::P1_X:Glossary [retrieved 3 Aug. 2015].
[10] Shappell, S. A., and Wiegmann, D. A., "*The Human Factors Analysis and Classification System–HFACS*," U.S. Dept. of Transportation, Federal Aviation Administration Final Rept. DOT/FAA/AM-00/7, Feb. 2000.
[11] ATA Specification 100-Specification for Manufacturers' Technical Data, Revision No. 37, Air Transport Association of America, 1999.
[12] "Federal Aviation Administration Joint Aircraft System/Component Code: Table and Definitions, Federal Aviation Administration," 27 Oct. 2008, http://av-info.faa.gov/sdrx/documents/JASC_Code.pdf [retrieved 27 Aug. 2015].
[13] Ast, M., Glas, M., and Roehm, T., "Creating an Ontology for Aircraft Design," *Deutscher Luft- und Raumfahrtkongress*, 2013, http://publikationen.dglr.de/?tx_dglrpublications_pi1%5Bdocument_id%5D=301356 [retrieved 29 March 2017].
[14] Valente, A., Russ, T., MacGregor, R., and Swartout, W., "Building and (Re)Using an Ontology of Air Campaign Planning," *IEEE Intelligent Systems*, Vol. 14, No. 1, Jan. 1999, pp. 27–36.
doi:10.1109/5254.747903
[15] Reiss, M., Moal, M., Barnard, Y., Ramu, J.-Ph., and Froger, A., "Using Ontologies to Conceptualize the Aeronautical Domain," *Proceedings of the International Conference on Human-Computer Interaction in Aeronautics*, 2006.
[16] Su, K.-W., Wang, H.-Y., Li, K.-J., Wang, C.-H., and Hsiao, P.-H., "Designing and Evaluating an Ontology-Based Air Traffic Control Digital Knowledge Learning System," *Proceedings of the International Conference on Human-Computer Interaction in Aeronautics*, Cépaduès-Editions, Toulouse, France, 2011, pp. 56–63.
[17] Abou Assali, A., Lenne, D., and Debray, B., "KoMIS: An Ontology-Based Knowledge Management System for Industrial Safety," *Proceedings of the 18th International Conference on Database and Expert Systems Applications, DEXA '07*, IEEE Computer Society, Washington, D.C., 2007, pp. 475–479.
[18] Guebitz, B., Schnedl, H., and Khinast, J. G., "A Risk Management Ontology for Quality-by-Design Based on a New Development Approach According GAMP 5.0," *Expert Systems with Applications*, Vol. 39, No. 8, June 2012, pp. 7291–7301.
doi:10.1016/j.eswa.2012.01.089
[19] Debray, B., Abou Assali, A., Pradaud, I., Vaudelin, J., and Lenne, D., "Knowledge Management for Industrial Safety, Generic Resource Platform Combined with an Ontology Based Approach," *International Symposium on Loss Prevention and Safety Promotionin the Process Industry*, Edimbourg, United Kingdom, May 2007, p. 8, https://www.researchgate.net/publication/278806601_Knowledge_management_for_industrial_safety_generic_resource_platform_combined_with_an_ontology_based_approach [accessed 29 March 2017].
[20] Lykourentzou, I., Papadaki, K., Kalliakmanis, A., Djaghloul, Y., Latour, T., Charalabis, I., and Kapetanios, E., "Ontology-Based Operational Risk Management," *13th IEEE Conference on Commerce and Enterprise Computing, CEC 2011*, edited by Hofreiter, B., Dubois, E., Lin, K.-J., Setzer, T., Godart, C., Proper, E., and Bodenstaff, L., IEEE Computer Society, Washington, D.C., Sept. 2011, pp. 153–160.
[21] Falbo, R. d. A., Ruy, F. B., Bertollo, G., and Togneri, D. F., "Learning How to Manage Risks Using Organizational Knowledge," *Proceedings of Advances in Learning Software Organizations, 6th International Workshop, LSO 2004*, edited by Holz, H., and Melnik, G., Vol. 3096, Lecture Notes in Computer Science, Springer, New York, 2004, pp. 7–18.
[22] Access to Air Safety Information, Oct. 2002, https://aviation-safety.net/pubs/asn/Access-ASI-paper.pdf [retrieved 29 March 2017].
[23] "Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the Reporting, Analysis and Follow-Up of Occurrences in Civil Aviation, Amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and Repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 Text with EEA Relevance," Council of the European Union "Regulation 376/2014," 3 April 2014, %http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0376 [retrieved 07 Feb. 2016].
[24] "Commission Implementing Regulation (EU) 2015/1018 of 29 June 2015 Laying Down a List Classifying Occurrences in Civil Aviation to be Mandatorily Reported According to Regulation (EU) No 376/2014 of the European Parliament and of the Council (Text with EEA Relevance)," Council of the European Union Regulation 2015/1018, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.163.01.0001.01.ENG [retrieved 7 Feb. 2016].
[25] *ICAO ADREP* [online database], SKYbrary, http://www.skybrary.aero/index.php/ICAO_ADREP [retrieved 5 Nov. 2016].
[26] *ECCAIRS Implementation* [online database], International Civil Aviation Organization, Bangkok, http://www2010.icao.int/SAM/SSP/Pages/ECCAIRS_Implementation.aspx [retrieved 5 Nov. 2016].
[27] ICAO ADREP, http://www.icao.int/safety/airnavigation/AIG/Documents [retrieved 3 Aug. 2015].
[28] Guizzardi, G., "Ontological Foundations for Structural Conceptual Models," Ph.D. Thesis, Univ. of Twente, Enschede, The Netherlands, Oct. 2005.
[29] Gruber, T. R., "A Translation Approach to Portable Ontology Specification," *Knowledge Acquisition*, Vol. 5, No. 2, 1993, pp. 199–220.
doi:10.1006/knac.1993.1008

[30] Studer, R., Benjamins, R. R., and Fensel, D., "Knowledge Engineering: Principles and Methods," *Data Knowledge Engineering*, Vol. 25, Nos. 1–2, 1998, pp. 161–197.
doi:10.1016/S0169-023X(97)00056-6
[31] Gomez-Perez, A., Fernandez-Lopez, M., and Corcho, O., *Ontological Engineering*, Springer, New York, 2005, p. 125.
[32] Auer, S., and Herre, H., "Rapid OWL—An Agile Knowledge Engineering Methodology," *Perspectives of System Informatics (PSI'06)*, edited by Virbitskaite, I., and Voronkov, A., Vol. 4378, Lecture Notes in Computer Science, Springer, Berlin, June 2006.
[33] Suárez-Figueroa, M. d. C., Gómez-Pérez, A., Motta, E., and Gangemi, A., (eds.), *Ontology Engineering in a Networked World*, Springer, New York, 2012, p. 9.
[34] Gangemi, A., Guarino, N., Masolo, C., Oltramari, A., and Schneider, L., "Sweetening Ontologies with DOLCE," *Proceedings of the 13th International Conference on Knowledge Engineering and Knowledge Management. Ontologies and the Semantic Web, EKAW '02*, Springer–Verlag, London, 2002, pp. 166–181.
[35] Grenon, P., and Smith, B., "SNAP and SPAN: Towards Dynamic Spatial Ontology," *Spatial Cognition and Computation*, Vol. 4, No. 1, 2004, pp. 69–104.
doi:10.1207/s15427633scc0401_5
[36] Niles, I., and Pease, A., "Toward a Standard Upper Ontology," *Proceedings of the 2nd International Conference on Formal Ontology in Information Systems (FOIS-2001)*, edited by Welty, C., and Smith, B., ACM, New York, 2001, pp. 2–9.
[37] Guizzardi, G., Wagner, G., Falbo, R. d. A., Guizzardi, R. S. S., and Almeida, J. P. A., *Towards Ontological Foundations for the Conceptual Modeling of Events*, Vol. 8217, Lecture Notes in Computer Science, edited by Ng, W., Storey, V. C., and Trujillo, J., Springer, New York, 2013, pp. 327–341.
[38] Green, P., and Rosemann, M., *Business Systems Analysis with Ontologies*, Idea Group Publishing, Hershey, PA, June 2005, p. 345.
[39] Nardi, J. C., Falbo, R. d. A., Almeida, J. P. A., Guizzardi, G., Pires, L. F., van Sinderen, M., and Guarino, N., "Towards a Commitment-Based Reference Ontology for Services," edited by Gasevic, D., Hatala, M., Motahari Nezhad, H. R., and Reichert, M., IEEE Computer Society, Washington, D.C., 2013, pp. 175–184.
[40] Allen, J. F., "Maintaining Knowledge About Temporal Intervals," *Communications of the ACM*, Vol. 26, No. 11, Nov. 1983, pp. 832–843.
doi:10.1145/182.358434
[41] Lano, K., *UML 2 Semantics and Applications*, Wiley, New York, 2009.
[42] Guizzardi, G., Paulo, J., Almeida, P. J., Guarino, N., and Carvalho, V. A., "Towards an Ontological Analysis of Powertypes," *Proceedings of the Joint Ontology Workshops 2015 Episode 1: The Argentine Winter of Ontology Co-Located with the 24th International Joint Conference on Artificial Intelligence (IJCAI)*, Buenos Aires, Argentina, July 2015, http://ceur-ws.org/Vol-1517/JOWO-15_FOfAI_paper_7.pdf.
[43] Motik, B., Patel-Schneider, P. F., and Parsia, B., "OWL 2 Web Ontology Language Structural Specification and Functional-Style Syntax," W3C Recommendation, Dec. 2012, https://www.w3.org/TR/owl2-syntax/ [retrieved 29 March 2017].
[44] Baader, F., Calvanese, D., McGuinness, D. L., Nardi, D., and Patel-Schneider, P. F., *The Description Logic Handbook: Theory, Implementation and Applications*, 2nd ed., Cambridge Univ. Press, New York, 2010.
[45] Horrocks, I., Patel-Schneider, P. F., Boley, H., Tabet, S., Grosof, B., and Dean, M., "SWRL: A Semantic Web Rule Language Combining OWL and RuleML," W3C Member Submission, World Wide Web Consortium, 2004, https://www.w3.org/Submission/SWRL [retrieved 29 March 2017].
[46] Kremen, P., and Kostov, B., "Expressive OWL Queries: Design, Evaluation, Visualization," *International Journal on Semantic Web and Information Systems*, Vol. 8, No. 4, Oct. 2012, pp. 57–79.
doi:10.4018/IJSWIS
[47] Barcelos, P. P. F., dos Santos, V. A., Silva, F. B., Monteiro, M. E., and Garcia, A. S., "An Automated Transformation from OntoUML to OWL and SWRL," *ONTOBRAS, CEUR Workshop Proceedings*, Vol. 1041, edited by Bax, M. P., Almeida, M. B., and Wassermann, R., CEUR-WS, 2013, pp. 130–141, CEUR-WS.org [retrieved 29 March 2017].
[48] *Czech Air Accidents Investigation Institute* [online database], http://www.uzpln.cz/en/ln_incident [retrieved 1 Feb. 2016].
[49] *INBAS Project* [online database], Technology Agency of the Czech Republic, Prague, http://www.inbas.cz [retrieved 1 Dec. 2016].
[50] *Chemical Entities of Biological Interest OntoQuery* [online database], https://www.ebi.ac.uk/chebi/tools/ontoquery [retrieved 27 Aug. 2015].
[51] "European Aviation Safety Plan 2013–2016," European Aviation Safety Agency Final Report, Cologne, Germany, https://www.easa.europa.eu/system/files/dfu/sms-docs-European-Aviation-Safety-Plan-(2013-2016)--v1.0-Final.pdf [retrieved 10 July 2016].
[52] "History of Quadcopters and Other Multirotors," Krossblade Aerospace Systems, Phoenix, AZ, http://www.krossblade.com/history-of-quadcopters-and-multirotors [retrieved 10 July 2016].
[53] Pan, F., and Hobbs, J., (eds.) "Time Ontology in OWL: W3C Working Draft," W3C, Cambridge, MA, 27 Sept. 2006, http://www.w3.org/TR/2006/WD-owl-time-20060927.
[54] Clementini, E., Di Felice, P., and van Oosterom, P., "A Small Set of Formal Topological Relationships Suitable for End-User Interaction," *Proceedings of the Third International Symposium on Advances in Spatial Databases, SSD '93*, Springer–Verlag, London, 1993, pp. 277–295.
[55] Brickley, D., "W3C Semantic Web Interest Group: Basic Geo (WGS845 Lat/Long) Vocabulary," edited by D. Brickley, 2006, W3C, Cambridge, MA, http://www.w3.org/2003/01/geo/ [retrieved 10 July 2016].
[56] Horrocks, I., and Sattler, U., "Decidability of $\mathcal{SHIQ}$ with Complex Role Inclusion Axioms," 2003.
[57] Horridge, M., *OWL 2 Web Ontology Language: Manchester Syntax*, 2nd ed., W3C, Cambridge, MA, 2012, http://www.w3.org/TR/owl2-manchester-syntax [retrieved 26 Aug. 2015].

K. M. Feigh
Associate Editor

Appendix G

VITTEK, Peter, Andrej LALIŠ, Slobodan STOJIĆ and Vladimír PLOS. Challenges of implementation and practical deployment of aviation safety knowledge management software. *Journal of Aerospace Information Systems*. 2017, 14(5), pp. 1-14. DOI: 10.1007/978-3-319-45880-9_24.

Challenges of implementation and practical deployment of aviation safety knowledge management software

Peter Vittek[1], Andrej Liš[2], Slobodan Stojić[3], and Vladimír Plos[4]

[1] Czech Technical University in Prague, Department of Air Transport, Horská 3, 128 03 Prague 2, Czech Republic
xvittek@fd.cvut.cz
[2] Czech Technical University in Prague, Department of Air Transport, Horská 3, 128 03 Prague 2, Czech Republic
lalisand@fd.cvut.cz
[3] Czech Technical University in Prague, Department of Air Transport, Horská 3, 128 03 Prague 2, Czech Republic
stojislo@fd.cvut.cz
[4] Czech Technical University in Prague, Department of Air Transport, Horská 3, 128 03 Prague 2, Czech Republic
plos@fd.cvut.cz

Abstract. This paper introduces practical issues of implementing and deploying safety knowledge management software to aviation safety. Domain specific intangible nature of the issues concerned is described and all factors which prevent successful application of any knowledge management system are documented. Aviation organizations are struggling to find any effective solution which would on one hand allow timely tracking of the dynamic knowledge and on the other to not limit or bias reporters or investigators within the knowledge gathering process. The article deals mainly with practical issues concerning the deployment of reporting software, which constitutes the interface between humans and ontology model behind the software, capable to address trade-offs between various conflicting design criteria as well as many aviation organization types, as the aviation safety knowledge is to be gathered in cooperation with the industry.

Keywords: aviation safety, reporting, knowledge management

1 Introduction

Aviation safety is currently the subject of many efforts and research activities. One of the aspects of these efforts is to formalize all available knowledge and to encourage common and harmonized process for keeping it up to date [1]. The knowledge is then to be used backwards within the industry for safety management or safety oversight activities, providing respective authorities with timely and adequate suggestions on what to do. Given the complexity of the

aviation industry, ever increasing safety standards as well as constant traffic growth, this process is a must and no single country or aviation organization can handle the issues completely on its own.

Because aviation became considerably globalized, the very same technology is being used all over the world. This entails not only more extensive experience with the technology itself, in terms of reliability and safety assessment, but also issues stemming from the cultural and maturity differences, especially as far as the intangible safety of aviation system components and human interactions is concerned. Typically, hardware issues are defined using sensory data which are easy to quantify and usually based on mathematical or physical equations, providing very little room for bias or uncertainty. Owing to this, nowadays hardware solutions have reached excellent degree of reliability [2] and certainly they are rarely considered as unsafe. On the other hand, human and component interactions are still quite easily capable of generating unacceptable level of risk [3], but despite the fact that human factors are still subjected to specific research[4], there are no sensory data available nor can they be effectively obtained.

All recent accidents and incidents in the aviation exhibit presence of contributory factors, which are hardly manageable; they are often difficult to define or track, creating much more room for bias and uncertainty and frequently leading to inadequate corrective measures or oversimplified solutions [5]. This is because authorities are for various reasons rather prone to fix the consequences than learn about the true causes, mostly because of the lack of knowledge needed and the demanding nature of the learning process.

Accordingly, the industry demands adequate software solutions, which would enable effective knowledge gathering, processing and sharing among multiple aviation organization types and authorities. The solutions have to ensure these mechanisms be harmonized so that the learning process can provide for all its stakeholders desired degree of understanding both the issues and how to effectively control them. This article will describe existing efforts in this domain as well as the approach being developed within research projects at Czech Technical University in Prague.

2 Aviation safety knowledge

Because the hardware technology and its individual components have reached satisfactory degree of safety and reliability, this chapter will deal only with the persisting issue of component interactions and human presence in the system.

From the standpoint of system theory and safety engineering, the interactions concerned need to be first identified within the hazard analysis, either when new system is being designed or when existing system is to be modified [5]. Aviation industry rules and regulations do not allow hazard analysis to be left out prior to the operations, so this scenario is omitted. In other words, hazards are typically well-known and should always be there appropriately documented. Each of the hazards must be mitigated by the means of applying suitable safety constraints to make sure that the process controlled will remain under control at all times.

Then, monitoring of the system, or more precisely controlled process, should allow for identification of any undesired behavior, usually utilizing safety key performance indicators [6]. Any violation of this designed safety control structure should be subjected to analysis to introduce adequate mitigation measures. Monitoring the system may also lead to identification of new hazards and subsequent modifications of the existing safety control structure.

Whilst from the standpoint of theory this is the best practice, dedicated systems are facing specific issues when being implemented and deployed. In the aviation, there are many different aviation organization types (such as airlines, flight schools, maintenance organizations, air navigation service providers etc.) which all operate within different part of the industry. Not only do they interact when it comes to the industry operations as a whole, but their internal safety control structures and technologies interact among themselves as well. Gathering information from all these interfaces, therefore, requires more than just interdepartmental cooperation; it is often about inter-organizational and international efforts.

To gather and track the interactions, individual interfaces must be monitored. Because the interfaces are mostly intangible, the only way how to achieve this is to observe them. In aviation, this typically requires someone to report anything he or she perceives as violation of the existing safety constraints, either originating directly from operational staff or indirectly from external or internal audits and occurrence investigation. In extreme cases, reporting may involve reporter's own mistakes or flawed actions. Depending on the way the information was achieved, these are called occurrence or investigation reports and audit findings. In some cases, semi-automated or automated processing is possible, but this is only in case where there is some hardware at least on one side of the interface.

Majority of the interfaces need to be observed so effective reporting forms are the key enabler towards the desired solutions. These must address the most common issue regarding any reporting forms: not to limit or bias the reporter in describing the occurrence or finding but, on the other hand, to guide him as much as possible to ensure highest quality of the data gathered. Processing and storing the data to knowledge management system database will then allow further decision-making about the system controlled. The more accurate the data stored, the better the mitigation measures.

3 Knowledge management tools

The essential tool used to manage aviation safety knowledge is the safety management system [7]. In its variations is can be applied to state level in form of a state safety plan or programme [2], but the principles remain always the same: it is a system of processes related to gathering and utilizing safety information in order to identify hazards and manage risks. The system has to be well documented in terms of roles and responsibilities, hazard analysis and risk assessment, data processing and privacy ensuring, and activities related to the

follow-up of the information gathered, first of all safety assurance and safety promotion. These principles are all documented in the domain-related literature [8][9] and are not subject of this article.

In practice, room for improvements of knowledge management process still exists in aviation safety in its very fundamentals: the reporting process and data quality assurance. European Union (EU) has established joint repository for data gathered throughout the European mandatory and voluntary reporting system ECCAIRS, named as European Central Repository (ECR). The repository was then used to derive industry safety knowledge, subsequently represented and formalized in the so-called "risk portfolios" produced by European Aviation Safety Agency (EASA) [10]. They present basic dependencies also named as "safety issues", i.e. patterns describing what are the key contributory factors of the most frequently observed incidents or accidents. Because this knowledge is derived from central repository based on data from all Member States, it is highly relevant and cannot be obtained so easily from individual safety management systems. It is to be implemented into local safety management systems afterwards and utilized for both investigation as well as mitigation measures.

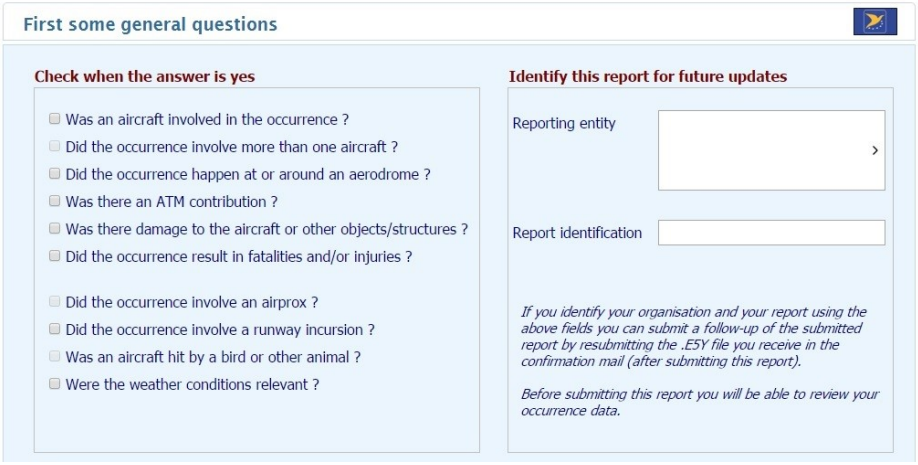


Fig. 1. EASA reporting form [12]

After years of its existence and more than one million records, the room for improvements was recognized as the data in ECR demonstrated various levels of quality, relevance and completeness and suggested that there are different reporting cultures among individual EU Member States [11]. Whilst this tells a lot about maturity, cultural differences and attitude towards safety of the reporting entity, it also points out the effectiveness and usability of the reporting system itself. It has a very complicated hierarchical structure of terms it uses and from the standpoint of user, an extensive training to use the system is a must.

Despite the training, many users did not recognize potential of many features of the system, such as Analysis Tools, Safety Performance Indicators tool, Server Side Services or Application Programming Interfaces [11]. Together with the complicated structure of the terms, the system certainly needs refinements.

With regard to this, European Commission adopted new safety reporting framework for aviation, enforced throughout Commission Regulation (EU) No 376/2014. This reporting framework sets new processes for safety reporting and also introduces attributes and contextual information to be gathered. It narrows the reporting process and provides reporting entities with some guidance on what and how to report. EU Member States and individual aviation organizations are encouraged to assure compatibility with their local software solutions and reporting systems. This framework aims to resolve many recognized deficiencies of the previous reporting scheme with providing guidance, ensuring higher degree of user-friendliness and finally higher level of data consistency.

As one of the examples of the progress, the so-called "smart forms" developed by EASA can be mentioned. The Agency recently introduced this concept aimed to simplify the reporting process by removing some burden from the reporter by limiting the fields in the form. The core of the concept is a simple hierarchical modeling of the form's sections. Each section has its context defined by the new EU legislation, e.g. aircraft section has attributes such as aircraft type, serial number or operator. Every reporter has to select his background and then is given a set of basic questions to answer (Figure 1). Based upon them the system filters irrelevant sections with their data fields. This should lead to the reporter having more time to focus on relevant data fields and not to spend too much time filling the form.

Apart from that, Reduced Interface Taxonomy (RIT) is currently under development at EU level to support usage of the ECCAIRS system itself. Not only is this taxonomy expected to reduce the vast amount of terms used by ECCAIRS (more than 4000) but it should also reduce the complicated structure of the original ICAO ADREP taxonomy [13] behind ECCAIRS. The structure of the system and the taxonomy is organized in a complex multilevel hierarchy (Figure 2), suggesting that the structure was apparently not designed to allow searching terms. Very few aviation experts are really familiar with the structure and terms thus this shortcoming needs to be addressed too.

Another example is that ADREP was intended to distinguish between for instance event types and contributory factors, whilst contributory factors were divided into explanatory and descriptive. It depended on some internal logic of the taxonomy, which distributed the terms into those two categories and limited users in the way they could be used. Whilst the logic may seem to be clear for the authors, it wasn't so much for the users from the industry. Due to this, explanatory and descriptive factors are now being abandoned in the very ECCAIRS system.

EU Member States and aviation organizations have established own reporting systems, which are all in line with the applicable Regulation. The EASA smart forms are, however, the most advanced solution available to date, despite the fact

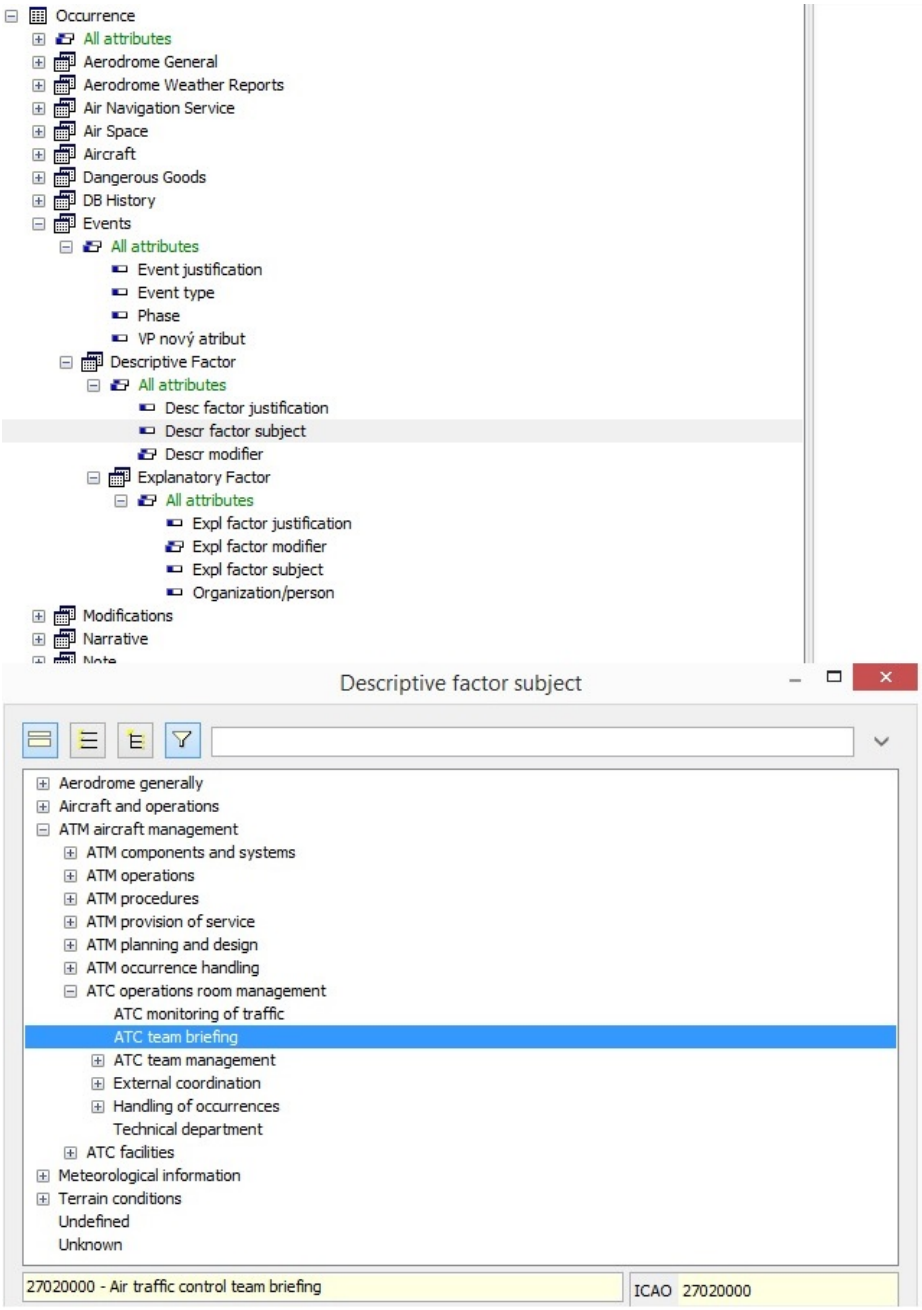


Fig. 2. ECCAIRS hierarchy

that they don't use any advanced modeling. Even compared to ECCAIRS, smart forms provide more user-friendly way how to record some safety occurrence. They assure higher quality of aviation safety data and in return more accurate risk portfolios etc.

4 Addressing practical issues with ontology

Due to its ability to cover all objects and relations between them, ontological modeling emerge as a powerful tool for systematic approach to aviation safety management. Ontology brings explicit specification of conceptualization [14], which offers great potential to address the issues with ECCAIRS and even to surpass EASA's smart forms. Ontology is formal, shared and explicit [15] and in its core well defines meanings in comprehensible structure. It is logic-based and easily processed, it covers whole domain and enable understanding of all its aspects. It was defined as shared understanding of a domain [16].

For research purposes a special ontology, related to the domain of aviation was developed. A domain model defines objects, events and relations that capture similarities and regularities in a given domain of discourse [17] [18].

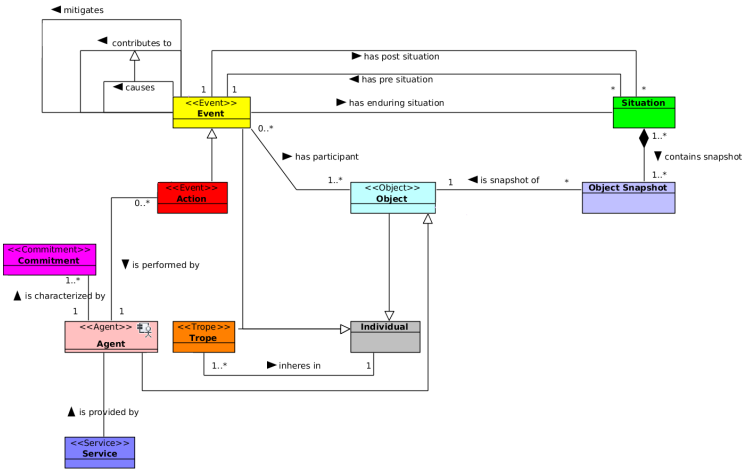


Fig. 3. Model of safety event

The primary task was answering the question how to approach modeling of terms used by ECCAIRS. EU legislation mandates EU Member States and aviation organizations to have ECCAIRS and ADREP compatible solutions for aviation safety reporting. The idea was to break down the ECCAIRS structure into its very terms and to model them using OWL, creating a new structure

which finally allows advanced features. RIT taxonomy reduction was also integrated so that, where possible, only reduced vocabulary is used.

To exemplify the use of OWL, the very same term as depicted on Figure 2 can be used, i.e. "27020000 - Air traffic control team briefing". Number 27020000 is an ECCAIRS identification, which can be preserved using OWL too, but the core difference is how the very term is modeled:

```
Briefing
and has_location some Operations_room
and has_participant some Air_traffic_controller
and has_participant min 2
```

The modeling is based on the core term, in this case it is "Briefing". It means that all other briefings are modeled likewise and so they can be all easily found and the differences between them identified. Links to other terms as "Operations room" and "Air traffic controller" are set using specific relations which allow effective searching of this particular "Briefing".

Ontology as such enables its application for many purposes and it depends on the application which needs are to be met. Formal description of the events (Figure 3) is an useful feature enabling creation of ontology-based safety management tools such as tool for safety indicators. This new approach to safety knowledge tools allows generation of ontology-based smart forms which can utilize many different relations (as outlined above) than just simple hierarchical modeling as EASA's smart forms or ECCAIRS are based on. A whole approach to making reporting more user-friendly and appearing is make it easy and logical.

Approach chosen within newly developed safety reporting tool includes ontology-based smart form concept. The idea lies in finding mutual connections between individual contributory factors, relevant safety events, model objects and relations in order to create clear structure of occurrences. Relations are used in a way that assures not only effective use of advanced tools and features, but also the option to search for desired term.

The objective of wizard is to help a reporter by reducing the list of attributes only to those related and relevant for specific event type. Presented form on the previous figure (Figure 4) shows a first step of interactive report submission, where form as such is reduced according to chosen fields. On the following picture (Figure 5) presented form is generated according to the chosen object involved in reported occurrence. Generation of these forms uses legislation requirements, expert assessment, available safety studies and advanced modeling of both the structure of the terms as well as their meaning. Especially the modeling plays key role in form generation; each filled information narrows the rest set of data fields to be filled.

Such approach is applied on all relevant event types. Its main purpose is to guide reporter correctly and logically through the reporting process in order to catch and emphasize all important facts regarding given safety event. Reporter is guided to submit comprehensible event description including underlining the contributing factors and circumstances. The tool allow using contributory factors but in line with the newest approach, i.e. using them as event types preceding

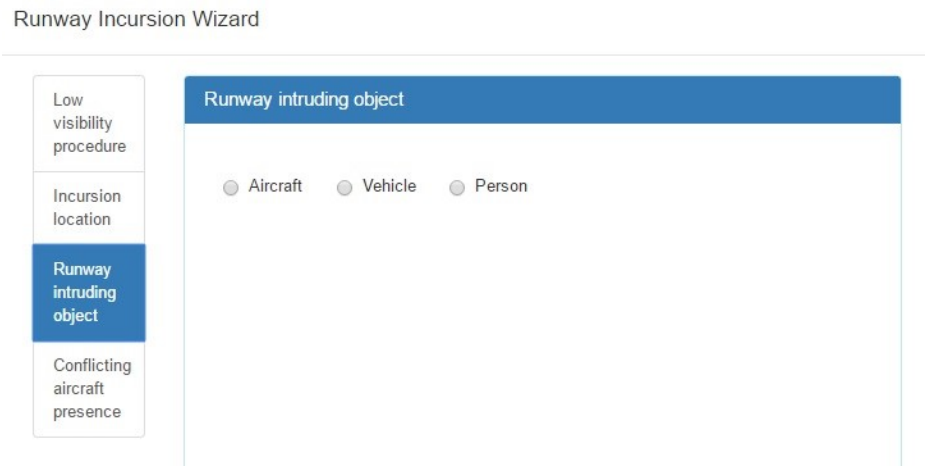


Fig. 4. Smart reporting form - first level

the occurrence and not as special terms to be selected from separate lists. The interface of the tool is appealing and provides reporter with clear information and instructions.

Additionally, the model allows searching the most appropriate term to be used for event type, contributing factor or circumstance. Using controlled OWL language and then full-text search, one can search the entire vocabulary (Figure 6). Analytic and statistical features of the tool bring additional possibilities for effective safety management. Different kind of data representation, statistics, query builders, etc., covers organization's needs and could support their productivity. Such easy-to-use software should decrease reluctance to such initiatives. Benefits brought through system implementation are numerous, including their compatibility and up-to-date format in relation to current legislation.

5 Conclusions

Development of safety knowledge systems is understood as support and encouraging step leading to effective safety management. It brings different kinds of benefits and covers whole domain. Current solutions have their strengths and weaknesses, but their main advantage is the fact that they are being used for quite some time, influencing their users to express quite strong reluctance toward implementation and deployment of the new, more advanced solutions.

Different strategies could be chosen in order to overcome this kind of problems. The focus should be placed on making the solution more understandable and easy to use, with clear expression of advantages that such system could provide. Also, the solution must fulfill the requirements for all kinds of organization, regardless of their current size of maturity level.

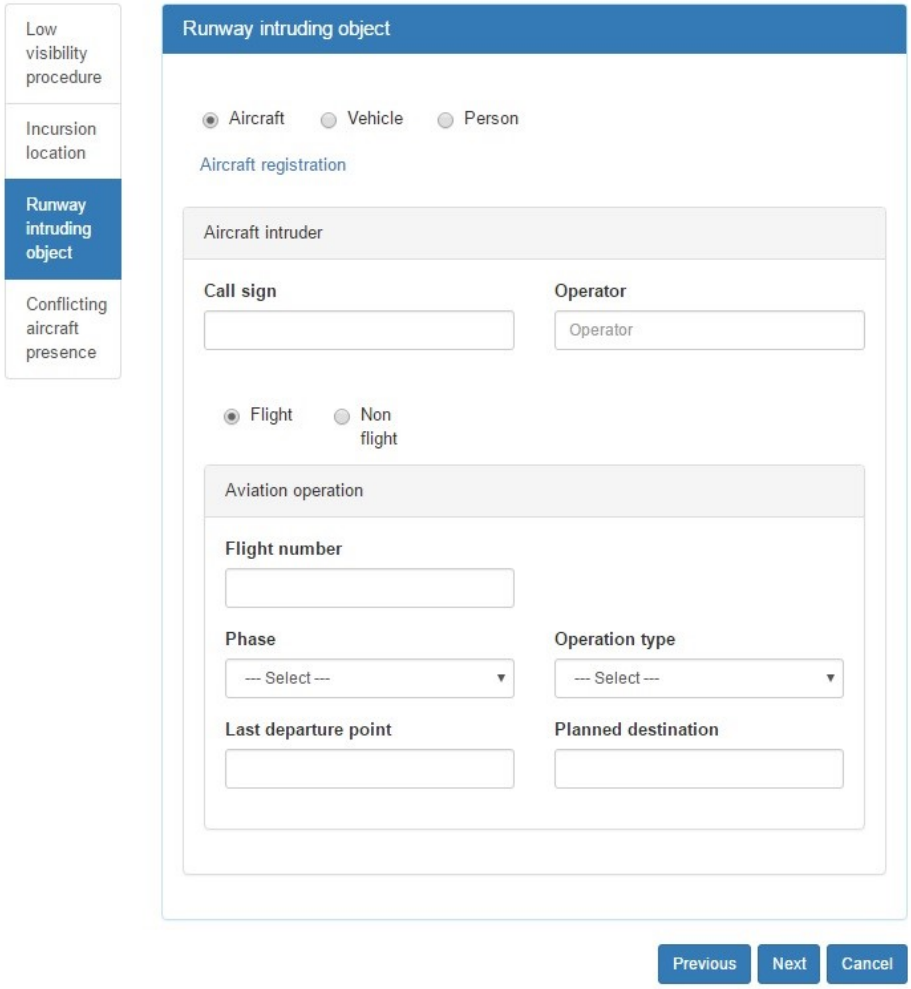


Fig. 5. Smart reporting tool - second level

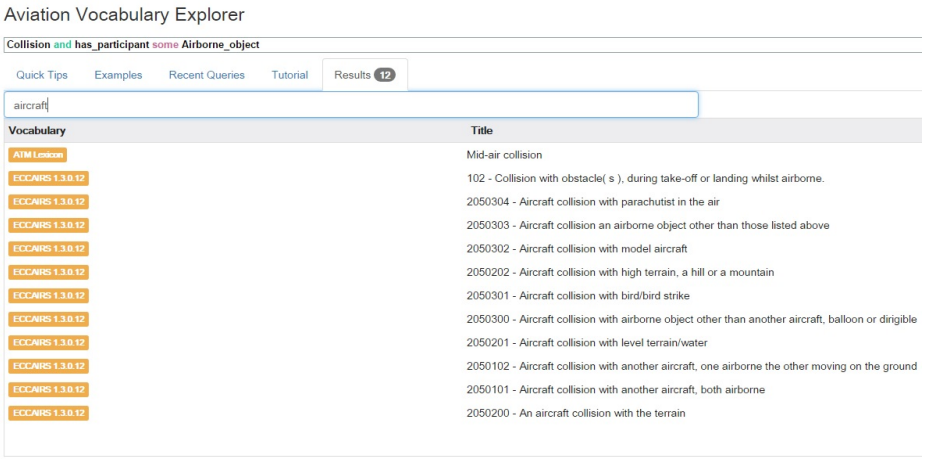


Fig. 6. Aviation vocabulary explorer

Ontological modeling is recognized as powerful tool for reaching expected result in the domain of aviation safety. It covers all aspects adequately and enables required level of occurrence structure description. Features that are brought as a result of an ontology implementation are numerous. Smart reporting forms developed through projects at the Czech Technical University defines the direction of the future safety management development.

Acknowledgement

This paper was supported by the Technology Agency of the Czech Republic, grant No. TA04030465.

References

1. ICAO - International Civil Aviation Organization, 2013. Paper A38-WP/85 on Consolidated Aviation Safety Knowledge Management: An Enabler of Improved Operational Safety for the 38th ICAO Assembly in September/October 2013. Montréal, Quebec, Canada.
2. ICAO - International Civil Aviation Organization, 2013. Safety Management Manual (SMM): Doc 9859. 3rd edition. Montréal, Quebec, Canada. ISBN 978-92-9249-214-4.
3. Socha, V., Schlenker, J., Kalavsky, P., Kutilek, P., Socha, L., Szabo, S. and Smrcka, P. 2015. Effect of the change of flight, navigation and motor data visualization on psychophysiological state of pilots. SAMI 2015 - IEEE 13th International Symposium on Applied Machine Intelligence and Informatics, Proceedings. Herlany, Slovakia 22-24 January 2015, p. 339-344. ISBN 978-1-4799-8221-9.

4. Novák, L., Němec, V. and Soušek, R. Effect of Normobaric Hypoxia on Psychomotor Pilot Performance. In The 18th World Multi-Conference on Systemics, Cybernetics and Informatics. Orlando, Florida: International Institute of Informatics and Systemics, vol. II, p. 246-250. 2014. ISBN 978-1-941763-05-6.
5. Leveson, N. 2011. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press. Engineering systems. ISBN 978-0-262-01662-9.
6. TRADE - Training Resources and Data Exchange. 1995. A Handbook of Techniques and Tools: How to Measure Performance. U.S. Department of Energy, Washington, DC.
7. Stolzer, A. J., Halford, C. D. and Goglia, J. J. 2011. Implementing safety management systems in aviation. Burlington, Vt.: Ashgate. Ashgate studies in human factors for flight operations. ISBN 978-1-4094-0165-0.
8. Waring, A. 1996. Safety management systems. 1st ed. London: Chapman, Hall. ISBN 978-0412719103
9. Gabbar, H. A. 2004. The design of a practical enterprise safety management system. Dordrecht: Kluwer Academic Publishers. ISBN 1-4020-2949-7.
10. EASA - European Aviation Safety Agency. 2015. Annual Safety Review 2014. Cologne, Germany. ISBN 978-92-9210-196-1.
11. Post, W. 2015. ECCAIRS Survey. Presentation at ECCAIRS Steering Committee Meeting, Brussels, 26-27 October 2015. Joint Research Centre, Brussels, Belgium, 2015. Available from Internet: http://eccairsportal.jrc.ec.europa.eu/index.php/Documents/39/0/
12. JRC - Joint Research Centre. 2016. Aviation Safety Reporting [online]. Available online: http://www.aviationreporting.eu/
13. International Civil Aviation Organisation, 2000. ADREP 2000 taxonomy.
14. Gruber, T.R., 1993. A translation approach to portable ontology specification. Knowledge Acquisition 5(2), 199-220
15. Studer, R., Benjamins, V. R., Fensel, D. 1998. Knowledge Engineering: Principles and Methods. Data Knowledge Engineering, 25(1-2), 161–197
16. Gomez-Perez, A., Fernandez-Lopez. M, Corcho, O. 2005. Ontological Engineering. Springer
17. Guizzardi, G. 2005. Ontological foundations for structural conceptual models. University of Twente, Enschede, The Netherlands, Enschede
18. Ledvinka, M. - Křemen, P.: JOPA: Accessing Ontologies in an Object-oriented Way. In Proceedings of the 17th International Conference on Enterprise Information Systems. Porto: SciTePress - Science and Technology Publications, 2015, p. 212-221. ISBN 9789897580963.

Appendix H

LEDVINKA, Martin, Andrej LALIŠ and Petr KŘEMEN. Towards Data-Driven Safety: An Ontology-Based Information System. *Journal of Aerospace Information Systems*. 2018, 16(1), pp. 22-36. DOI: 10.2514/1.I010622.

JOURNAL OF AEROSPACE INFORMATION SYSTEMS
Vol. 16, No. 1, January 2019

Toward Data-Driven Safety: An Ontology-Based Information System

Martin Ledvinka,* Andrej Lališ,† and Petr Křemen*
Czech Technical University in Prague, 166 27 Prague, Czech Republic

DOI: 10.2514/1.I010622

In the age of data, enterprise-related data can be efficiently used for supporting safety management decisions. In this paper, the state of the art in the domain of aviation safety is reviewed and problems that current aviation safety information systems suffer from are identified. Based on the outcomes, ontologies are defended as a technology for safety data management and the design and implementation of an ontology-based information system for aviation safety data integration is presented. The system was developed in cooperation with the Civil Aviation Authority of the Czech Republic, and it is described in terms of design, core technologies, and achieved functionalities. Subsequently, it is compared to other available solutions in the domain. The results indicate that, by linking the features to ontologies, many desired characteristics of the safety information system are achieved due to proper utilization of top-level ontologies and that the solution offers a systematic and sustainable way for improving aviation safety.

I. Introduction

SAFETY management has relevance only for specific industries that deal with everyday risks of serious harm to persons or damage to properties, such as nuclear, aviation, railway, and marine industries. Effective and efficient safety management is fundamental to their everyday operations, and so they strive to ensure it. Regardless of the industry concerned, the principles of how safety is managed are similar. Many problems stem from inadequate data management, such as the inability to collect accurate and relevant data about safety occurrences, insufficient integration of heterogeneous safety data, and the consequent inability to perform relevant analyses and evaluation of safety performance. In fact, these problems prevent safety management departments from closing the loop of efficient data-driven safety with well-established safety culture.

The issue is that data-driven safety is highly susceptible to the quality of data and their management. Especially data collection and processing are critical for producing accurate safety-related knowledge about the managed system. Therefore, it has to be ensured that the quality, relevance, and completeness of safety data are taken into account during integration. Only after that is it possible to exploit the benefits of data-driven systems. However, their implementation to safety management is far from perfect because the majority of the existing data-driven systems do not address these issues systematically and often deal with inconsistent, incomplete, or biased data. There is a room for every safety manager to set up his/her own system using diverse terminology, different levels of detail, and different data management processes, leading to limitations in safety oversight. As an example, one may take the assessment of piloting precision during simulator training [1]. When using the European Coordination Centre for Accident and Incident Reporting System's (ECCAIRS) standardized aviation taxonomy [2], the following terms describe contributory factors in the case of a safety occurrence: *human/system interface-basic/initial training, simulator training, specific training, emergency training, recurrent training, and route training*. With regard to simulator training, these terms are not disjoint, and their semantics allow for interpretation variance. According to the authors' experience with aviation industry stakeholders, safety managers may prefer some of them while completely omitting others.

This paper describes our research efforts toward a safety data collection and processing system (SDCPS), which would ensure a high quality of safety data while integrating heterogeneous data from different sources. This SDCPS has to support the standard use case of national civil aviation authorities (CAAs), which receive occurrence reports (mandatory as well as voluntary) and process them in order to support their internal processes. The data processing might range from consolidation of information when an occurrence report is received from multiple aviation organizations to investigation in which the CAA looks for additional information clarifying a particular occurrence (typically, the causal factors or other relevant information). Subsequently, the SDCPS must be capable of representing the data so that weak parts and areas of greater concern in the industry are easily identified to allow the CAA to take adequate and timely measures. The aforementioned problems with current safety management are addressed by modeling the meaning of data by domain ontologies to minimize misinterpretations during data sharing and distribution between distinct systems or people. The system can serve as a core solution for data-driven safety, which can be incorporated into any safety management software or existing solutions for safety data collection and processing.

The research described in this paper is performed in the aviation industry, with the focus on national aviation authorities. Unlike typical high-risk industries, aviation is highly complex with many stakeholders and overlapping technology used in everyday operations. Due to the complexity, the sector poses an ideal environment for research of an advanced data-driven approach to safety. National aviation authorities deal with numerous organizations in their area of responsibility; because they typically collect and process data from multiple stakeholders, they are suitable candidates for the application and validation of the proposed solution. The Civil Aviation Authority of the Czech Republic was an industry partner of the research, supporting the system development with subsequent deployment and testing in the aviation environment.

The following sections provide details on the current state of the art in aviation (Sec. II), which was the starting point for the research, and the selected methodology to achieve its goal (Sec. III). Section IV describes the design of the developed system, and Sec. V presents its evaluation. The paper is concluded in Sec. VI.

Received 28 November 2017; revision received 14 September 2018; accepted for publication 18 October 2018; published online 19 November 2018.

*Researcher, Department of Cybernetics, Faculty of Electrical Engineering, Technická 2.
†Researcher, Department of Air Transport, Faculty of Transportation Sciences, Horská 3.

II. State of the Art

International regulatory bodies govern aviation standards, including those related to safety data collection and processing. Top-level requirements are defined by the International Civil Aviation Organization (ICAO), which stipulates and justifies the existence of SDCPSs. Furthermore, it specifies their distribution between state-level and organization-level management [3]. All aviation safety management systems must follow these standards. SDCPSs, in particular, must include support for capture, storage, and aggregation of data on accidents, incidents, and hazards. Also, there has to be a distinction made between the mandatory and voluntary reporting systems, and the system shall be designed as a web application.

A. Aviation Safety Management in Europe

Regional and national legislations further specify what an SDCPS is supposed to collect and how this should be done. In the European region, there are regulations issued by the European Commission, detailing the list of relevant safety occurrences and various contextual information to be collected [4,5]. In addition, they specify the very process of data collection, which includes the dissemination of a part of the data to national and European civil aviation authorities. To this end, the European Coordination Centre for Accident and Incident Reporting Systems was established together with the European Central Repository (ECR) and, recently, the Internal Occurrence Reporting System (IORS), which is an ECCAIRS compatible solution interconnected with the ECR.

However, practical experience with the ECCAIRS has revealed several issues by now. As an example, users are not familiar with tools and add-ins (such as the tool for safety performance indicators, the add-in for validation, etc.), the system does not support meaning sharing, and its capabilities for data quality enforcement or data inconsistencies checking are limited. The ECCAIRS has a weak point in how it manages safety data: it offers extensive taxonomies (hundreds to thousands of terms each [6]), with little guidance on how to effectively use them by reporters. As in almost every taxonomy, it is regularly updated by moving existing terms or adding new ones, but there are also cases in which the update involves a change of meaning. For example, in taxonomy version 1.3.0.12, the term altitude bust was moved from the context (its parent in the taxonomy tree) of aircraft handling-related events to deviation from an air traffic control clearance, with some changes in the term description. The result of all the aforementioned is that, without proper management of all the changes in taxonomy terms and their meanings, safety reports can easily become incomplete, or even incorrect in terms of event/factor classification [6].

To reduce the negative effects related to taxonomy complexity, the so-called Reduced Interface Taxonomy (RIT) was introduced. The taxonomy significantly reduced the ECCAIRS taxonomy (e.g., the number of attributes dropped from 455 in the ECCAIRS to about 150 in the RIT). To improve data quality, online smart forms [7] for European Union (EU)-level reporting were introduced. Even though these measures shifted the European SDCPS (ECCAIRS, IORS) to support more consistent information gathering, there is still no robust layer for managing safety data. This problem gets even more apparent when realizing that the ECCAIRS deals with one type of safety data only, completely omitting any integration with other safety data, such as data from audits or inspections. National regulatory authorities in Europe share the EU-level issues, and there is no adequate solution.

Looking at the organization-level safety management systems, the issue gets less apparent. This is because, on a smaller scale, the complexity is not as significant as on the national or regional level, and safety managers often manage to keep track of the most apparent and common issues, especially in small- to medium-size enterprises. In Europe, they all have to obey both the ICAO standards and the European regulations, and so they are forced to work at least with the RIT. Internally, organizations may (and often do) use their own vocabularies and tools to collect and process safety data, whereas for reporting to regulators, they have different processes. Typically, only larger organizations integrate them. However, an SDCPS with advanced integration and management of safety data is missing in the industry but would be beneficial because safety data are to be shared and disseminated among the industry and regulators in a consistent way and with adequate quality.

B. SDCPS Comparison

To place our solution into the context of others, a collection of state-level SDCPS and commercially available safety management system (SMS) software, which features SDCPS capabilities, was evaluated. The initial set of systems comprised all EU member states systems, including EU-level systems, as well as state-level SDCPSs in the United States and Australia. For commercial software, a standard search was used to identify safety management solutions available online. The final selection was based on an expert assessment of available occurrence reporting websites and state annual reports regarding aviation (indicating the maturity of a respective system), whereas for commercial SMS solutions, they were based on various information and materials available on respective producers' websites. Systems with advanced behavior (either exhibiting it or advertising it), surpassing basic features of an information system, were selected.

1. *Compared SDCPSs*

The final selection included the following state-level systems: the Aviation Safety Reporting System (ASRS) [8] by the Federal Aviation Administration, the European Aviation Safety Agency (EASA) aviation reporting portal [7] (ECCAIRS-based solution at the EU level, implemented as the IORS internally at the EASA), the aviation accident or incident notification form[‡] by the Australian Transport Safety Bureau (ATSB), and the Finland[§] and Norway[¶] aviation occurrence reporting portals. Ireland complements the analysis because it was contacted directly upon expert recommendation. Other European countries were also contacted, but they use ECCAIRS as their primary SDCPS, and thus are not explicitly discussed in the analysis. These countries included France, Germany, Iceland, Italy, and Switzerland. From commercially available software solutions, Aviation SMS-Pro[**],[††] Q-Pulse, Baldwin SMS,[‡‡] Intelex,[§§] and SMS by Rolls–Royce [9] were selected.

2. *Evaluated Features*

A list of features was composed to check how the systems dealt with the issues mentioned throughout this and the previous sections to compare their maturity. The selection was based on the current state of the art; other features may become more relevant in the future. The complete list of evaluated features is in Table 1, together with their categorization.

[‡]https://www.atsb.gov.au/mandatory/asair-form/.
[§]https://www.trafi.fi/en/aviation.
[¶]https://www.altinn.no/en/forms-overview/civil-aviaton-authority/accidentincidentoccurrence-reporting-in-civil-aviation/.
**https://www.asms-pro.com/.
[††]https://www.ideagen.com/solutions/safety-management-system/.
[‡‡]http://www.baldwinaviation.com/about1.
[§§]https://www.intelex.com/products/applications/ehs-incident-management.

Table 1 SDCPS feature comparison

Category	Feature	Description
Knowledge quality	Taxonomy management	Does the software manage different versions of taxonomy(-ies)?
	External taxonomies usage	Does the software use one or multiple external taxonomies?
	Custom controlled vocabulary	Does the software support customized vocabularies/taxonomies?
	Modeling of event/contributory factors chains	Is it possible to model the chain of events (including contributory factors), i.e., to express their sequence and mutual relations?
Intelligent analysis	Integrating knowledge from occurrence and audit reports	Is the software able to record or identify dependencies between occurrence and audit reports?
	Event chain analysis	Is the software able to identify frequent behavioral patterns in data?
Ergonomics	Adaptive occurrence report forms	Do reporting forms take into account the filled-in information when deciding which additional data fields to display?
	Adaptive audit report forms	Do audit forms take into account the filled-in information when deciding which additional data fields to display?
Flexibility	Compliance with European occurrence reporting scheme	Is the software able to produce reports compliant with the current EU regulatory framework (especially EU regulation nos. 376/2014 Ref. [4] and Ref. [5] 2015/1018)?
	Open data exchange formats	Does the software support using open data exchange formats, such as comma-separated values, open document spreadsheet, or structured query language?
	Support for safety performance indicators/safety issues	Are there safety performance indicators/safety issues displayed and evaluated?

a. Knowledge Quality Features. Knowledge quality features regard the issue of data management. With respect to this, taxonomy management is considered important for users to assure report consistency in time with regard to taxonomy evolution. There are multiple taxonomies available in civil aviation that can be used to complement insufficient or imprecise coverage of certain aspects of a taxonomy, and so the usage of external taxonomies can be of benefit to their users. The option to customize the vocabulary complements this feature by the possibility of customizing or translating taxonomies as needed. The last feature of this category regards the modeling of contributory factor chains. It allows the user to not only classify what happened but also to add the information about the chronological order and causality between the contributory factors and the final event outcome. All these features contribute to data quality (i.e., consistency, completeness, and relevance), with a strong focus on how a system manages the data.

b. Intelligent Analysis Features. Intelligent analysis features aim to check the maturity of analytical modules available within the solutions, elaborating further on the issue of data management. The first assessed feature regards the integration of knowledge from occurrence and audit reports. These two types of reports are based on different processes and, for state-level oversight, it is important to find dependencies in the data. To allow this kind of analysis, data are to be properly integrated. The other feature regards the analysis of event chains or, more precisely, the capability to identify behavioral patterns. This is also crucial for any safety management solution because behavioral patterns are to be identified to allow for effective control of unwanted occurrences.

c. Ergonomic Features. Ergonomic features are selected to check the user friendliness of a solution, supporting the improvements in data completeness, relevance, and consistency. Considering a typical SDCPS, this property is observable in form adaptability because aviation safety taxonomies are robust and the user should never be given more than its well-selected parts. An ergonomic solution shall allow for adaptive report forms with flexible data fields selection, both for occurrence and audit reporting, limiting the burden on the end user to support better quality reports.

d. Flexibility Features. Flexibility features consider additional features that are interesting with regard to the state of the art in aviation and that mostly regard the issue of the ability to share meaning. Compliance with current EU reporting, which includes data exchange with the assurance of meaning, is required almost by every aviation stakeholder in the EU, and so it is considered. Open data exchange formats are interesting from the perspective of data exchange between multiple and possibly incompatible systems. The last checked feature regards the support for safety performance indicators and safety issues. These are to be established based on current ICAO standards in aviation [3] and are subject to data exchange, where the meaning is to be assured, as the performance of different states and aviation organizations are compared in the industry.

3. Comparison Results

The comparison was based on publicly accessible information. It was not possible to evaluate all the selected systems because some of their features were not declared publicly, and thus needed to be identified in the course of discussion, either with representatives of the respective regulator (in the case of a state-level SDCPS) or the software producer. The companies and institutions were mostly contacted by official means (online contact form, e-mail, or phone); the Czech CAA helped to establish some additional contacts. Unfortunately, from state-level systems, the ASRS, ATSB, and Norway did not respond to the survey. From commercial software producers, none replied, but it was possible to evaluate Q-Pulse based on a discussion with one of their customers. SMS Pro was evaluated from their website and YouTube demonstration videos. The survey results are shown in Table 2.

The results indicate that most of the features are not provided at the state level. For commercially available SMS software, the situation is better; but still, there are some features unavailable for both evaluated solutions. Also, they use different, sometimes completely proprietary vocabularies. For instance, SMS Pro uses its own *accident/incident-type* classification instead of the *occurrence category* defined in the ECCAIRS. These solutions clearly aim to meet safety management standards and to provide a common software platform for different user tasks; however, there is no emphasis put on integration and subsequent knowledge generation from safety data. This is illustrated by the fact that both evaluated commercial software systems highlight a variety of supported tasks while completely omitting remarks on knowledge generation and quality assurance.

For state-level SDCPS, there is no commercially available safety management or SDCPS solution to support safety data collection and processing, and thus the authorities develop their own customized systems or reuse the ECCAIRS-based approach. In addition to the performed survey, reporting forms and periodically issued reports, both at regional and national levels, indirectly indicate the domain state. None of the mandatory and voluntary reporting forms, including those outside the European region, guide the user through the reporting process when working with data fields. They use simple hierarchical filtering instead, forcing users to follow the same reporting process for every report they create.

Table 2 Evaluated SDCPS solutions

Feature	EASA	Finland	Ireland	SMS-Pro	Q-Pulse
Taxonomy management	✓	✓	✓		
External taxonomies usage	✓	✓	✓	✓	✓
Custom controlled vocabulary		✓	✓	✓	✓
Modeling of event/contributory factors chains	✓	✓		✓	✓
Integrating knowledge from occurrence and audit reports				✓	✓
Adaptive occurrence report forms			✓	✓	✓
Adaptive audit report forms					✓
Event chain analysis					✓
Compliant with European occurrence reporting scheme	✓	✓	✓	✓	✓
Open data exchange formats				✓	✓
Support for safety performance indicators/safety issues				✓	

Annual reports on safety are missing identification of deeper behavioral patterns; the only exception is the recent ECR evaluation [10], in which efforts were spent to identify top-level correlations. However, even at this level, improvements are possible because the knowledge derived from the repository is limited in the identification of relevant contributory factors. For example, it merges factors into so-called safety issues, such as *flight planning and preparation*, without specifying the necessary details to enable aviation stakeholders to draw an action plan for their prevention.

III. Methodology

Application of ontologies was selected as the core solution to address the issues identified in the previous section and with regard to the goal to be achieved. In this section, the research concept is introduced, followed by a description of how it was used to build a robust, interoperable SDCPS. The suitability of the ontology-based approach is also defended.

A. Ontologies

Ontologies serve to conceptualize and formalize a domain of discourse [11]. Such conceptualization distinguishes, for instance, endurants (entities changing in time) from perdurants (events), their tropes (dependent properties), and other notions. Formalization of these concepts can be done in terms of formal logic, i.e., using individuals, classes, properties, and their logical relationships. A formal ontology consists of two parts: a schema, which describes general relationships in the domain (a *runway incursion* is a special case of an *incident*); and data representing the description of an actual state (two aircraft participated in runway incursion X that occurred at time Y at airport Z).

The first applications of ontologies and the original driving force of development of more expressive ontological languages emerged in medicine, in which ontologies were used to build terminological taxonomies, e.g., SNOMED CT [12]. Later, the advantages of ontologies were recognized in other domains. Safety-related uses of ontologies first regarded road transportation safety [13] and topics bordering with medicine [14]. As far as aviation safety was concerned, the works of Garst [15], Keller [16], and Denney and Pai [17] showed that the U.S. aviation authorities and researchers considered ontologies useful for modeling of the domain, data integration, and sharing vocabularies. In Europe, the ECCAIRS taxonomy and related systems were built without any explicit formalism [6]. Carvalho et al. [18,19] built an ontology-based system supporting the investigation of accidents in the space industry. Eventually, this system evolved into a commercially available, patented tool [20]. Another area in which ontologies have become popular is industrial manufacturing. There, they can be used to support requirements analyses [21] or to describe the manufactured systems and their domain [22,23].

In information technology, an ontology can be viewed from two viewpoints: one, discussed so far, is an abstract model of a particular domain of discourse. The other is a physical artifact, which is a realization of the model expressed in the selected ontological language. The main distinguishing features of these physical artifacts are described in the following paragraphs.

1. Shared Schema

An ontological schema represents a description of data, which can be shared among systems (ontology schemas are often published online) and ensures their semantic interoperability. For instance, the aviation safety ontology (ASO) discussed in Sec. III.B.1 is used by the SDCPS developed in this research and by a safety data management and reporting tool created as part of the INBAS project [24]. In the future, it is expected that these applications will cooperate, bypassing the current practice of reporting safety occurrences to the CAA via e-mail.

2. Distributed Nature

Ontologies are one of the cornerstones of the Semantic Web [25], which was envisioned as a successor of the web. As such, it has the same distributed nature. For ontologies, this means that they can be interlinked; ontological schemas often reference other ontologies, and many ontologies consist of a number of smaller modules capturing more specific portions of the described domain. For instance, ASO consists of several specialized subontologies concerning safety, documentation and reporting, auditing, etc. These ontologies can be reused by other systems; for example, the documentation and safety ontologies could be used in occurrence reporting for other high-risk industries, and the data from both systems could be eventually integrated into a national safety program.

3. Global Identifiers

The terms in ontologies are identified by Internationalized Resource Identifiers (IRIs), which are unambiguous identifiers that allow global identification of entities. For example, multiple systems can have in their database the aerospace manufacturer Boeing represented by the IRI http://dbpedia.org/resource/Boeing, and they would all recognize it as the same entity. Were they based on relational databases, the object would most likely have a different vendor-specific identifier in each system.

4. Schema and Data Together

Schema and data can be stored together and are defined using the same language. The SPARQL query language [26] can be used to query both the schema and the data (or their combination) [27], whereas SPARQL Update [28] can be used to update both. Therefore, the user can explore a newly discovered data source without any prior knowledge of its schema; he is able to gather basic information using just a few queries

(e.g., select all classes, properties, etc.). This can significantly enhance the end-user experience. An ontological search engine can competently answer a query searching for aircraft manufacturers without doing a full-text search in the data and without knowing the ontological schema beforehand because such companies (entities) belong to a specific ontological class. In addition, IRIs often have the form of uniform resource locators, and so the query results can be directly dereferenced to obtain web pages with further information about respective resources (try opening the IRI http://dbpedia.org/resource/Boeing in a web browser). This allows us to efficiently share data inside a community (or publicly) as linked data [29].

5. Inference

Formal ontologies are written in languages of different expressiveness. Even low-expressiveness ontological languages can be used to build hierarchies of classes and properties. More expressive languages are based on the formalism of description logics [30], and they support the definition of more complex relationships between classes and properties (e.g., disjointness, one being an inverse of the other, etc.) Given these hierarchies and relationships, the formalism of ontologies allows automated procedures to infer new knowledge from existing data. Consider the following example (Turtle syntax [31] is used throughout the paper, omitting IRI prefixes for the sake of compactness):

```
ex:manufactures owl:inverseOf ex:hasManufacturer
ex:B ex:manufactures ex:D
```

The property `manufactures` is the inverse of `hasManufacturer`. Owing to this definition and the fact that `ex:B` manufactures `ex:D`, a reasoner (which is a specialized software that understands the languages used to define ontologies) can deduce the following:

```
ex:D ex:hasManufacturer ex:B
```

Moreover, imagine that `ex:D` experiences a technical failure. The inferred information can be used to easily find its manufacturer; `ex:B` and a statistics service can find any other incidents involving products of `ex:B`. Based on this, safety inspectors can react and plan a safety audit at `ex:B`.

It is important to note that the reasoner has no prior knowledge of the schema of the ontology. It only knows the general rules of the respective ontological language.

6. Standard Languages

The most often used ontological languages are standardized by W3C–RDFS [32] and the current state-of-the-art languages OWL [33] and OWL 2 [34]. The expressiveness of these languages (particularly OWL 2) is high, which makes reasoning using them computationally difficult. Therefore, there exist profiles with more favorable computational properties.

These standardized ontological languages can be serialized using the Resource Description Framework (RDF) [35], which is a standard model for data exchange on the web. The RDF is an evolution of the original linking schema of the web; it represents data as triples of subject, predicate, and object; and it can be visualized as a directed, labeled graph in which the nodes represent resources (subjects and objects) and the edges represent their connecting properties, as shown in Fig. 1. Most important, the RDF represents a standardized machine-readable structured format to which systems can adhere.

B. Ontological Pillars of Aviation Safety

The approach of this research is based on several requirement pillars, which are determined by the current issues in safety management and the state of the art in the domain (discussed in Sec. II): 1) integration of safety data from different sources based on a common domain model, 2) ability to express contributory factors of safety occurrences and audit findings, 3) stable and well-structured taxonomies and vocabularies, and 4) context-based input methods aiming to improve data quality.

The remainder of this section discusses these pillars and shows how the ontology-based solution supports each of them. The focus is put on Europe, considering regulations on the EU and the member states levels, respectively. An example report depicted in Fig. 2 is used throughout this section to illustrate important points of the methodology. This report is based on an accident investigated by the Czech Air Accidents Investigation Institute [36]. The image uses shortened IRIs with prefixes corresponding to respective ontologies, e.g., doc refers to the documentation ontology. Nodes represent objects; and edges represent relations between them. Each node contains type information (bold labels above the line) and a simple object name (label below the line). Labels in italics refer to external vocabularies (see pillar three). Note that ECCAIRS identifiers are written with human-readable labels for illustration purposes instead of ECCAIRS code values (e.g., *eccairs:loss_of_control* is actually *eccairs: vl-a-430/v-13*, which identifies value *v-13* in value list *vl-a-430*). Note that event-0-a is marked in bold to show the integration of occurrence and audit report factors, which will be discussed in Sec. III.B.2.

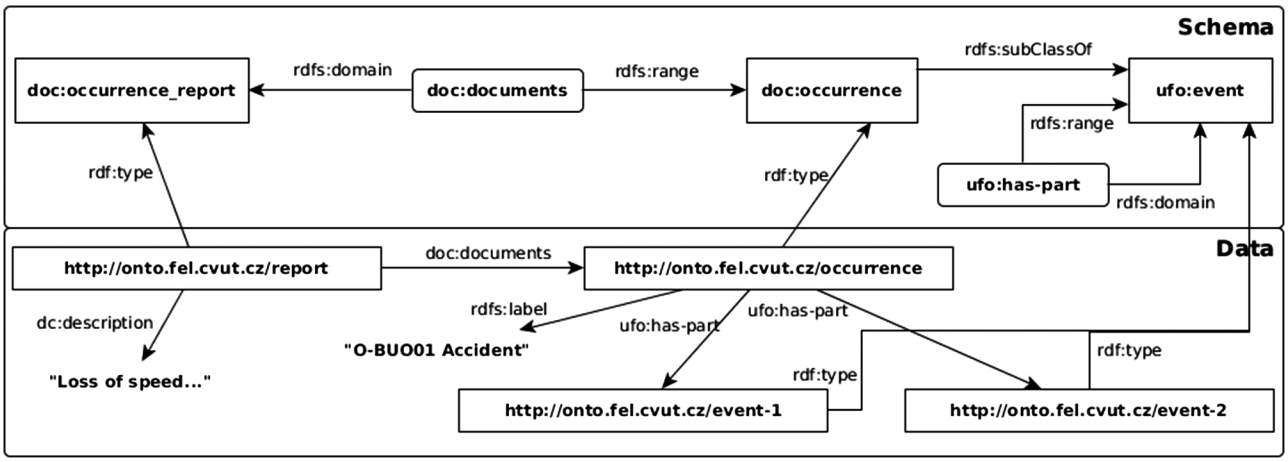


Fig. 1 Ontology visualization example. XML namespace prefixes are used to shorten full IRIs.

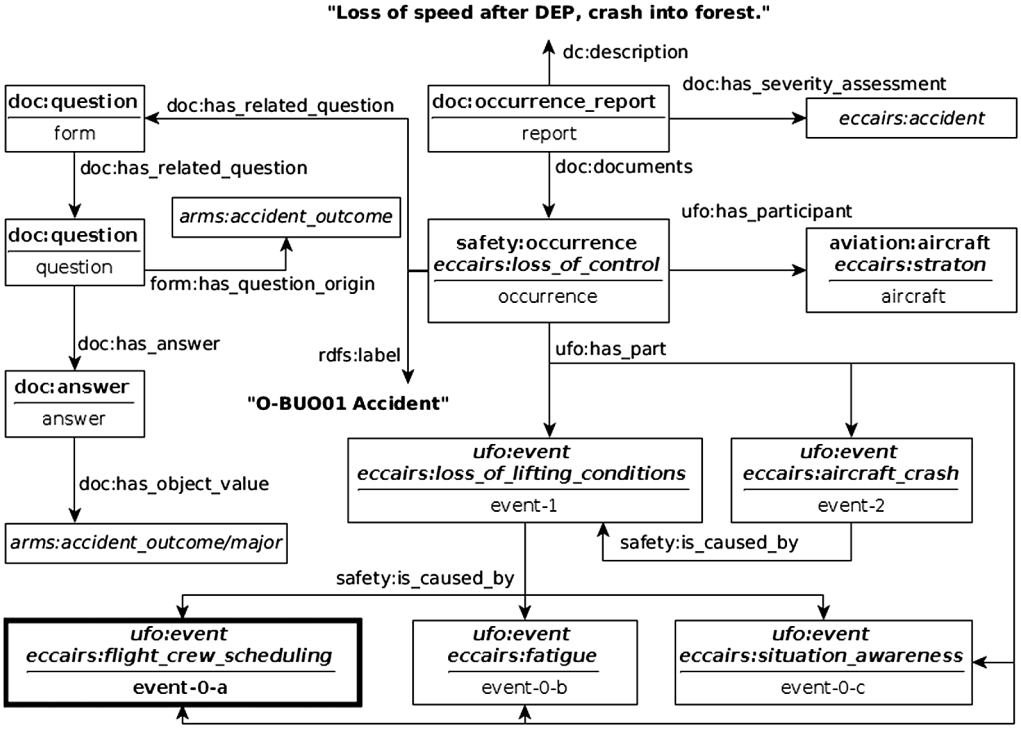


Fig. 2 Report example visualization (DEP, departure; LOLI, loss of lifting conditions; QA, question-answer).

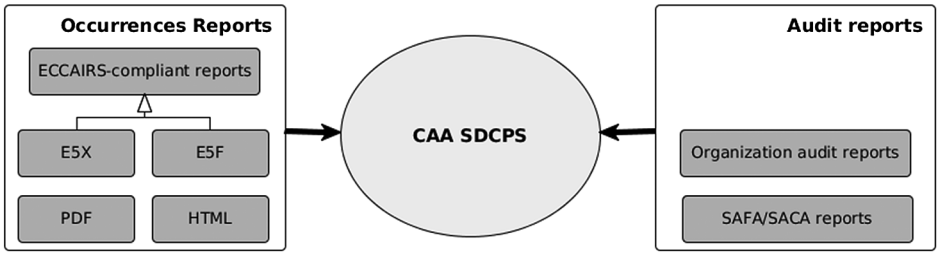


Fig. 3 Civil aviation authority inputs.

1. Ontology-Based Safety Data Integration

There are two main types of reports received or created by a civil aviation authority: occurrence reports and safety audit reports. This is schematically depicted in Fig. 3. The figure also shows that reports often exist in various formats, which is an issue to deal with (E5X, E5F, portable document format, hypertext markup language, and SAFA/SACA are various report formats that will be discussed later).

The problem of many aviation authorities is that their departments do not systematically share data. For instance, the staff performing safety audits does not have access to occurrence reports because occurrences are usually investigated by a different department. Moreover, both departments often have reports in different formats. The aviation safety ontology [37] represents a comprehensive ontological model of the aviation safety domain aiming to remedy this situation. It allows an SDCPS to integrate both reactive safety data (occurrence reports and their investigation) and proactive data (audits and audit findings) to complete the picture of safety performance. An analytical module (discussed in Sec. IV) is then able to provide an integrated view of the data. For instance, the user can view all reports concerning a particular organization, e.g., an airline operator. Auditors may use this information when planning an audit, concentrating on the issues identified in occurrence reporting and previous inspections.

The ASO is based on the unified foundational ontology (UFO) [38]: a generic ontology that provides basic concepts for the description of entities, their relationships, roles, and events (see items with the prefix ufo in Fig. 2). Using an upper-level ontology (an ontology of generic terms, on which more specific ontologies can be based [39]), such as UFO, makes the aviation safety ontology more suitable for integration with other systems. The overall structure of the ASO is depicted in Fig. 4, where the arrows denote an ontology extending another ontology (e.g., the safety ontology extends the UFO), and the geometrical relationships between the ellipses represent structural relationships of the ontologies, e.g., the ASO consists of the aviation safety core and the CAA ontology.

The ASO consists of a core, divided into specialized submodules, and an application-specific ontology, which is based on the core. For the purpose of this paper, the application-specific ontology concerns the CAA. At this point, let us discuss the crucial modules of the ASO.

a. Aviation Ontology. Aviation ontology [40] forms a general model of the aviation domain. It contains the specification of *events*, their types, and *objects*, which can be *agents* such as a *person* or *organization*, and *physical objects*, such as *aircraft* or *aerodromes*. Figure 5 shows a simplified excerpt from the ontology. In the example report (Fig. 2), the specification of aircraft being an instance of *aviation:aircraft* relates it to the aviation ontology. It is actually the only part of the report example that ties it to the aviation domain. Real reports obviously contain more aviation-specific data. On the other hand, this illustrates that many concepts in safety reporting are not specific to the aviation domain.

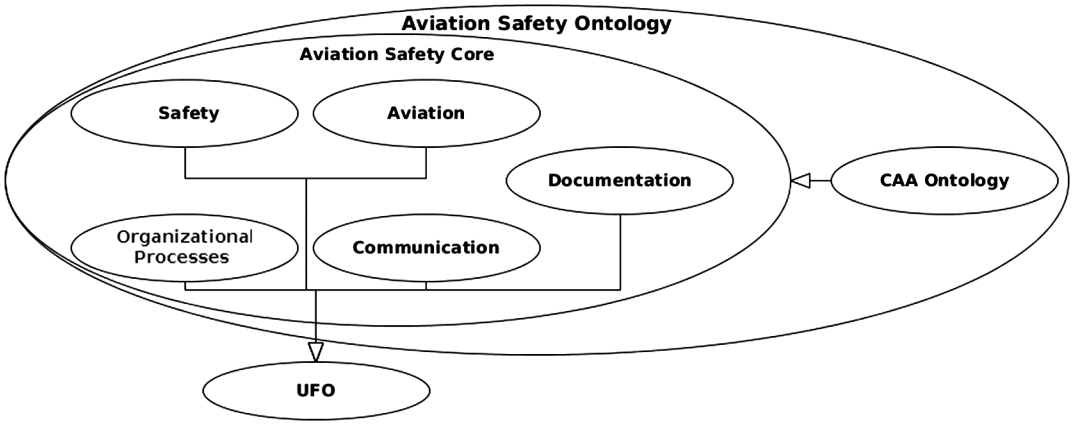


Fig. 4 Overall structure of the aviation safety ontology. Its submodules are related to particular areas.

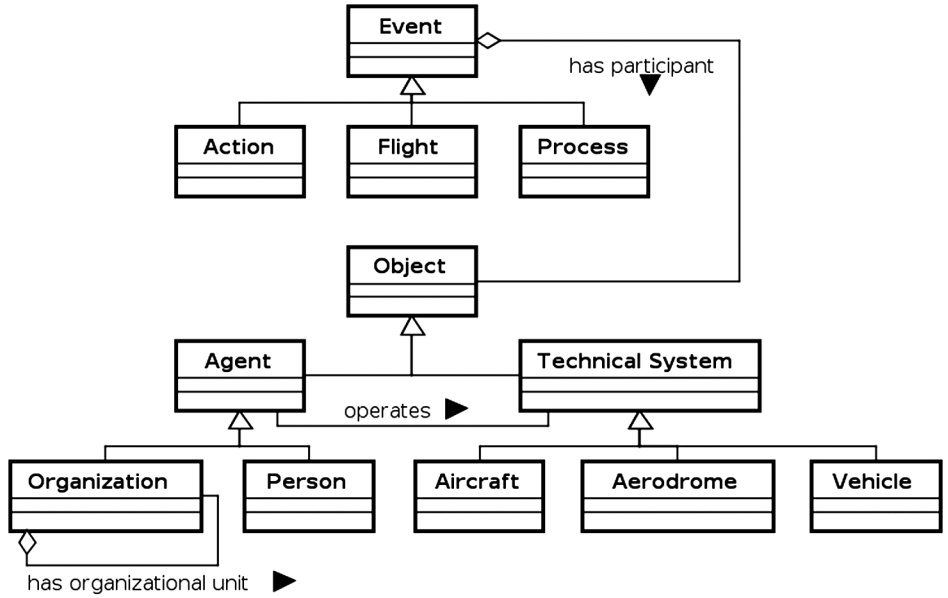


Fig. 5 Unified modeling language visualization of an excerpt from the aviation ontology. Event and Object are classes corresponding to the UFO types with the same names.

b. Documentation Ontology. Documentation ontology [41] is a generic model of documents and reports. It specifies various types of *records* that *document entities*: for example, events or objects from the aviation ontology. It also defines the structure of *questions* and *answers*, which are closely related to the generated forms that will be discussed later. A simplified example of the documentation ontology is shown in Fig. 6. The *documents*

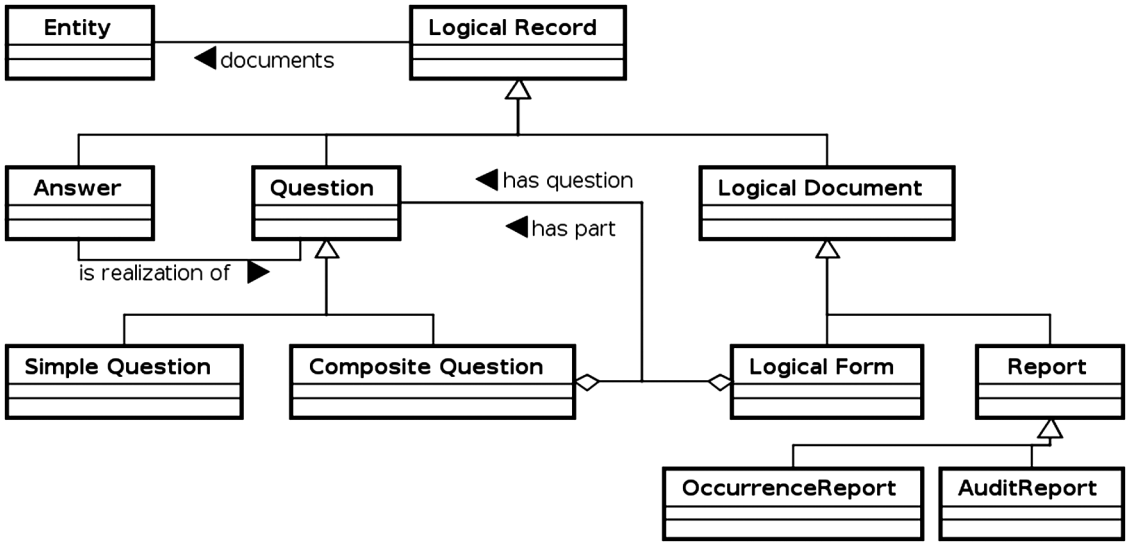


Fig. 6 UML visualization of a documentation ontology sample.

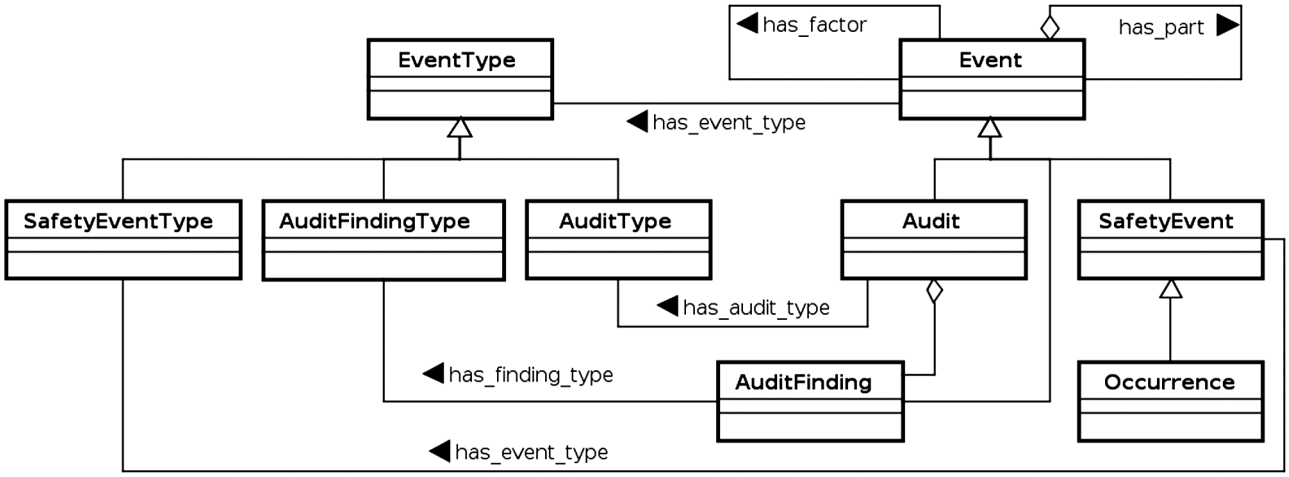


Fig. 7 UML visualization of an excerpt from the safety ontology. Event is a UFO class.

property connects the documentation ontology to the aviation and safety ontologies because its value can be from either of them. The report example in Fig. 2 shows that a *report documents* an *occurrence*. It also contains a *severity assessment* of the occurrence and *a question–answer* tree.

c. Safety Ontology. Safety ontology [40] conceptualizes the fundamentals of safety data management. In this research, safety deals with the flight risks of aircraft and property damage or the loss of lives. It does not concern, for example, financial risks. An excerpt from the safety ontology in Fig. 7 shows how reactive safety (*Occurrence, SafetyEvent*) can be integrated with proactive safety (*Audit, AuditFinding*) by being based on the UFO *event* class. It can also be seen that events may consist of subevents and have other events as *factors*. The *has_factor* relationship has subtypes (not shown in the diagram): for instance, *is_caused_by, is_mitigated_by.* The *EventType* hierarchy allows distinguishing types of different kinds of events so that, e.g., an *Occurrence* cannot be assigned an *AuditType*. A graph of events connected via the *has_part* and *has_factor* relationships is called a factor chain (which will be further discussed in the next section) and can be used to analyze event patterns. In the example report (Fig. 2), the *Occurrence* class belongs to the safety ontology. It contains five subevents, where event-1 is a *factor* (a *cause*) of event-2; and event-0-a, event-0-b, and event-0-c are *factors* of event-1.

d. CAA Ontology. CAA ontology defines the internal organizational structure of the CAA, i.e., its departments and person roles, which are used, for example, when assigning responsibilities for report investigation. The CAA ontology is not the only application extension of the aviation safety core. Kostov et al. [37] also showed extensions for air traffic management, aerodromes, airlines, and maintenance organizations.

Another area in which ontologies help with data integration is dealing with the variety of safety report formats. As Fig. 3 shows, there exist ECCAIRS-compliant E5X and E5F file formats (ZIP archives containing XML files) for occurrence reports. E5X is suitable for data exchange, and E5F is used for internal storage of the data. Unfortunately, these two formats are not fully compatible. Moreover, some of the reporters provide only E5X files, and others provide only E5F. Some organizations even send reports in PDF or HTML. Similarly, the CAA receives audit reports from the European-wide ramp inspection program (SAFA/SACA [42]). These reports are in Excel files. Reports of audits performed by the Czech CAA auditors are usually Word files based on several templates. To overcome the issue of so many different input file types, mappings to the ASO were created for all of them. As a result, there are models of various input formats, e.g., an ontological model of the E5X format. When an E5X report is received, it is transformed into an RDF form corresponding to the E5X ontological model. The system uses a mapping (mostly in the form of SPARQL Update statements), which transforms data from the E5X ontological model to the main occurrence report model of the aviation safety ontology. The same approach is taken for other kinds of reports.

2. *Contributory Factors of Events*

The approach described in this paper allows expressing the chain of factors, which lead to an event. For instance, when a runway incursion occurs, it is rarely a self-contained event with no contributory factors. A misunderstanding between the pilot and the air traffic controller may have caused the incursion. Similarly, in Fig. 2, a *loss of lifting conditions* (event-1) *caused* the *aircraft crash* (event-2). It is necessary to be able to formalize these relationships because patterns may emerge from such structures. An analysis of these patterns can lead to proactive solutions.

As an additional feature, the contributory factors in the scope of this work are not limited to what went wrong (the so-called Safety-I perspective). This reflects the recent shift in understanding of safety, namely, the introduction of the Safety-II approach [43]. This approach focuses on what went right and how respective events helped the course of deviations to avoid undesired consequences, in essence, linked to the resilience engineering [44]. To this end, the approach in this paper allows expressing a positive relationship between contributory factors and the outcome: the so-called *mitigation*. In this sense, we can say, for instance, that *training* (event-0) *mitigated* the *loss of lifting conditions* (event-1) using the aforementioned example, meaning that the loss was not as significant due to a timely reaction of a well-trained crew.

Similarly, when a safety audit reveals issues in an organization, these audit findings may also have factors. As an example, a frequent problem is the tight scheduling of flight crews to maximize their productivity. This scheduling may violate standards and eventually lead to crew fatigue or reduced situational awareness. In the end, we have a *loss of lifting conditions* (event-1) with three contributory factors: *flight crew staffing and scheduling* (event-0-a), *fatigue* (event-0-b), and *situational awareness* (event-0-c), as shown in Fig. 2. The event-0-a may be identified or confirmed during an audit, creating a logical link between audit and occurrence reports. Figure 8 shows such a simple audit report, with a1 representing an audit-specific vocabulary used by the CAA and event-0-a marked in bold, demonstrating the integration with occurrence report factors.

The aviation authority can, based on an analysis of these factors, provide recommendations to other organizations in order to avoid recurrence of the same problem.

3. *Taxonomy and Vocabularies*

Whenever possible, users of an information system are provided with options to choose from. The main reason for such a strategy is, besides user convenience, easier machine processing of the entered data. For example, the system does not have to deal with various date formats if the user

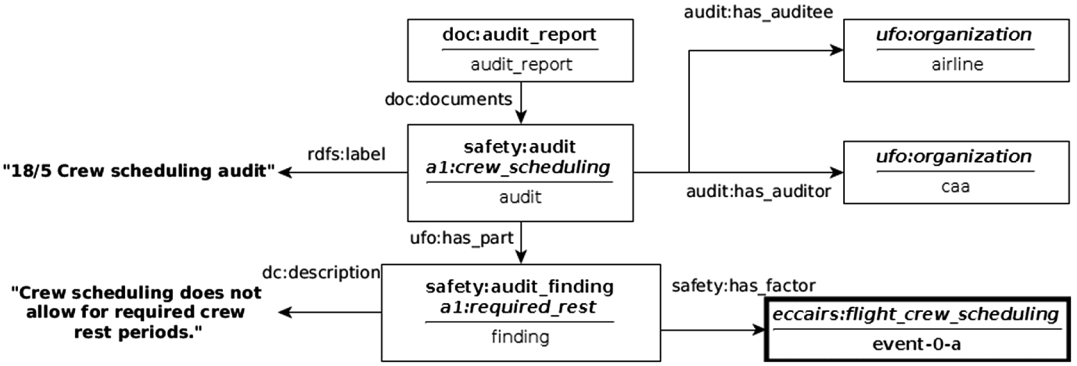


Fig. 8 Visualization of an audit report example.

chooses from a date picker. The aviation safety domain is no exception to this rule; value lists exist for occurrence severity, types of events, and many others. In Europe, these lists are provided through the ECCAIRS and RIT taxonomies. However, as shown in Ref. [6], value lists in the ECCAIRS are hard to use and sometimes even incorrect. Therefore, some of these value lists and the entire ECCAIRS the taxonomies were transformed into ontologies as part of the research on which this paper is based. This allows, for instance, building of a natural hierarchy of event types, in which the user can navigate from more general event types, such as *runway incursion*, to specific types like *runway incursion by a person* or *runway incursion by a vehicle*. Another example of how the ontology-based taxonomy resolves issues of the original ECCAIRS taxonomy is term disambiguation. For instance, the ECCAIRS defines the terms *loss of separation* and *separation minima infringement*, which represent the same event type. An ontology allows us to specify them as being the same so that statistics and other parts of the systems can treat them as such.

In addition to building a clearer terminology, ontologies can also smoothly evolve via ontological versioning [45]. With a versioned vocabulary or model, users are able to use older revisions if necessary because they coexist in the storage and can be distinguished.

Unfortunately, due to license restrictions, we could not publish the transformed ECCAIRS taxonomy directly. However, it is described in Ref. [6] and can be viewed online using the "Aviation Vocabulary Explorer" [46]. Besides all ECCAIRS terms, the transformed vocabularies also contain terms from RIT, ICAO, the air traffic management (ATM) lexicon,[¶] the Aviation ontology, Toolkit for ATM Occurrence Investigation (TOKAI)[***] and several more to maximize the SDCPS applicability and support for data/information exchange

The report in Fig. 2 uses several ECCAIRS terms: the severity assessment value originates in an ECCAIRS value list, and the occurrence and its subevents are classified using this taxonomy.

4. *Improved Input Methods*

Given the breadth and depth of the ECCAIRS taxonomy, it is no surprise that reporting systems based on it are difficult to use. This is arguably one of the main reasons for the reporting culture limitations in the aviation domain. Users are discouraged by the complexity of the systems (e.g., the EU *Aviation Safety Reporting* [7]), and they enter only the minimal amount of information required.

One of the important steps toward making the data gathering less painful for users is more structured and precise taxonomies. Another step is to move the SDCPS toward context-based dynamic forms. Based on the choices the user makes, it is possible to modify the form they fill to ask only for relevant information. Consider a form describing events: when the user selects an event type, the system is able to modify the form so that it contains only fields relevant to the given event type. As an instance, for the event type *runway incursion*, the user can fill in information about the runway on which the event occurred. However, such information is irrelevant for an event of type of *loss of separation*, which occurs in the air. This often significantly reduces the size of the form.

In our case, the dynamic forms framework is, again, grounded in ontologies. The forms are represented by ontological models. As the user fills in data, the form model undergoes transformations that filter out irrelevant fields, restrict value list options, and provide validators for the user's input. After the user fills in the form, the dynamic forms framework generates an updated form that is then presented to the user. However, the shape of the form may radically change at runtime as the user works with it. To be able to process such data and avoid huge classes accounting for every possible choice the user may make, the forms are transformed into a tree of questions and answers. To put it simply, each input field in the form represents a question, and its value is the answer. Form sections are represented by answerless questions.

The report in Fig. 2 illustrates this, due to space restrictions, on a single question–answer pair under a question representing the form root. Question–answer trees tend to have dozens of questions. In addition, the question is related to the original form model element it represents via the *has_question_origin* property. This connection is necessary so that the form generator (discussed in Sec. IV) is able to reconstruct the form.

IV. System Design

The overall architecture of the researched SDCPS is depicted in Fig. 9. As the declarative part of the system was already discussed, this section continues with a description of the application modules. The reporting tool is the primary user-facing module of the SDCPS; it integrates the output of other modules: the form generator, which creates dynamic forms; and the analytical module, which provides statistics from the data.

A. Reporting Tool

The reporting tool (RT) allows users to create new reports or import them from different sources. It contains a connector to the ECCAIRS and an Internet Message Access Protocol (IMAP) connector for report retrieval from an e-mail box. The IMAP connector is especially important because the Czech CAA receives the majority of reports via a dedicated e-mail box. Both connectors translate imported data to the RDF (using an appropriate model, e.g., E5XModel) and then map them to the primary ontological model represented by the ASO using the declared transformations (e.g., E5XtoASO). Reports created in the RT are stored directly using the ASO schema. The RT supports three kinds of reports: occurrence reports, audit reports, and safety issues.

[¶]"EUROCONTROL ATM Lexicon (online database)," EUROCONTROL, Brussels, http://www.eurocontrol.int/lexicon/ [retrieved 09 Nov. 2017].

[***]"Toolkit for ATM Occurrence Investigation (TOKAI)," EUROCONTROL, Brussels, http://www.eurocontrol.int/services/tokai [retrieved 09 Nov. 2017].

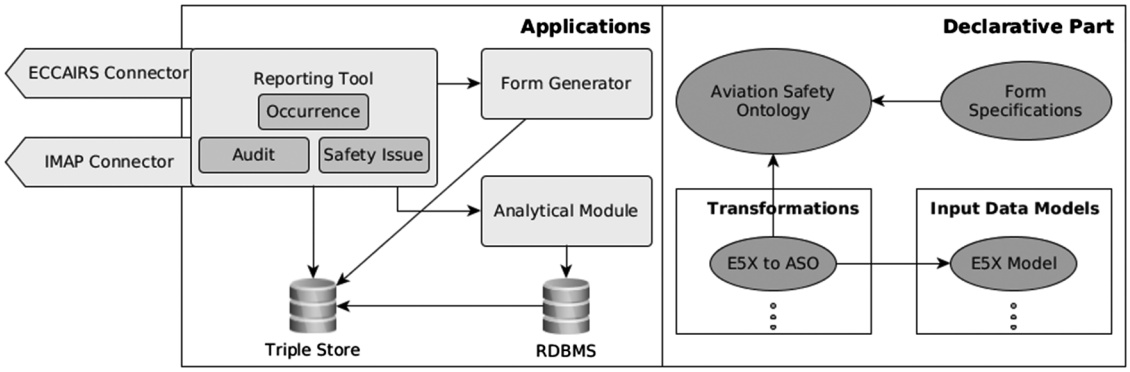


Fig. 9 Overall architecture of the researched system. Arrows represent usage dependencies.

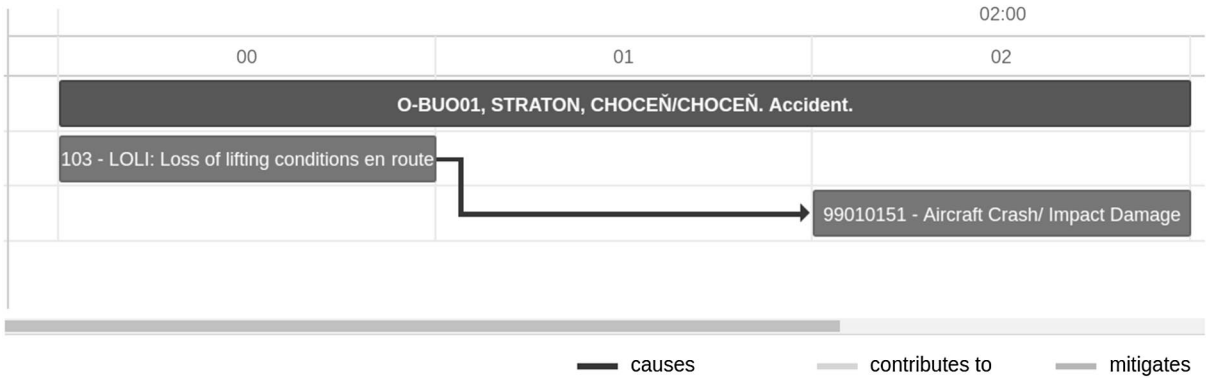


Fig. 10 Visualization of the occurrence from Fig. 2, along with its subevents, connected with the causal relationship.

1. Occurrence Reports

Occurrence reports are the main data source of the system. A distinctive feature of the RT is that it allows users to model chains of factors involved in the occurrence. Factors denote events that were part of the occurrence. The system also recognizes their relationships: for instance, causality or mitigation. Figure 10 shows an example of the factor graph editor in the RT.

2. Audit Reports

Audit reports allow users to enter the results of audits performed by safety inspectors. There are two main sources of audit reports identified at the Czech CAA: safety audits performed in organizations by the CAA employees, and ramp inspection audits performed by auditors of foreign aviation authorities on aircraft of operators overseen by the Czech CAA. Each audit report can contain zero or more audit findings, which specify the discovered problems. Statistics from the audit reports can help the inspectors focus future audits on areas of greater concern.

3. Safety Issues

Safety issues represent problematic patterns discovered in the data. These are, for example, repeatedly occurring factor configurations in occurrence reports or frequent audit findings. Safety issues represent a proactive approach to safety, in which users search for patterns with the potential to increase the risk of safety occurrences and want to keep track of them. A safety issue can be created based on an audit finding or an occurrence report. Further reports can then be classified as matching an existing safety issue, and a factor chain can be modeled as part of a safety issue.

B. Form Generator

Dynamic forms are provided by a separate module: the form generator. It generates event description forms using the user's input as a parameter. The principle is that there exists a model of the complete form, which contains all the possible attributes. Upon request, the form generator runs a transformation pipeline for which the inputs are the default form model, the selected event type, and possibly an existing question–answer tree (when the form has been filled in before). Then, based on expert knowledge encoded as SPARQL-based rules and inference upon the ASO, it filters out irrelevant fields and prepares queries for value lists. For instance, as was already mentioned in Sec. III.B.4, it will filter out attributes concerning runway if the type of the event is *loss of separation*, which takes place in the air. The resulting form model is eventually returned to the client in SON-LD (JavaScript Object Notation for Linked Data). A generator then renders the actual form. The process is illustrated in Fig. 11.

C. Analytical Module

The analytical module provides users with statistics generated based on the data managed by the RT. The module uses Pentaho [47] as the analytical platform. Because Pentaho uses a relational database [relational database management system (RDBMS)], data from the RT, stored in a triple store, are exported to the RDBMS on a daily basis. They are transformed into a suitable relational schema, and analytical queries are applied to them. Pentaho then provides various statistics, e.g., reports classified by occurrence category or severity, trends in the number of reported occurrences, or filtering by time intervals or operators.

V. System Evaluation

The system evaluation is provided from three points of view. First, existing reporting systems in general, including commercial SMS solutions, are considered. However, they are not an exact match for the developed system because they capture more than an SDCPS (typically the entire SMS, i.e., safety policies, risk management, hazard analysis, various communication channels, etc.) and their target customers are aviation

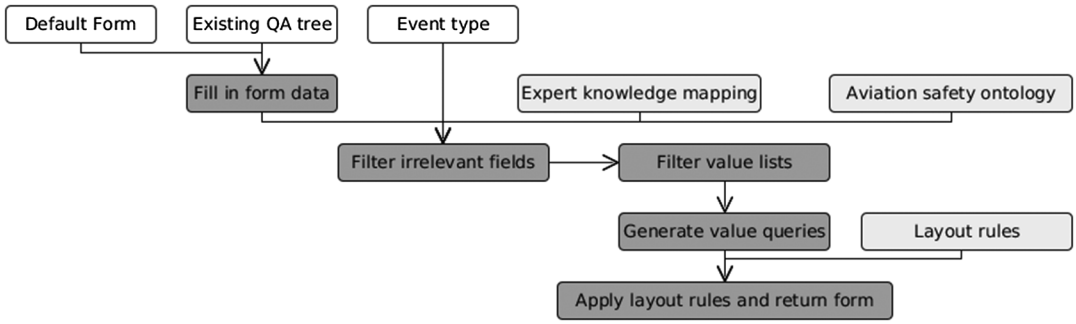


Fig. 11 Event-type specific form generation. White and light-gray boxes are physical artifacts; and dark boxes represent operations.

organizations instead of civil aviation authorities. Second, the developed system is compared with the ECCAIRS, which is a core safety data management solution used by European aviation authorities and the closest match for the developed SDCPS in terms of target functionality and audience. Third, experience with its practical deployment is discussed.

A. Domain-Oriented Evaluation

When comparing the developed system with the mandatory occurrence reporting systems available (Sec. II), the difference becomes clear at first glance. When opening the tool, domain users (safety inspectors or other safety management staff) are not burdened with long lists of data fields. Initially, the form asks for basic contextual information such as headline, occurrence date, and location, classification, and aircraft information (if relevant); then, it follows with a factor chain designer. This encourages the user to provide the core of the information needed, i.e., to model what happened and how it happened. To exemplify the simplicity, an empty occurrence report is depicted in Fig. 12.

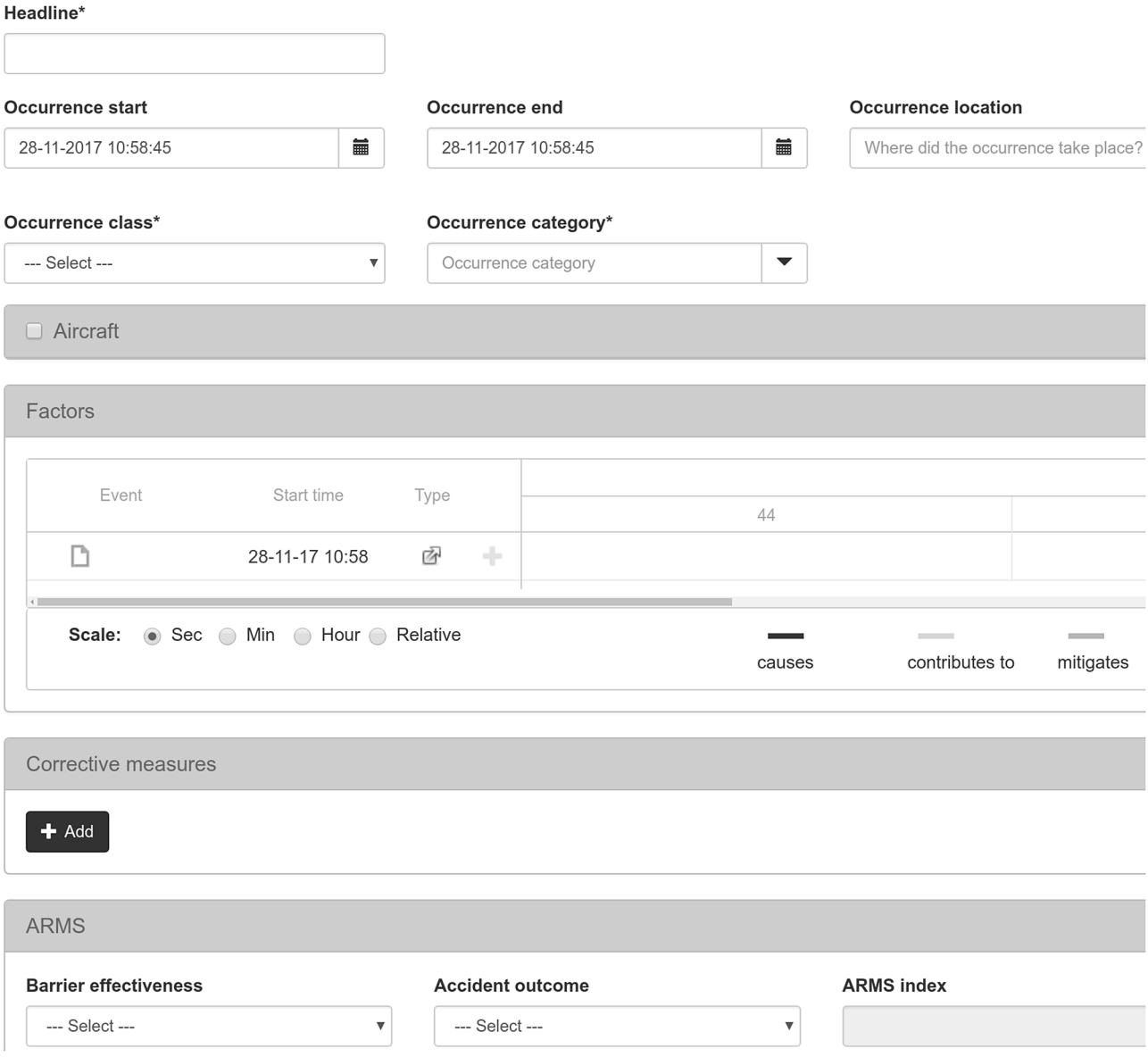


Fig. 12 An empty occurrence report as displayed by the developed SDCPS.

Once the user fills and models the relevant event types and contributory factors involved in the occurrence, it is possible to fill in other data fields. The form filters and displays only fields relevant to the event types and contributory factors declared in the chain designer. This dynamics surpasses any of the features introduced by the discussed reporting systems or commercially available safety management solutions, reducing the user workload, room for error, or information omission. From the perspective of an SDCPS, this implies a significant improvement of data quality.

Because of integration based on the ASO, the information and analytics are provided in an enhanced way, especially due to improved data consistency. The SDCPS can accommodate any vocabulary or taxonomy by mapping it to the ASO; for the CAA, this is beneficial because they collect reports from all stakeholders in the area of their responsibility and, at the same time, correlate them with data available from safety audits. The integration allows such correlation using contributory factors. This feature is unparalleled; there is no satisfactory integration of safety audits and occurrence reports available to date with consistent knowledge derivation. This is especially important concerning safety performance indicators (in terms of both Safety-I and Safety-II; see Refs. [44,48–50]); for support of which, there are safety issue reports available, capturing the formalized knowledge.

Comparing the researched SDCPS with commercially available solutions, it cannot substitute any of those listed in Sec. II. The SDCPS is normally an SMS module, and the researched SDCPS can thus substitute only a part of the listed solutions. However, as per the evaluation in Sec. II, the researched system performs better with regard to safety data collection and processing. There are no similar features mentioned or demonstrated by any of the commercially available software. However, it is true that none of these systems is designed for CAAs, despite some clear overlaps.

Table 3 summarizes how the presented SDCPS conforms to the features discussed in Sec. II.

B. Comparison to ECCAIRS

The target users of both the ECCAIRS and the developed SDCPS are mainly European aviation authorities. European legislation requires national authorities to use the ECCAIRS to manage mandatory safety occurrence reports and send them to the European central repository [4]. In the following, the ECCAIRS and the developed SDCPS are compared in terms of functionality and user experience. The comparison is then summarized in Table 4.

1. Data Integration

The ECCAIRS concentrates on safety occurrence reporting, whereas the developed SDCPS has a broader scope. It integrates occurrence and audit reports to provide a more comprehensive view of safety. Users are also able to create safety issues to track patterns of interest.

2. Factor Chains

The ECCAIRS allows specifying child events of an occurrence. However, this does not fully allow users to model the chain of events involved in the occurrence. The developed SDCPS enables the creation of a part-of hierarchy of events and to interconnect them to express additional relationships such as causality or mitigation.

3. Taxonomy

The issues of the ECCAIRS taxonomy were already addressed in Ref. [6] and in Sec III.B.3. The formal facilities of ontologies make the developed system's taxonomy arguably cleaner and easier to use. The system also supports other taxonomies, including TOKAI, the ATM

Table 3 Conformance of the presented SDCPS to the features discussed in Sec. II

Feature	Researched SDCPS	Comment
Taxonomy management	✓	Ontology versioning
External taxonomies usage	✓	ICAO, ATM Lexicon, TOKAI, ASO
Custom controlled vocabulary	✓	
Modeling of event/contributory factors chains	✓	
Adaptive occurrence report forms	✓	
Adaptive audit report forms	✓	
Event chain analysis	✓	Analytical module
Integrating knowledge from occurrence and audit reports	✓	
Compliant with European occurrence reporting scheme	✓	
Open data exchange formats	×	JSON via representational state transfer application programming interface only
Support for safety performance indicators/safety issues	✓	

Table 4 Summary of the feature comparison between the ECCAIRS and the newly developed SDCPS[a]

Feature	ECCAIRS	Newly developed SDCPS
Data sources/integration	Occurrence	Occurrence, audit, safety issue
Input data formats	E5X, native	E5X/E5F, SAFA/SACA excel, native
Input forms	Predefined, event-type agnostic	Generated, event-type specific
Factor modeling	Child events	Event hierarchy, factor chains
Taxonomy	Own (extensible)	Own (extensible), ICAO, ATM Lexicon, TOKAI, ASO
Access type	Desktop, web application	Web application
Analytics	User-defined queries + visualization	Predefined, filterable visualization

[a]Native input data format represents data directly entered by the user.

lexicon, and the ICAO taxonomy, as well as adding new taxonomies. Both the ECCAIRS and the developed SDCPS allow taxonomies to evolve. However, ontological versioning allows us to better express the changes. For example, it is not possible to formalize a change of meaning of a term in the ECCAIRS. In an ontology, terms can be related using, e.g., the *sameAs* and *differentFrom* relationships.

4. User Interaction

The ECCAIRS consists of a number of desktop applications (a web server can be configured to allow remote access as well), one of which is a data browser. This browser works similarly to visual database editors like pgAdmin [51], i.e., one has to first query the database to view reports. The user is then able to edit the records via a form with multiple views. However, as is the case with the online reporting application [7], the views are event-type agnostics, often showing input fields irrelevant to the particular event type. The SDCPS presented in this paper is a web application. It provides the user with a filterable and sortable table of reports. The report detail window allows the user to view and edit the report data in two distinct views. One is the general occurrence information, which is common to all occurrence reports. The other is the event-specific generated form, which contains fields relevant to the selected event type.

5. Analytics

The ECCAIRS allows users to define queries to retrieve data that can be visualized using a built-in chart module. The developed SDCPS contains a predefined business intelligence solution that enables users to filter the results using various criteria (year, organization, etc.). More important, the system also integrates audit data, making the statistics more comprehensive.

C. Deployment Experience

The developed system has been deployed at the Civil Aviation Authority of the Czech Republic, where it is currently used at the division of commercial aviation. The system has about 10 regular users: mostly members of the Safety Action Group (a working group of professionals with different aviation backgrounds who need to decide upon the reaction of the CAA to respective occurrences) who access the dashboards and overall statistics as the output of the system. Two users create/update records in the system. As of September 2018, it contains over 3500 occurrence and audit reports and multiple safety issue definitions. The system is used on a daily basis.

Several functional and usage problems have surfaced during the system's deployment time. First, because organization audits are handled by a different department, the audit module is actually not used to create audit reports. Only the incoming SAFA/SACA audit reports are used for data integration. The organizational processes that deal with reports are more complex than expected, making the set of possible states a report can have in the developed SDCPS insufficient. This, for example, means that multiple users cannot create revisions of the same report without interfering with each other's work. An organizational and data audit is planned at the CAA, and its results will be used to define a more robust report management process. The users also find the predefined outputs of the analytical module limited and prefer the module to be more configurable; for example, the length of the reporting period was set to last 30 days, with no configuration option. The users also miss an additional way of classification: a tagging system allowing them to group reports. The consequence is the inability to filter reports based on more specific criteria. For instance, one of the users needed an overview of aircraft laser attacks in 2017. However, because *laser attack* is not an occurrence category in the ECCAIRS, the system could not filter these reports, and a more generic *security-related* category had to be used instead. Another issue regards mostly the quality of incoming data; aircraft operator names are often misspelled, and the system is not able to map them to existing operator records.

D. System Limitations

The limitations of the described system were given by the real aviation environment and the requirement to produce an ECCAIRS-compatible solution. Instead of a full focus on ontology exploitation, it was necessary to transform and process the ECCAIRS taxonomy and the European regulatory framework in the first place and map them to the ontological model. This was reflected by the generated forms, which bore some limitations in their dynamics, displaying many data fields with respect to several event types. Due to various operational requirements, including compatibility with the ECCAIRS and a limited project execution time, it was impossible to develop own practical and useful ontology-based vocabulary for both occurrence and audit reports that would 23 adequately reflect modern safety engineering principles [52]. Another limitation existed with regard to the analytical module. Due to the lack of experience with safety data visualization and the insufficient quality of historical safety data, the module displayed only basic statistics of occurrences per severity, flight phase, risk index, etc. The risk index was calculated using the Aviation Risk Management Solutions [53] methodology, and the system only recorded its key parameters. As such, the methodology was found sufficient for the needs of the Czech CAA, and there were no plans to revise it.

VI. Conclusions

The developed system represents a prototype solution for building a data-driven safety management based on well-founded taxonomies used for integration of heterogeneous data. While initially created for the aviation industry, its applicability extends to other high-risk industries as well. The factor-based safety methodology sketched in this work has been worked on as part of other research projects. Their results should eventually be implemented into the system. The Czech civil aviation authoritie also plans to use the developed safety data collection and processing system (SDCPS) in the future, adding users from other departments so that its data integration capabilities can be exploited to a greater extent.

It is planned that the presented safety data collection and processing system will be integrated with another enterprise-level SDCPS developed for Czech aviation organizations in order to build a fully operational safety management environment on the national as well as enterprise levels. The aforementioned limitations provide additional motivation for long-term work that shall include more extensive ontology utilization and advanced visualization of safety data. Developing these solutions further will lead to building competitive modules for available safety management solutions at all levels in the aviation industry, eventually opening new ways to control safety.

Acknowledgments

This work was supported by grant no. GA 16-09713S (Efficient Exploration of Linked Data Cloud) of the Grant Agency of the Czech Republic, no. SGS16/229/OHK3/3T/13 (Supporting Ontological Data Quality in Information Systems), and no. SGS16/188/OHK2/2T/16 (Safety Performance Time Series Analysis and Evaluation Model at the Air Navigation Service Providers) of the Czech Technical University in Prague. We thank Vladimír Nekvasil from the Czech Civil Aviation Authority for his help with the safety data collection and processing system features survey among the European aviation authorities. We also thank Slobodan Stojić for his aid in the research of safety management systems and Leoš Zavřel for his feedback on the system description.

References

[1] Socha, V., Socha, L., Szabo, S., Hana, K., Gazda, J., Kimlickova, M., Vajdova, I., Madoran, A., Hanakova, L., Nemec, V., et al., "Training of Pilots Using Flight Simulator and its Impact on Piloting Precision," *Proceedings of the 20th International Scientific Conference Transport Means 2016*, Kaunas Univ. of Technology Press, Kaunas, Lithuania, 2016, pp. 374–379.

[2] International Civil Aviation Organization (ICAO), "Accident/Incident Data Reporting (ADREP) Taxonomy," April 2013, https://www.icao.int/safety/airnavigation/AIG/Pages/ADREP-Taxonomies.aspx [accessed 17 April 2018].

[3] *Safety Management Manual (SMM)*, International Civil Aviation Organization Doc. 9859 AN/474, 3rd ed., Montreal, 2013.

[4] "Regulation (EU) No 376/2014 of the European Parliament and of the Council on the Reporting, Analysis and Follow-Up of Occurrences in Civil Aviation," *Official Journal of the European Union*, Vol. L122, No. 18, 2014, pp. 18–43

[5] "Commission Implementing Regulation (EU) 2015/1018 Laying Down a List Classifying Occurrences in Civil Aviation to be Mandatorily Reported According to Regulation (EU) No 376/2014 of the European Parliament and of the Council," *Official Journal of the European Union*, Vol. L163, No. 1, 2015, pp. 1–17

[6] Křemen, P., Kostov, B., Blaško, M., Ahmad, J., Plos, V., Lališ, A., Stojić, S., and Vittek, P., "Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems," *Journal of Aerospace Information Systems*, Vol. 14, No. 5, 2017, pp. 279–292. doi:10.2514/1.I010441

[7] "Aviation Safety Reporting (online database)," European Aviation Safety Agency, http://www.aviationreporting.eu/ [retrieved 08 Sept. 2018].

[8] "ASRS–Aviation Safety Reporting System," (online database), NASA, https://asrs.arc.nasa.gov/ [retrieved 09 Nov. 2017].

[9] Rolls-Royce Controls and Data Services, "Safety Management System Solution for Civil Aero," https://www.controlsdata.com/civil-aero/safety-management-system-solution [retrieved 09 Nov. 2017].

[10] European Aviation Safety Agency, *Annual Safety Review 2017*, Cologne, Germany, 2017. doi:10.2822/26228

[11] Gruber, T. R., "Toward Principles for the Design of Ontologies Used for Knowledge Sharing," *International Journal of Human-Computer Studies*, Vol. 43, Nos. 5–6, Dec. 1995, pp. 907–928. doi:10.1006/ijhc.1995.1081

[12] Donnelly, K., "SNOMED-CT: The Advanced Terminology and Coding System for eHealth," *Studies in Health Technology and Informatics*, Vol. 121, 2006, pp. 279–290.

[13] Chen, D., Asplund, F., Östberg, K., Brezhniev, E., and Kharchenko, V., "Towards an Ontology-Based Approach to Safety Management in Cooperative Intelligent Transportation Systems," Springer International, Cham, Switzerland, 2015, pp. 107–115.

[14] Runciman, W. B., Baker, G. R., Michel, P., Dovey, S., Lilford, R. J., Jensen, N., Flin, R., Weeks, W. B., Lewalle, P., Larizgoitia, I., et al., "Tracing the Foundations of a Conceptual Framework for a Patient Safety Ontology," *Quality and Safety in Health Care*, Vol. 19, No. 6, 2010, Paper e56.

[15] Garst, W. J., Jr., "Mind Games: The Ontology of Aviation Safety and Its Consequences," Ph.D. Thesis, Virginia Polytechnic Inst. and State Univ., Blacksburg, VA, 2009.

[16] Keller, R. M., "Ontologies for Aviation Data Management," *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, IEEE, New York, 2016, pp. 1–9. doi:10.1109/DASC.2016.7777971

[17] Denney, E., and Pai, G., "Towards an Ontological Basis for Aviation Safety Cases," SGT/NASA Ames Research Center, Aug. 2015, https://www.faa.gov/air_traffic/technology/swim/governance/service_semantics/media/Safety%20Cases.pdf [accessed 31 Oct. 2018].

[18] Carvalho, R., Wolfe, S., Berrios, D., and Williams, J., "Ontology Development and Evolution in the Accident Investigation Domain," *2005 IEEE Aerospace Conference*, IEEE Publ., Piscataway, NJ, March 2005, pp. 1–8.

[19] Carvalho, R. E., Williams, J., Sturken, I., Keller, R., and Panontin, T., "Investigation Organizer: the Development and Testing of a Web-Based Tool to Support Mishap Investigations," *2005 IEEE Aerospace Conference*, IEEE Publ., Piscataway, NJ, March 2005, pp. 89–98.

[20] "Multi-User Investigation Organizer" (online database), NASA Ames Research Center, Mountain View, CA, https://technology.nasa.gov/patent/TOP2-150 [retrieved 17 April 2018].

[21] Kossmann, M., Gillies, A., Odeh, M., and Watts, S., "Ontology-Driven Requirements Engineering with Reference to the Aerospace Industry," *2009 Second International Conference on the Applications of Digital Information and Web Technologies*, IEEE, New York, Aug. 2009, pp. 95–103. doi:10.1109/ICADIWT.2009.5273953

[22] Gyawali, B., Shimorina, A., Gardent, C., Cruz-Lara, S., and Mahfoudh, M., "Mapping Natural Language to Description Logic," *The Semantic Web*, edited by E Blomqvist, D. Maynard, A. Gangemi, R. Hoekstra, P. Hitzler, and O. Hartig, Springer International, Cologne, Germany, 2017, pp. 273–288.

[23] Angele, J., Kifer, M., and Lausen, G., *Ontologies in F-Logic*, Springer, Berlin, 2009, pp. 45–70.

[24] "INBAS Project" (online database), Knowledge-Based Software Systems Group, Faculty of Electrical Engineering Czech Technical Univ., Prague, https://www.inbas.cz [retrieved 09 Nov. 2017].

[25] Berners-Lee, T., Hendler, J., and Lassila, O., "The Semantic Web," *Scientific American*, Vol. 284, No. 5, 2001, pp. 34–43. doi:10.1038/scientificamerican0501-34

[26] Harris, S., and Seaborne, A. (eds.), "SPARQL 1.1 Query Language," W3C Recommendation, W3C, 2013, https://www.w3.org/TR/sparql11-query/ [accessed 31 Oct. 2018].

[27] Křemen, P., and Sirin, E., "SPARQL-DL Implementation Experience," *Proceedings of the Fourth OWLED Workshop on OWL: Experiences and Directions*, Vol. 496, edited by K. Clark, and P. F. Patel-Schneider, CEUR-WS.org, Aachen, Germany, 2008, http://ceur-ws.org/Vol-496/owled2008dc_paper_10.pdf [retrieved 2018].

[28] Gearon, P., Passant, A., and Polleres, A., "SPARQL 1.1 Update," *W3C Recommendation*, Vol. 21, W3C, 2013, https://www.w3.org/TR/sparql11-update/ [accessed 31 Oct. 2018].

[29] Wood, D., Zaidman, M., Ruth, L., and Hausenblas, M., *Linked Data*, 1st ed., Manning Publ., Greenwich, CT, 2014.

[30] Baader, F., Calvanese, D., McGuinness, D. L., Nardi, D., and Patel-Schneider, P. F., *The Description Logic Handbook: Theory, Implementation and Applications*, 2nd ed., Cambridge Univ. Press, New York, 2010.

[31] Beckett, D., Berners-Lee, T., Prud'hommeaux, E., and Carothers, G., "RDF 1.1 Turtle," W3C Recommendation, W3C, 2014, https://www.w3.org/TR/turtle/ [retrieved 08 Aug. 2017].

[32] Brickley, D., and Guha, R. V., "RDF Schema 1.1," *W3C Recommendation*, W3C, 2014.

[33] Bechhofer, S., Van Harmelen, F., Hendler, J., Horrocks, I., McGuinness, D. L., Patel-Schneider, P. F., and Stein, L. A., "OWL Web Ontology Language," *W3C Recommendation*, W3C, 2004.

[34] Motik, B., Parsia, B., and Patel-Schneider, P. F., "OWL 2 Web Ontology Language Structural Specification and Functional-Style Syntax," *W3C Recommendation*, W3C, 2009.

[35] Cyganiak, R., Wood, D., and Lanthaler, M., "RDF 1.1 Concepts and Abstract Syntax," W3C Recommendation, W3C, 2014.

[36] "Průvodní Formulář k Předběžné a Závěrečné Zprávě | UZPLN" (online database), Air Accidents Investigation Inst., Prague, (in Czech) http://www.uzpln.cz/incident/506 [retrieved 09 Nov. 2017].

[37] Kostov, B., Ahmad, J., and Křemen, P., "Towards Ontology-Based Safety Information Management in the Aviation Industry," *On the Move to Meaningful Internet Systems: OTM 2016 Workshops: Confederated International Workshops*, edited by I. Ciuciu, C. Debruyne, H. Panetto, G. Weichhart, P. Bollen, A. Fensel, and M. E. Vidal, Springer International, Cham, Switzerland, 2017, pp. 242–251.

[38] Guizzardi, G., "Ontological Foundations for Structural Conceptual Models," Ph.D. Thesis, Univ. of Twente, Enschede, The Netherlands, 2005.

[39] Mascardi, V., Cordì, V., and Rosso, P., "A Comparison of Upper Ontologies. In: WOA 2007: Dagli Oggetti Agli Agenti," *8th AI*IA/TABOO Joint Workshop "From Objects to Agents": Agents and Industry: Technological Applications of Software Agents*, Seneca Edizioni, Torino, Italy, Sept. 2007, pp. 55–64.

[40] "Aviation Safety Ontology," "INBAS Project" (online database), Knowledge-Based Software Systems Group, Faculty of Electrical Engineering Czech Technical Univ., Prague, https://www.inbas.cz/aviation-safety-ontology [retrieved 19 April 2018].
[41] "Documentation Ontology," "INBAS Project" (online database), Knowledge-Based Software Systems Group, Faculty of Electrical Engineering Czech Technical Univ., Prague, https://onto.fel.cvut.cz/ontologies/documentation [retrieved 01 Nov. 2018].
[42] "COMMISSION REGULATION (EU) No 965/2012 of 5 October 2012 Laying Down Technical Requirements and Administrative Procedures Related to Air Operations Pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council," *Official Journal of the European Union*, Vol. L296, No. 1, 2012, pp. 1–148.
[43] Hollnagel, E., *Safety-I and Safety-II: The Past and Future of Safety Management*, Ashgate, Farnham, England, U.K., 2014.
[44] Patriarca, R., Bergström, J., Gravio, G. D., and Costantino, F., "Resilience Engineering: Current Status of the Research and Future Challenges," *Safety Science*, Vol. 102, Feb. 2018, pp. 79–100.
doi:10.1016/j.ssci.2017.10.005
[45] Klein, M., and Fensel, D., "Ontology Versioning on the Semantic Web," *Proceedings of the First International Conference on Semantic Web Working, SWWS'01*, CEUR-WS.org, Aachen, Germany, 2001, pp. 75–91, https://pdfs.semanticscholar.org/417f/b1dd895a9416f9d56932e6b3870749ba582c.pdf [accessed 31 Oct. 2018].
[46] "Aviation Vocabulary Explorer," "INBAS Project" (online database), Knowledge-Based Software Systems Group, Faculty of Electrical Engineering Czech Technical Univ., Prague, https://www.inbas.cz/aviation-vocabulary-explorer [retrieved 09 Nov. 2017].
[47] "Pentaho" (online database), Hitachi Vantara, Santa Clara, CA, http://www.pentaho.com/ [retrieved 07 Sept. 2018].
[48] Mousavi, S. S., Cudney, E. A., and Trucco, P., "Towards a Framework for Steering Safety Performance: A Review of the Literature on Leading Indicators," *Advances in Intelligent Systems and Computing*, Springer International, Cham, Switzerland, June 2017, pp. 195–204.
[49] Walls, L., Revie, M., and Bedford, T., "Risk, Reliability and Safety: Innovating Theory and Practice," *Proceedings of ESREL 2016*, CRC Press, Boca Raton, FL, Sept. 2016.
[50] Pariès, J., and Wreathall, J., *Resilience Engineering in Practice: A Guidebook*, Ashgate Studies in Resilience Engineering, CRC Press, Boca Raton, FL, 2013.
[51] Page, D., "pgAdmin–PostgreSQL Tools (online database)," https://www.pgadmin.org/ [retrieved 09 Nov. 2017].
[52] Leveson, N. G., "Engineering a Safer World: Systems Thinking Applied to Safety," *Engineering Systems*, MIT Press, Cambridge, MA, 2012.
[53] Aviation Risk Management Solutions Working Group, "The ARMS Methodology for Operational Risk Assessment in Aviation Organisations," Aviation Risk Management Solutions (ARMS) Working Group, 2010, https://skybrary.aero/bookshelf/books/1141.pdf [accessed 31 Oct. 2018].

M. D. Davies
Associate Editor

Appendix I

HANÁKOVÁ, Lenka., Andrej LALIŠ, Bogdan KOSTOV, Markéta KAFKOVÁ, Jana AHMAD, Slobodan STOJIĆ and Katarína SZENTKERESZTIOVÁ. *Methodology for improving analysis and management of risk with the utilization of conceptual modeling*. Certified methodology by the Ministry of Transport, Czech Republic, 2019.

METHODOLOGY

for improving analysis and management of risk
with the utilization of conceptual modeling

Research project TA CR Zéta No. TJ01000377

Department of Air Transport Faculty of Transportation Sciences CTU in Prague	Department of Cybernetics Faculty of Electrical Engineering CTU in Prague	Prague Airport, Ltd.	Czech Airlines Technics, Ltd.
Hanáková Lenka, Ing. Lališ Andrej Ing., Ph.D. Stojić Slobodan Ing., Ph.D.	Ahmad Jana, Ing. Kostov Bogdan, Ing.	Kafková Markéta, Ing.	Szentkeresztiová Katarína, Ing.

T A Č R

Technology Agency of the Czech Republic

Program Zéta

Methodology for improving analysis and management of risk with the utilization of conceptual modeling

Contents

Introduction

Safety data collection, processing and analysis belongs to basic and essential functionalities of every safety management system [1,2]. In complex socio-technical systems, such as the aviation, it is rather impractical if not completely impossible that operational records of aviation organizations are stored in simple software tools developed e.g. using MS Excel or MS Access environment and, simultaneously, achieving data quality as required by current needs of operations and management, especially in the context of performance-oriented processes of safety management. In fact, even more advanced systems for safety data collection and processing often possess numerous inherent deficiencies and it is the very complexity of aviation operations, which practically disables complete and correct description of a controlled system or specific event. This leads to the safety analyst and his or her conceptualization influencing the content and form of safety records, so as the process of their creation and further management [3]. While there are efforts spent on standardization of procedures and content of safety data by means of legislation, various industrial standards or by development of aviation safety taxonomies, these are largely based on long-term experience with aviation operations and widely accepted models of safety such as SHELL or Reason's model [6], also known as the Swiss cheese model. Undoubtedly, all this verified experience allowed for current high level of aviation safety, but the theory of safety is being developed further and today there is already concrete vision for further progress in the domain [7].

The need for further improvement may seem not significant given the current aviation safety records, however, it is important to realize that the industry is also developing further and one of the aspects of the development is ever increasing complexity and interconnectedness of operations, which is manifested in our limited ability to predict aviation accidents and incidents. Further, is it possible to observe increasing pace of technology modification and innovation, often without opportunity to earn sufficient experience with particular system as the technology is modified or replaced earlier that such experience can be earned [8]. Finally yet importantly, there are new hazards emerging such as unmanned aerial vehicles or new types and modes of aircraft automation, all contributing to new relations among the flight operation participants. They can resonate across the entire industry and so contribute to new types of aircraft accidents and incidents. Under such conditions, it can hardly be claimed that current level of aviation safety is stable and also sustainable in the future with the utilization of current tools.

At present, there is opportunity for further development by utilizing available theory of safety, which is oriented to systemic approach to safety management and which attempts to grasp system-level phenomena of complexity, resonance and emergence [3,8,9]. This methodology builds upon one of the first systemic models of safety - model STAMP (System-Theoretic Accident Model and Processes) [8], developed at the MIT in the U.S. This model was carefully selected due to proximity of its focus and content to current state of safety management in the aviation and because it offers new possibilities for progress with no fundamental changes to understanding of safety issues. The methodology focuses on utilizing systems theory and STAMP with safety data collection and processing systems in the aviation. To achieve necessary practical applicability, the methodology uses modern technology of ontology engineering [10], which allows creation of technologically advanced systems for safety data collection and processing. This technology also allows creation and management of quality data and owing to its conceptualization grounding, it reduces the impact of individual interpretation of a safety analyst on the data quality.

1. Goal of the methodology

The methodology aims to disseminate the results of executed research project No. TJ01000377 by the Czech Technical University in Prague, in cooperation with Prague Airport and Czech Airlines Technics, funded by the Technology Agency of the Czech Republic. The methodology is a summary of knowledge resulting from project execution and it contains key procedures for introducing new functionalities for support of analysis and management of risks in the context of safety data collection and processing. The document aims to further improve the level of safety in the aviation, with some overlap regarding other high-risk industries.

2. Dedication

The methodology is primarily dedicated to middle-size and larger organizations in the aviation industry, which plan to implement or already possess a safety data collection and processing system, typically within their safety management system, and which want to extend it with the newest knowledge from safety theory. The methodology can be also applied in other high-risk industries such as nuclear power installations, chemical industry or in the military, as a support for detailed hazard identification and consequent increase of effectiveness and efficiency of analysis and management of risk, with the use of systemic approach to safety management. Even though the procedure described in this methodology is general, in case of application in other industrial branches, the methodology does not guarantee full correspondence to the specifications of these domains and possible modification should be considered.

3. Methodology description

This section contains core description of key procedures of the new safety data collection and analysis framework. The methodology provides for new technical means of how to realize safety data collection and processing systems compatible with other systems and technologies used in the aviation industry, and as such is primarily intended to be used by technical and engineering personnel supporting development and implementation of the systems. Because the methodology is based on theory of STAMP and its formal representation by means of developed STAMP ontology, the first subsection describes relevant theory and the ontology. Next subsection follows with detailed description of the procedure and principles of the new framework for safety data collection and processing.

3.1 Theory of STAMP [8]

STAMP (System-Theoretic Accident Model and Processes) is predictive model of safety. It is one of the first systemic models of safety, explaining safety as a control problem. The model works with basic assumption that each safety occurrence (accident or incident) bears some failure of the safety control structure in place, i.e. hierarchically organized socio-technical system in which people are organized into operational and managerial positions in interaction with various types of technology and which is proposed as active barrier preventing failure of risk systems, i.e. as a barrier preventing accidents and incidents. Apart from the very organization, work distribution, obligations and responsibilities, there is systemic aspect, i.e.

the need for managing interactions across the entire system. In such a system, the key is information distribution, first of all the feedback from controlled processes to safety control structure. Due to that, STAMP works with feedback control theory-based representation [11] of a socio-technical system and guides the safety analyst to depict relevant parts of a system of interest in line with the theory. The advantage of STAMP-based analyses is utilization of systemic approach to explain safety occurrences, which is in contrast to conventional explanation based on linear factor chain modeling, barrier modeling or descriptive statistics for identification of base trends in monitored occurrence types (i.e. safety performance indicators) [4]. Systemic view of processes guides the analyst to use schemas depicting system parts of interest to explain safety occurrences from the system-level, i.e. analyze why the system failed as a whole. By this, the theory of STAMP established foundation for preventive measures at the system level and not only at the level of individual contributory factors or events.

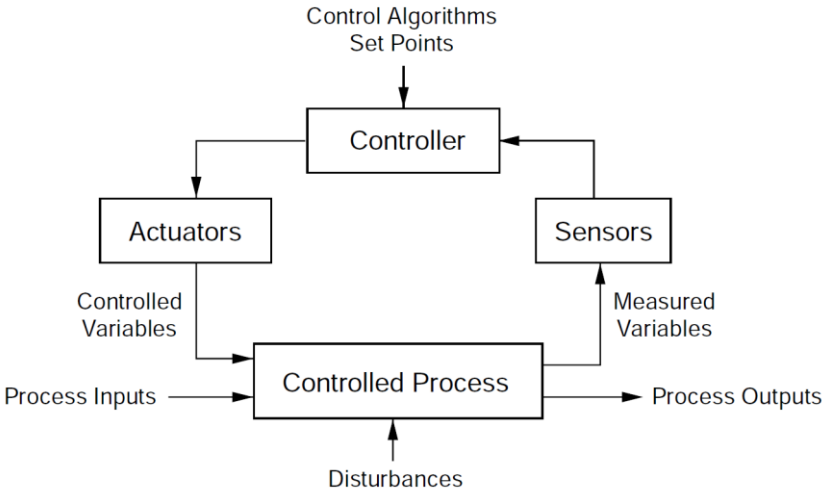


Fig. 1 Control loop based on feedback control theory [8]

As already mentioned, the core for executing STAMP-based analysis is description of system's part of interest in form of diagrams compatible with feedback control theory. The basic building block of such diagrams is a control loop depicted in Fig. 1. The figure shows all elements of a control loop - controlled process, sensors, controller and actuators. Controller can be human or automated. To enable controller to control a process, it is necessary that it has up-to-date information about the current state of the controlled process by means of sensors measuring state variables and also that there are actuators in the system, by means of which the controller controls the process, or more precisely influences specific state variables in the controlled process. The diagram in Fig. 1 can be extended or specified according to given context to progressively establish the entire socio-technical system representation. An example of socio-technical system with focus on safety-relevant processes is depicted in Fig. 2. The figure represents simplified hierarchy of feedback control loops without detailed description of actuators and sensors. As it is apparent from Fig. 2, the system description according to theory of STAMP is an object-based diagram.

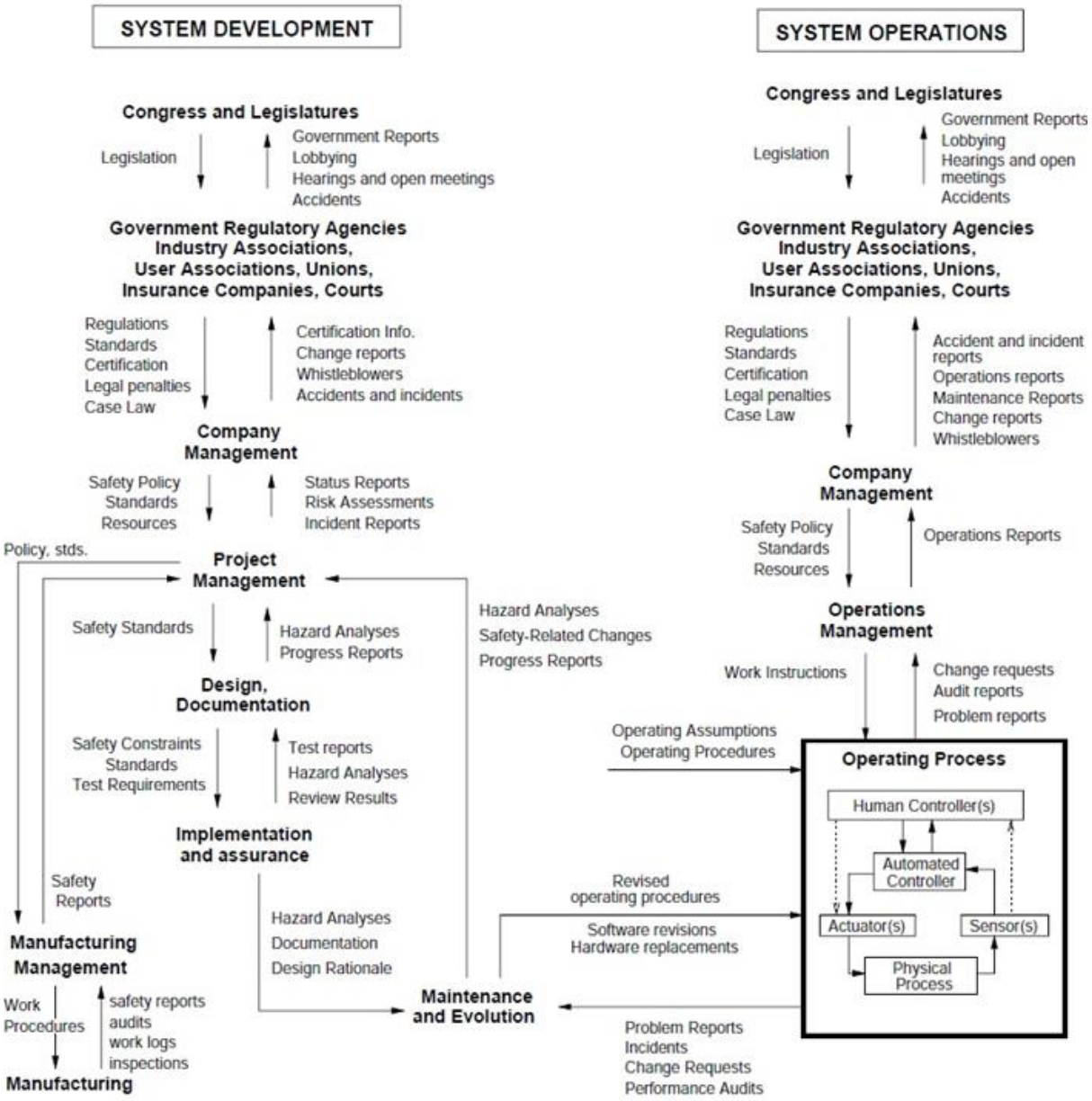


Fig. 2 Generic schema of a socio-technical system [8]

As a support to achieve completeness of safety analyses, the theory of STAMP offers generic taxonomy of all possible safety issues at the level of a control loop, according to Fig. 1. The taxonomy is depicted in Fig. 3 and for safety analyst it serves as a support tool for identification of contributory factors with respective safety occurrence report, or audit findings during typical process of safety data collection and processing. The taxonomy serves also identification of the complete list of hazards in the assessed system, however, this use case in out of the scope of this document.

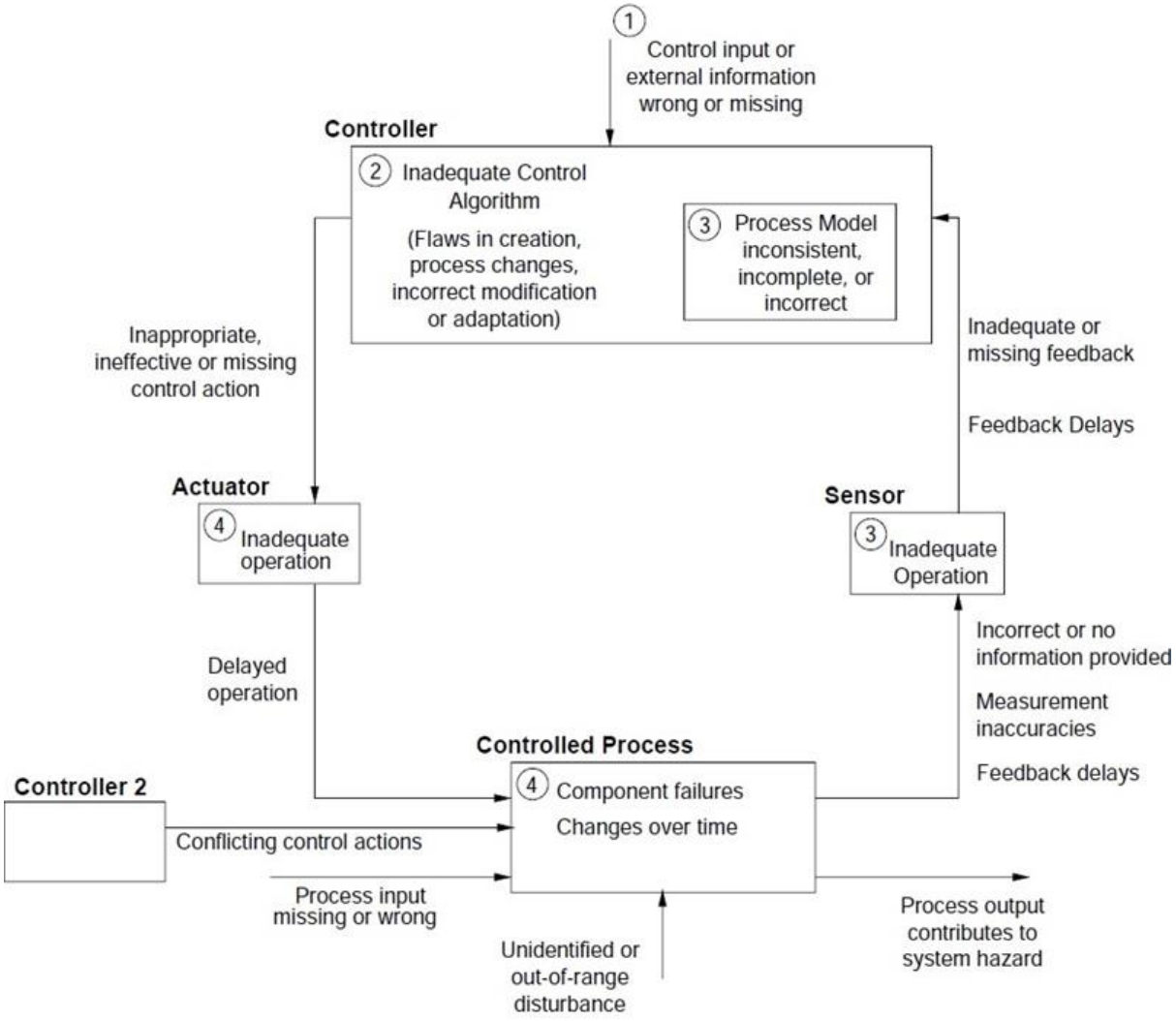


Fig. 3 Basic schema for identification of hazards and taxonomy of safety issues according to the theory of STAMP [8]

From the perspective of data collection and processing, the theory of STAMP offers support in form of CAST (Causal Analysis based on STAMP) methodology. This methodology is primarily dedicated to accident and incident investigation, its content however corresponds to key steps of usual data collection and processing in aviation, both from the perspective of data collection and processing about accidents and incidents, so as from the perspective of usual safety occurrence reporting with no significant impact on safety. The methodology consists of the following steps [8]:

1. Identification of the system(s) and hazard(s) involved in the loss
2. Identification of the system safety constraints and system requirements associated with the hazard
3. Documentation of the safety control structure in place to control the hazard and enforce safety constraint (diagram of feedback control loops)
4. Determination of proximate events leading to the loss
5. Analysis of the loss at the physical system level
6. Determination of how and why each successive higher level allowed or contributed to the inadequate control at the current level

7. Examination of the overall coordination and communication contributors to the loss
8. Determination of the dynamics and changes in the system and the safety control structure
9. Generation of recommendations

From the very steps of the CAST methodology it follows that the base is the documentation of object-based diagram (step 3) describing relevant part of the safety control structure, as per the example in Fig 2. The base for the documentation are steps 1 and 2 which help to narrow the selection of system parts of interest, which take part in the loss. From practical point of view, it is desirable that such a diagram contains only relevant parts of the evaluated system, because complete documentation of the entire system is usually impossible or greatly impractical.

The next steps of the CAST methodology (steps 4 and 5) are typical steps from the domain of accident and incident investigation. In case where safety data collection and processing pertains this type of occurrences, steps 4 and 5 can be executed with no change. If the situation involves an initial report, it may contain only general information which will be complemented during later stages of an investigation. In case where the subject of data collection and processing are data from regular occurrences from operation, which do not classify as accident or incident according to ICAO (International Civil Aviation Organization) standards [12], the steps 4 and 5 can be executed in simplified form, i.e. with no detailed identification of overall chain of events of the reported occurrence.

Steps 6, 7 and 8 of the CAST methodology are steps of systemic analysis, where the safety analyst is tasked to consider the evaluated system with respect to the processed safety data. These steps are innovative analytic steps based on STAMP, since in currently utilized safety data collection and processing systems in the aviation there is no need for correlation of safety data with documentation of a system, which generated the data; basic analysis by means of descriptive statistics to estimate trends and correlations suffice. In the CAST analysis, by contrast, such analysis is absent since analysis and interpretation of data with no system documentation provides insufficient support to propose targeted preventive measures. Correlation of safety data with system documentation, on the other hand, generates guidelines how the controlled system can be modified to be acceptably safe. It also offers base for better risk comprehension and subsequent prioritization of safety issues.

Step 9 concludes CAST methodology and it is typically step of any accident and incident investigation process. In case where the scope of interest are normal everyday occurrences from the operation, recommendations may not necessarily be drawn.

3.2 STAMP ontology

The key parts and aspects of the developed ontology are closely described in this section. The STAMP ontology was designed with two high-level requirements; first, to allow formally specifying statements about STAMP concepts and the relations among them, such as specifying statements about the control structure and the investigated loss as described in the CAST methodology. Second, the ontology was designed to support data integration with other information systems and methodologies.

The STAMP ontology is formalized using the OWL 2 language and aligned with the Unified Foundational Ontology (UFO). The ontology is available online[1].

Fig. 4 shows a fragment of UFO which represents a causal network using its object-event model. Events are characterized by their triggering situation and the situation that they bring about. *Actions* are a special kind of events which are *performed* by *Agents*, i.e. objects with a mental/internal state. *Situations* represent the state of objects and relations among them, e.g. the speed of the vehicle and the structural strength of the aircraft. *Situations* describe the state of affairs before and after the events occur. Apart from that, *situations* can *activate dispositions* of objects such as the structural strength of the aircraft fuselage. The activation of a disposition is manifested as an *event* which brings about a new *situation*. Note, that it is not necessary to describe every aspect of the UFO model in order to create a network. However, specifying additional information allows for automated reasoning according to UFOs formalization of events. For example, when describing causal networks, one can use the *causes* relation between events and the *performs* relation between agents and action events and omit/postpone the description of situations, dispositions and moments of objects.

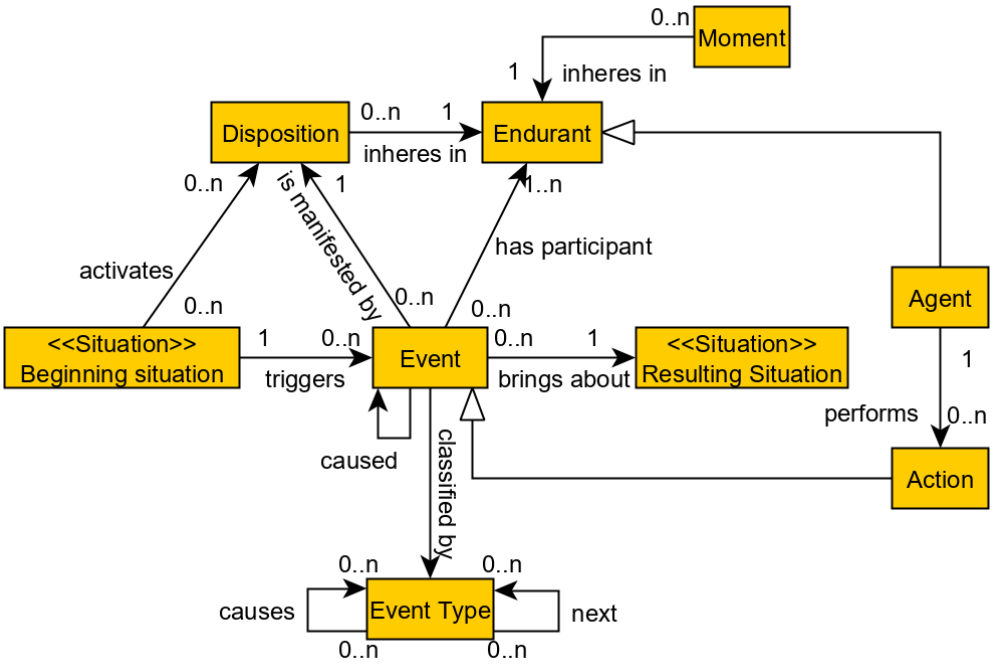


Fig. 4 Basic causal network of objects and events in UFO.

STAMP is based on several widely used conceptual models. The main model used in STAMP is the feedback control model. This model is used to specify the control structure. Apart from that STAMP refers to an object-event model, a causality model, a constraint model and a business process model. The object-event model is used to describe actual events, e.g. loss events in CAST and hypothetical loss event scenarios in STPA (Systems-Theoretic Process Analysis) methodology, even though STPA is out of the scope of this document. The causality models are used to represent the findings of the investigations of loss scenarios (both actual and hypothetical). A causality model typically captures a causal network of events, states and

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

object dispositions. In safety, this network leads to a loss event. Finally, business process models are used to represent behavioral patterns and constraints needed to avoid and or minimize losses.

We propose the use of a generic structure which allows to represent both the control structure and the structure of the controlled process, see Fig. 5a. A *Structure* is composed of several parts, here *Structure Elements*, specified using the “has-structure-element-part” relation in the ontology. There are two main types of Structure Elements, namely the *Structure Component* and relational element named *N-ary Structure Connection*. The *ufo:mediate*s relation specifies the components of which the connection is composed. The *Structure Connection* is a binary connection, a specialization of the N-ary connection, with two mediation relations, *from-structure-component* and *to-structure-component*. Fig. 5b shows the types of structures used in STAMP, i.e. the *Control Structure* and the *Process Structure*. Additionally, the ontology allows to specify the structure of structure elements. This allows describing elements in more detail, if necessary. As a result, this model is capable of capturing different views of the control structure where some control components are viewed in detail while others are not. Finally, Fig. 5c shows the different kinds of components (on the left) and connections (on the right) used to represent the control and the process structures.

STAMP specifies five key kinds of *Control Structure Components*, namely *Controller*, *Process Model*, *Algorithm (part of the Controller)*, *Sensor*, and *Actuator* but the list might be extended if necessary. Furthermore, STAMP specifies three types of connections, represented in the STAMP ontology as *Action Control Connection* (representing control by means of actuators), *Feedback Control Connection* (representing feedback connection with sensors) and *Information Control Connection (r*epresenting coordination and information links between *Controllers)*. A process structure is described in terms of the *Process* components, which can be connected with *Next Connection* (i.e. organized in a flow).

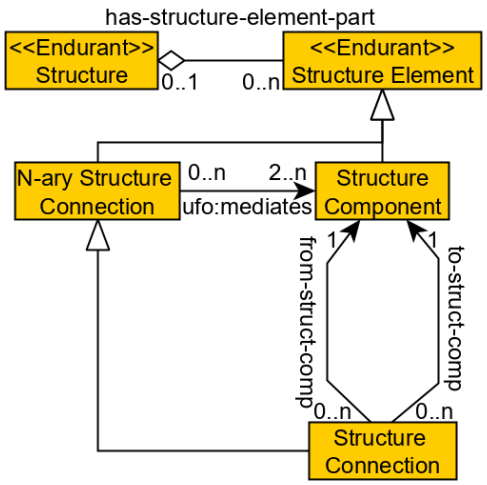


Fig. 5a STAMP Structure Model

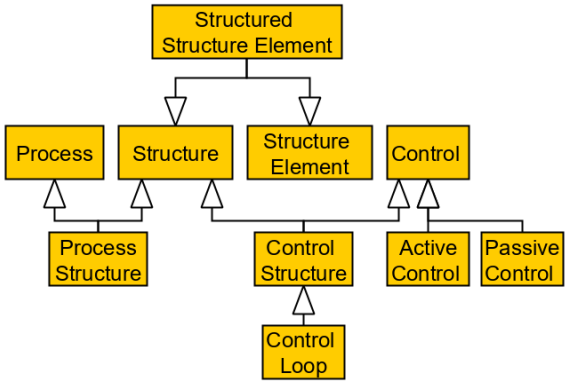


Fig. 5b STAMP Structure Taxonomy

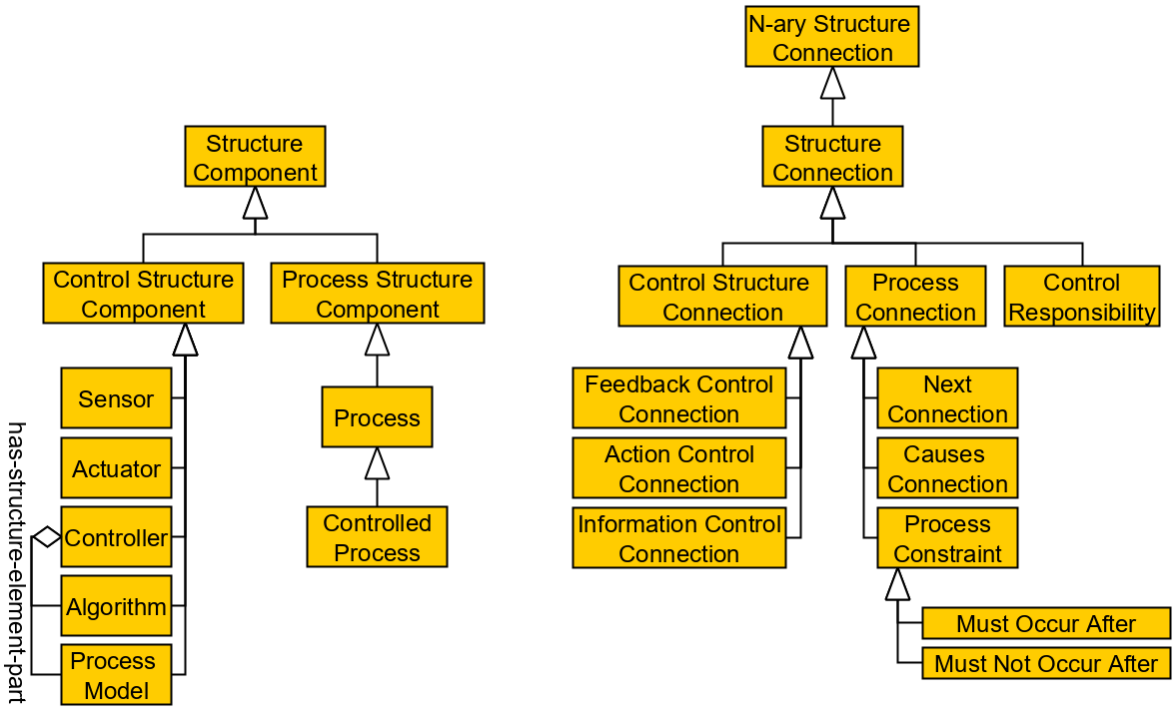


Fig. 5c Structure element taxonomy

The core of the ontology is visually depicted in Fig. 6. The central concept is *Controlled Process*, which usually consists of a task sequence and is described in typical operational documentation. In the context of a UFO ontology, this process is modeled as *Event Type*, where various objects and agents can *participate in*. The objects and agents are commonly modeled by means of *Substantial* concept (orange in Fig. 6). Further, the participant in the *Controlled Process* is a *Control*, which is modeled as specialization of the *Substantial* concept. *Control* is responsible to control certain *Variables* and it is an aggregate of objects and agents as per the theory of STAMP (i.e. organized controllers, sensors, actuators) which may change in time, but retain their identity. *Hazard* is considered as a capability or a property of objects and agents as well as their abilities or functions. However, STAMP defines the term hazard as a state. In the proposed ontology we use the term *Hazardous State* instead for such states to avoid terminology confusion. Hazards in the ontology are modeled as *Dispositions* which *inhere in Endurants* and are *manifested in Unwanted Events*, *violating* existing Safety *Constraints* as per the STAMP theory. Safety constraints are modeled as *Substantials* and their goal is to *mitigate* manifestation of *Hazards* in *Unwanted Events*. This is done by *constraining Variables*, which *describe* different aspects of the *Controlled Process.* Furthermore, *Variables* can be defined in terms of objects and events (not shown in the figure). For example, the variable “distance between the aircraft and a vehicle” can be modeled as a UFO formal relation between objects “aircraft” and “vehicle”. This and other similar ontology patterns aim at better definition of control and grasping quantifiable aspects of controlled processes, which in the context of STAMP theory are utilized as variables in the controlled process and which can be manipulated or measured. *Enforcing* of safety *constraints* is realized by the concept *Control*.

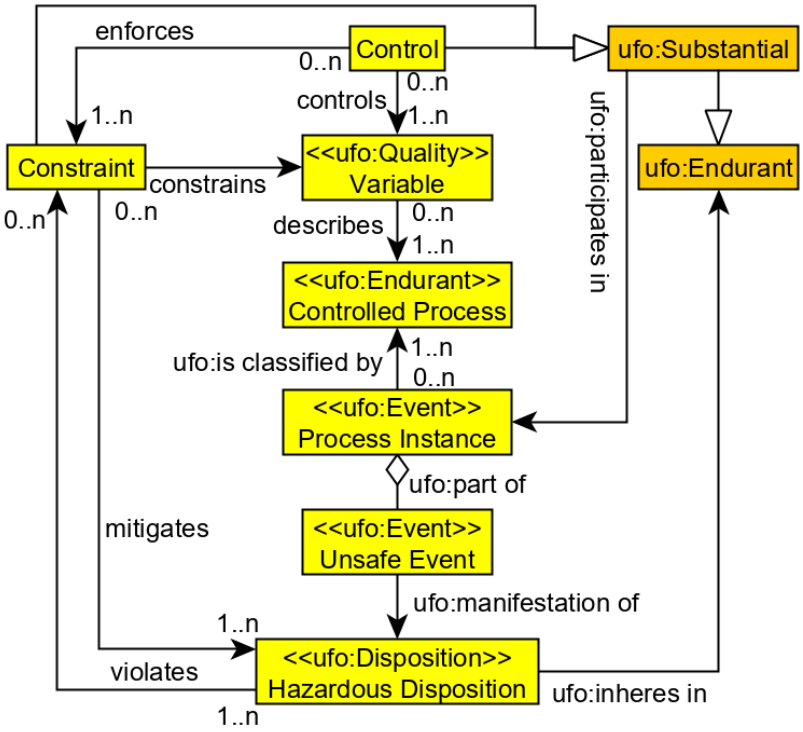


Fig. 6 The core of developed STAMP ontology

The next key part of the published ontology is description of events associated with the *Control Structure Components* from Fig. 5 and the *Controlled Process*, see Fig. 7. For example, a *Control* can be composed of a *Controller* and several *Sensors* and *Actuators*. Furthermore, the *Controlled Process* is modeled as consisting of several parts (events) which are the focus of interest in STAMP theory (hence the class *STAMP Event*) and which can be divided into events related to communication (*Communication Event*), control (*Control Action*), actuation (*Actuating Event*) and measurement (*Sensing Event*). The participants in these events are specified by means of *participates in* relation and also by relation *performs*, which ties the *Controller* with *Control Action*. For illustration and intelligibility, Appendix 1 to this document includes several specific examples about ontology application in the aviation industry.

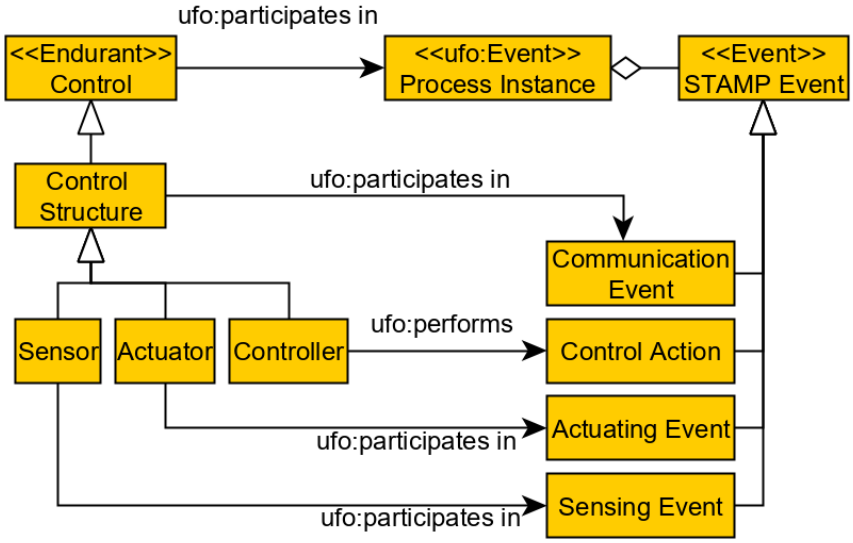


Fig. 7 Key concepts related to control as per the STAMP ontology

The STAMP model describes *Control Actions* and other control structure events such as controller's decision or sensors' operations. The STAMP ontology models this in terms of *Capabilities* (a specialization of the concept *Disposition*). Fig. 8 depicts the schema pattern to associate *Capabilities* with the *Control Structure Elements,* in this case the *Capabilities* of the *Control Connections.* The property used to represent this association is *has capability.* Fig. 9 shows how to specify a particular unsafe capability, the *Unsafe Action Capability* (unsafe control action in STAMP terminology). The schema allows to describe a capability from which the unsafe capability is derived, e.g. "unsafe brake capability" is derived from the "break capability". Also, the schema allows to specify the particular type of the *Unsafe Action Capability* according to STAMP, e.g. action "not provided" and action executed "too early" Furthermore, the schema allows to specify the hazardous state (*Hazardous State Type*) to which the capability potentially leads, the source, i.e. the *Control Component Controller* (e.g. the *Controller* who performed the action) and the *Context* (e.g. the process or activity during which the capability is unsafe).

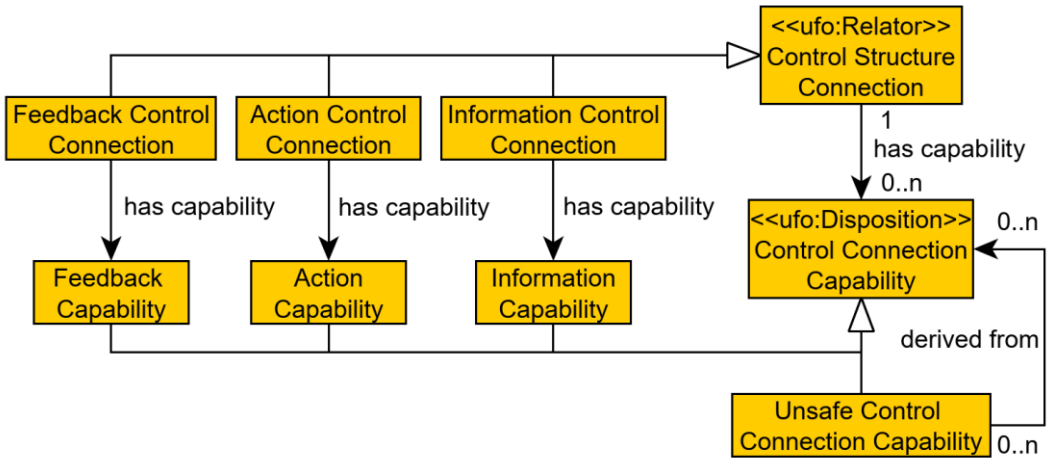


Fig. 8 Specifying *Capabilities* of a *Control Structure*

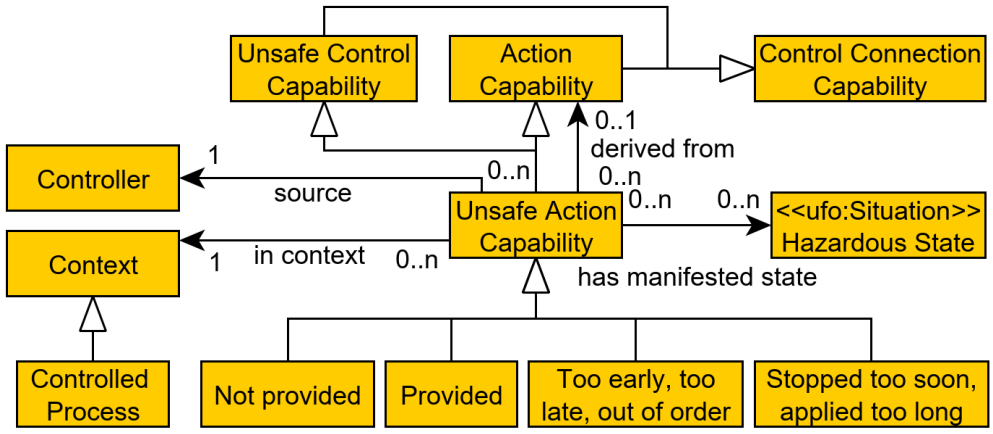


Fig. 9 Schema of *Unsafe Action Capability*

Finally STAMP requires to specify *Control Responsibility*, see Fig. 10. A *Controller* is associated with a *Control Responsibility* via the *has responsibility* relation. The responsibility *has goal* a *State Constraint* and is related to a *Process* by the *has plan* relation. This part explains that a controller is designed to take pre-defined measures with certain conditions

emerging to avoid unwanted events that could lead to a hazard, i.e. the *Controller enforces* the *State Constraint*. *State Constraint* and *Hazard State* reflect the safety constraints and hazards as used with the theory of STAMP.

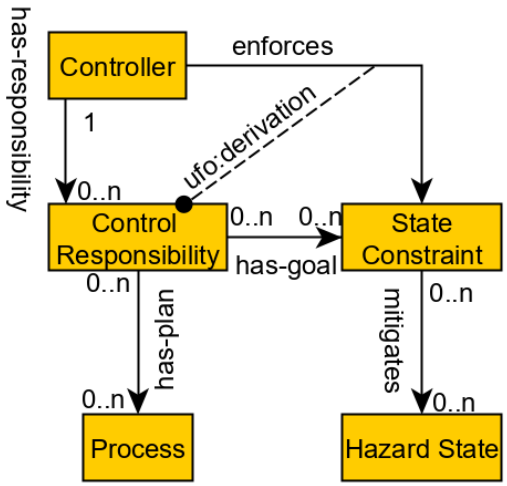


Fig. 10 Schema of *Control Responsibility*

3.3 Application of STAMP ontology

This part of the methodology describes utilization of the developed STAMP ontology in the context of safety data collection and processing.

3.3.1 Basic information about application

The process of ontology application is compatible with the theory of STAMP so as the CAST methodology, however, it brings new technical capabilities for storing data so as how to execute specific steps of the CAST methodology. The basic difference is ontological definition of STAMP theory concepts. This mostly influences the execution of step 3, i.e. documenting the safety control structure in place, which is now limited by the ontology according to its patterns. Because the ontology is machine-readable artefact, it does not require the documentation by means of object-oriented diagrams similar to the one in Fig. 2, even though such representation may be useful in some cases. The ontology allows mainly machine-readable documentation, which is normally stored in RDF (Resource Description Framework) format in a triple store (subject, predicate, object) such as RDF4J.

Realization of the machine-readable documentation of a safety control structure can be performed either directly with the utilization of the published ontology artefact (e.g. in Protégé[2] tool) or by implementation of the ontology into existing software environment used to support safety or documentation management in respective organization. Especially in the latter case there is the opportunity to implement it into an integrated management system, which usually includes several information necessary for STAMP-based analyses and which can be utilized for multiple purposes within a single system. It is especially convenient to use standard

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

process documentation, if there is one available, because it includes a basic description of processes, their participants so as distribution of responsibility. In case the process documentation is not available electronically, a solution is to utilize available business process modeling tools with the use of BPMN language (such as free open-source tool Modelio[3] or commercially available Adonis[4] or Bizagi Modeler[5] and similar). The created system description is then necessary to complement with additional information according to the published ontology, which produces documentation of safety control structure as per step 3 of CAST methodology and, at the same time, operationally exploitable artefact for normal business management. The only difference is that such safety control structure would be complete and not filtered to the particular accident or safety occurrence. On the other hand, by application of the methodology in combination with business process modeling, a synergy effect is achieved and so a unique opportunity to maintain complete and up-to-date description of a system, compatible with STAMP theory. This way it is possible to significantly simplify and expedite the process of safety data collection and processing based on STAMP. Step 3 of CAST methodology is eventually reduced to simple filtration of existing system description according to the scope of respective safety data processing, i.e. according to the output from steps 1 and 2 of the CAST methodology. Execution of initial steps (1 and 2) of CAST methodology then depends on the way of carrying step 3. If the step 3 is carried in form of integrated solution, then the filtration of existing documentation is performed in all three initial steps. If the STAMP ontology is applied as a stand-alone solution (e.g. with Protégé), then the documentation of safety control structure shall be performed each time safety data are collected and processed, as is usual with STAMP-based methodologies. Due to the mentioned reasons, it is therefore more advantageous to use the first option, i.e. filtration of an already existing artefact.

3.3.2 Ontology application on the CAST methodology

Documentation of the safety control structure as per step 3 of CAST methodology requires definition of control loops, control structure, controlled processes, constraints and all objects and relations, which are mutually connected and relevant to particular accident or safety occurrence. The base of STAMP is a control loop and Fig. 11 depicts an example of single control loop definition in line with the developed STAMP ontology. Specifically, the figure shows a *controller* - driver of conveyor belt vehicle for loading baggage into an aircraft, which controls the process of parking for baggage loading with a *sensor* measuring distance between the vehicle and aircraft. Apart from basic elements of the loop, in the ontology there is also support for definition of *variables*, which are controlled by the *controller* in the *controlled process*, here the distance and orientation between aircraft and vehicle (see Fig. 12). Figs. 13, 14 and 15 provide detailed description of parts of the control loop from Fig. 11 in terms of representing details of connection, objects and events relevant to the loop. Fig. 11 (so as all other figures in this section) are only an attempt to visualize result of data collection and processing by means of UML language, even though recording the data in RDF does not require any visualization. Stereotypes (names of classes in parentheses) correspond to types of objects according to the STAMP ontology.

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

After definition and modeling of control loops, it is necessary to determine distribution of control loops with respect to the controlled processes and safety constraints. The distribution is graphically represented in Fig. 16 where *control loops* are tied to specific *controlled processes* (with control-feedback relations) according to the process documentation and their task is to *enforce* specified safety *constraints*. The STAMP ontology provides that each safety *constraint* must be *enforced* by some *control loop*. Example is safety constraint - 1 from Fig. 16 which requires that the parking process of the conveyor belt cannot be initiated without parking coordinator and which is part of baggage loading process, specifically part of control loop CL12-CSP of parking coordinator. Certainly, it is possible and in practice rather usual, that one *control loop enforces* several safety *constraints* and also that one safety *constraint* can be enforced by several *control loops*. From the perspective of safety, however, it is unacceptable if some safety *constraint* is not enforced by any *control loop*.

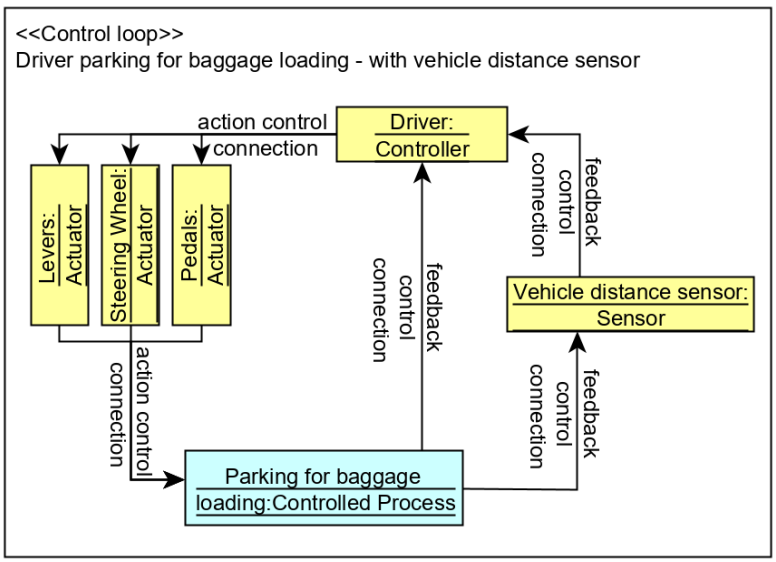


Fig. 11 Example of control loop modeling by means of STAMP ontology

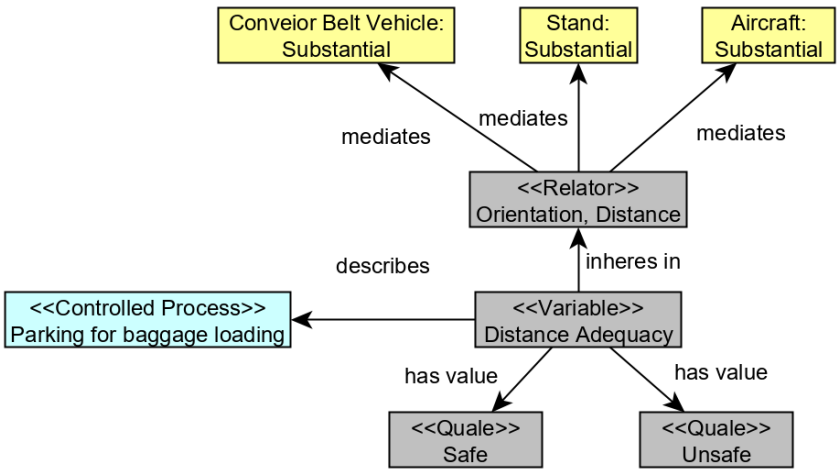


Fig. 12 Specification of control variables used to control the controlled process

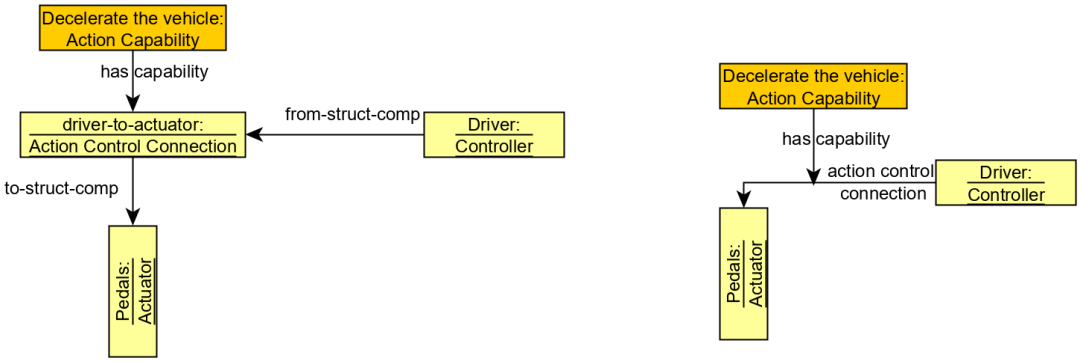


Fig.13 Notation used to represent of connections in the diagrams

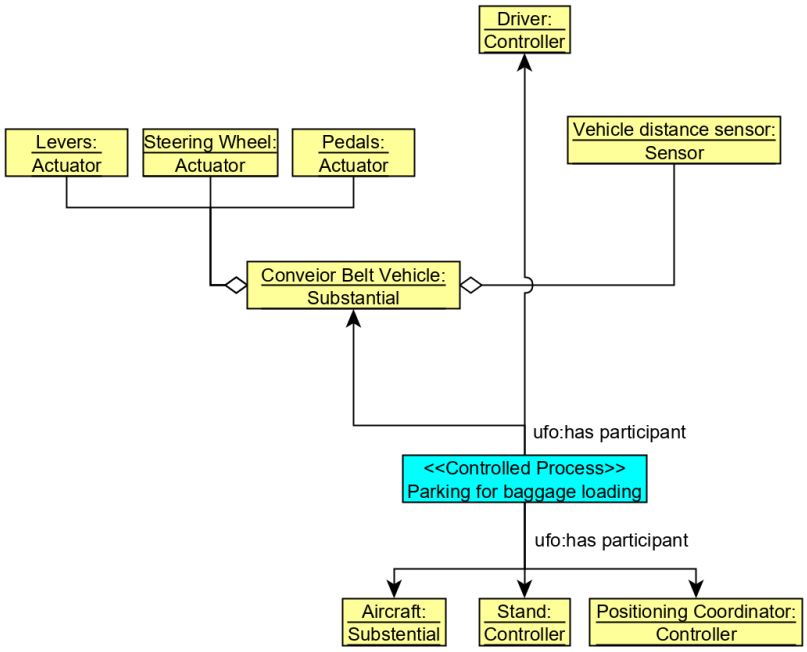


Fig. 14 Detailed specification of the objects referenced in the control loop

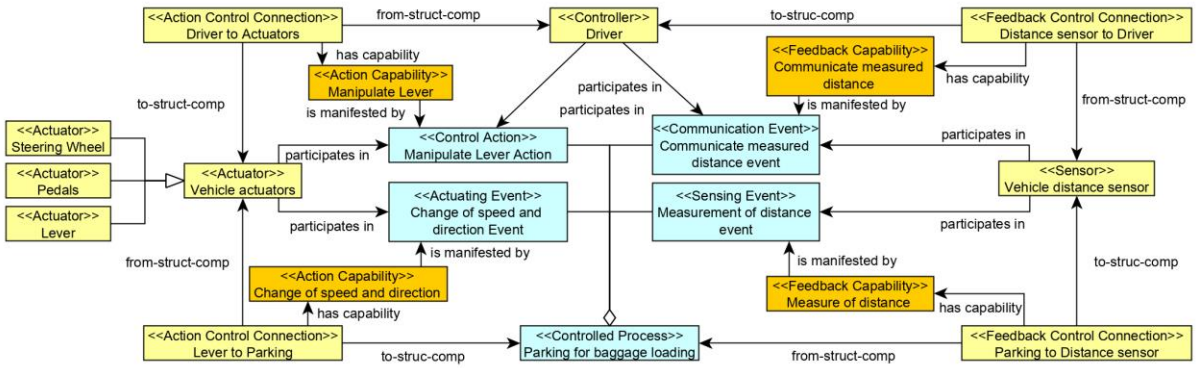


Fig. 15 Detailed specification of the events related to the control loop

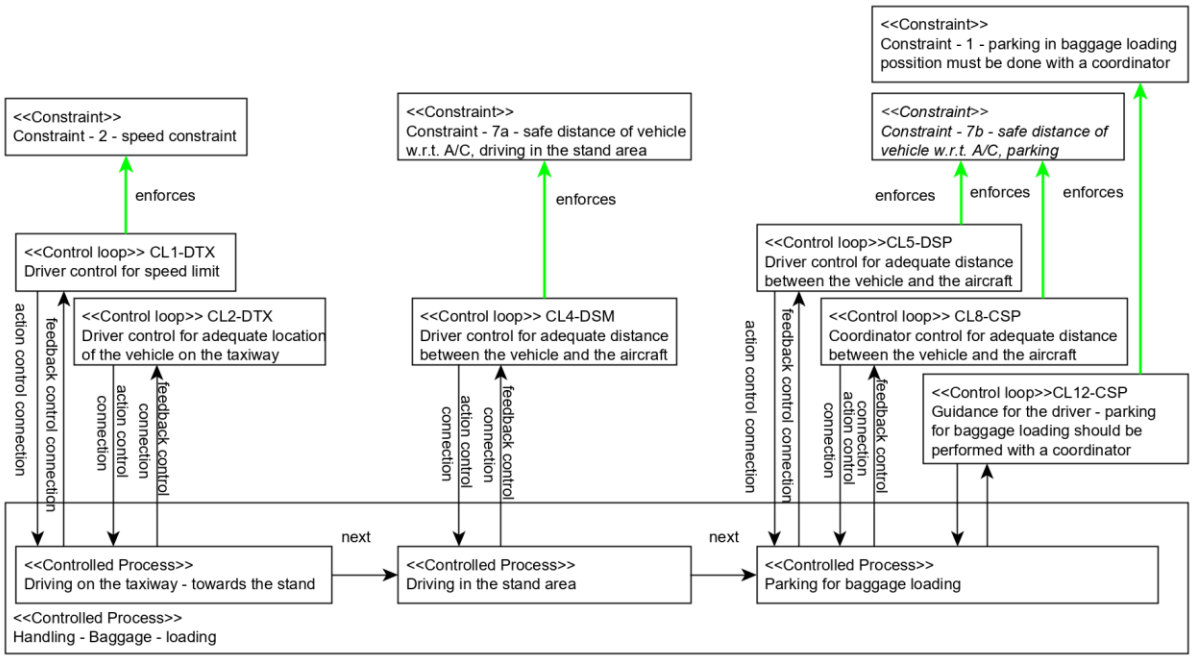


Fig. 16 Modeling of operational processes and their relations with safety constraint by means of STAMP ontology

Steps 4 and 5 of CAST methodology are supported by STAMP ontology in similar way as it is with steps 1, 2 and 3. Here, it is necessary not only to set a chain of events, as it is common with every investigation, but also to map this chain to the established documentation of safety control structure from step 3, i.e. in the context of schemas from Figs. 11-16. Fig. 17 in this respect shows an example of fictional occurrence where a collision occurred between the conveyor belt vehicle for baggage loading and an aircraft. The collision occurred during vehicle parking into position, from which it is possible to load baggage into an aircraft, by means of the conveyor belt. The vehicle driver wrongly estimated relative distance and position of the vehicle with respect to the aircraft and crashed with the conveyor belt into the aircraft fuselage, causing a damage. Contributing factors of this event were approach started without positioning coordinator, no feedback from positioning coordinator, driver's belief about situation not matching reality and inadequate vehicle movement. The event chain is depicted in magenta, documentation of safety control structure in yellow (objects), blue (events) and orange (capabilities), and the accident in red. Relations among magenta/red and orange elements shows mapping of the chain to the system description (documentation of the safety control structure).

After finishing the basic event description according to the example in Fig. 17, it is then necessary to define how and why each individual parts of a system contributed to inadequate control during the event, i.e. to execute step 6 of CAST methodology. In this respect, there are two types of information important and definition of which is required by STAMP ontology: which safety constraints were violated and how these constraints map to the model of processes, i.e. to the safety control structure documented in step 3 of CAST methodology. Fig. 18 shows specification of violated safety constraints according to the STAMP ontology. It is possible to infer mapping of the constraints to the control loops from the already created

documentation, specifically from schema in Fig. 16. When implementing the ontology into software environment, this can be inferred automatically.

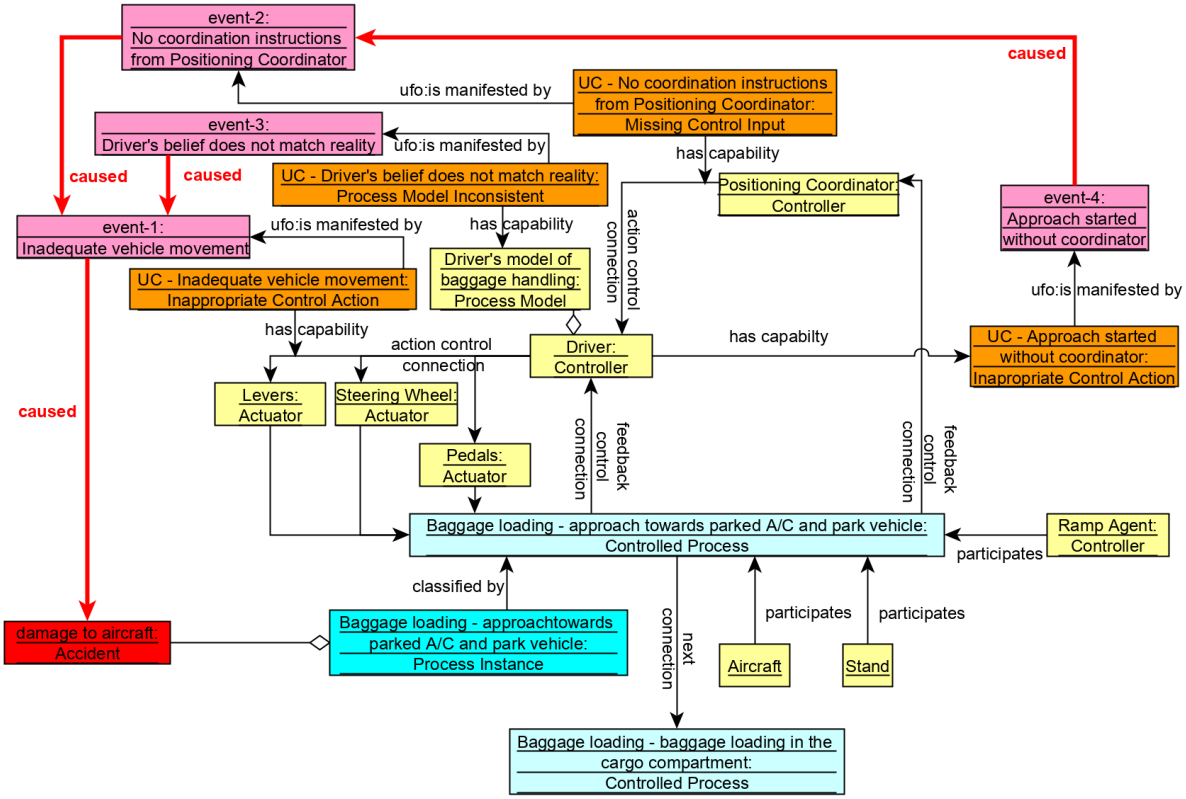


Fig. 17 Modeling of fictional event of aircraft damage during process of vehicle parking by means of STAMP ontology

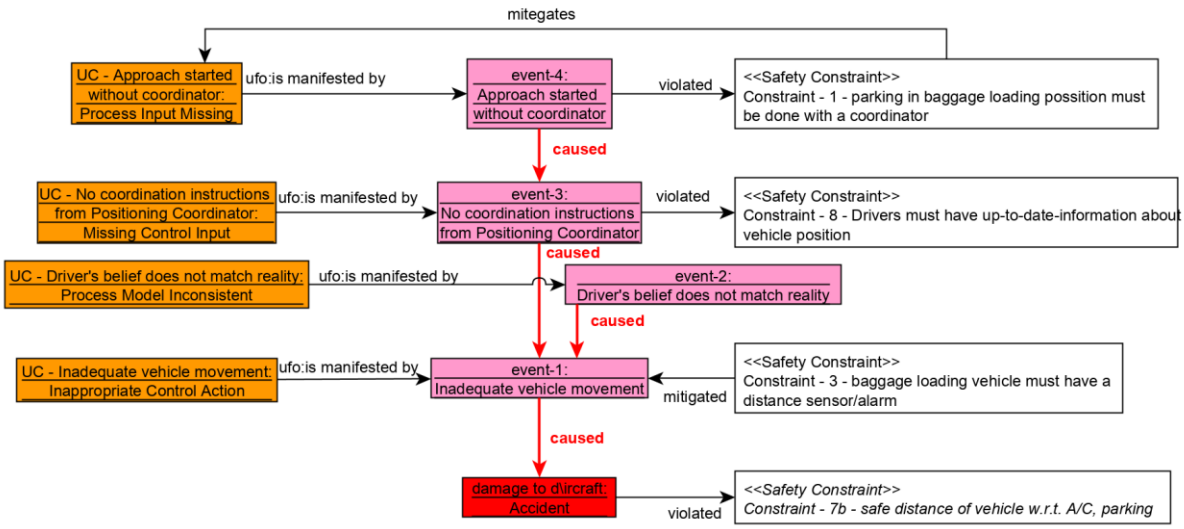


Fig. 18 Modeling of fictional occurrence of damage to aircraft and its mapping to safety constraints by means of STAMP ontology

As is apparent from Fig. 18, STAMP ontology specified the process of data collection and processing. The ontology requires here definition of violation relations between contributory factors of an occurrence and safety constraints. The mentioned example of safety constraint -1 from Fig. 16 is in Fig. 18 violated by specific contributory factor - approach started without coordinator. Even though the example used in this chapter is rather simple and regards only two control loops, the same procedure applies when multi-level hierarchy of control loops would be considered.

3.3.3 Practical recommendations

Performing safety data collection and processing with the utilization of the developed STAMP ontology brings several possibilities for how to facilitate, expedite but simultaneously maintain the advantages of ontology application with respect to supporting the execution of some of the steps of CAST methodology based on STAMP.

First of the possibilities for facilitation is introduction of libraries covering object types, employee roles and similar. Ontology inherently works with types and it is not necessary to specify all the instances. In some cases it may be beneficial to work with instances (e.g. define personal details of individual employees, who are playing different roles in the processes or define identifiers of individual vehicles which are being used in different processes), however, STAMP aims at systemic point of view and so it aims rather at mutual relations, links and arrangement of objects, control loops and similar entities appearing in the processes at more generic (functional rather than particular object-dependent) description. With respect to this, definition of roles and types suffice (e.g. conveyor belt driver, or aircraft, or even fleet etc.) and by establishing a library of all such types, manageable sets of objects are created from which a safety analyst can pick relevant objects during both process definition in the process documentation so as during mapping of events to the documentation.

Another from practical recommendations pertains modeling of complex control, when a higher level of detail is necessary for an analysis. Theory of STAMP admits existence of overlapping control loops but it is rather limited in providing the ways of how to depict details of such control in real conditions. Example of such a situation is depicted in Fig. 19. The example includes the already described control loop of conveyor belt driver from Fig. 11 and, in addition, also detailed description of a control loop of parking coordinator (highlighted in magenta) with the relations among the two control loops. Similarly as for the previous figures, Fig. 19 is an attempt to visualize the situation, even though the main goal would be definition of its content by means of classes and relations in RDF format. In this way, by means of the STAMP ontology, it is possible to document an accurate description of a complex control in desired level of detail, which may not be easily visualizable, and the documentation can be conveniently used for safety data collection and processing.

The last recommendation relates to the possibility of utilizing STAMP taxonomy depicted in Fig. 3. The taxonomy is general and applicable for safety data classification. In the context of STAMP ontology application, this taxonomy can be used in its general form to classify safety occurrences and contributory factors (as used in Fig. 18 in orange boxes). Because the general STAMP taxonomy is mapped to specific objects of a control loop (e.g. inadequate process model maps to controller), by modeling the general taxonomy by means of the

STAMP ontology there is an opportunity to filter the taxonomy per object of interest and so to enable practical pre-defined lists for event classification.

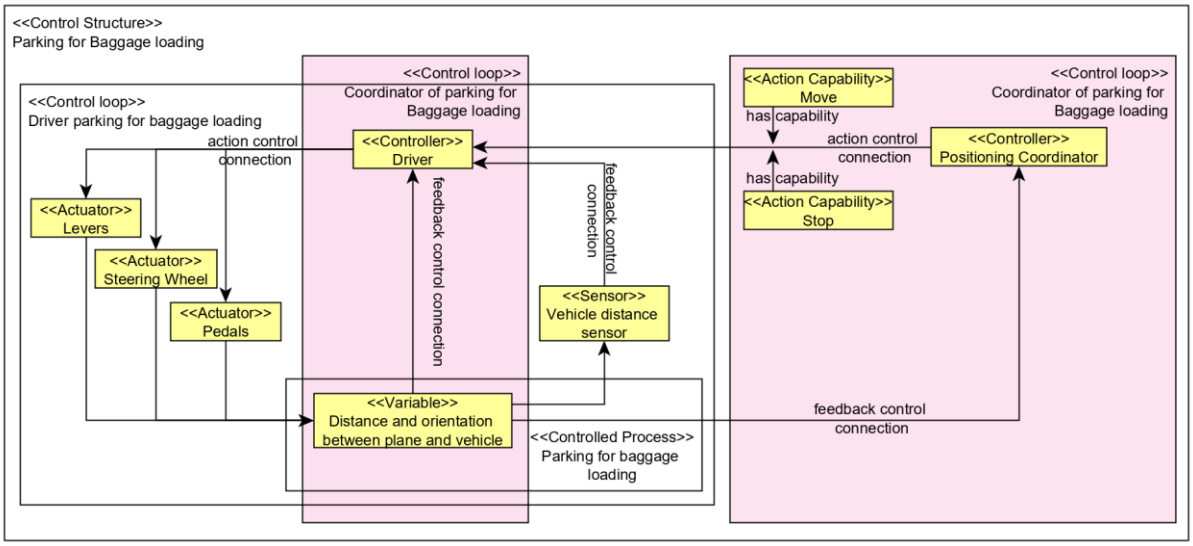


Fig. 19 Modeling of detailed relations between two control loops by means of the STAMP ontology

3.4 Utilization of process documentation and its tools

Process documentation lays down principles and procedures for execution and management of processes and activities in respective organization with the aim to achieve unified and effective control. The documentation is issued in common form and single system and there are rules and responsibilities specified for its creation and management. It specifies binding rules needed for correct functioning of company processes, it describes them, their sequence or connections, including authority and responsibility. Following that, it can be noted that the process documentation is suitable foundation for establishing documentation of a system of interest.

Graphical representation of business processes by means of process diagrams, which is suitable and valid tool for documenting a system, is governed by rules and principles of BPMN. Process diagram is a set of single or multiple interconnected procedures or activities carried in given order. Other external conditions can be also included. The tools available for modeling with BPMN allow integration of all principles described in the previous chapters in a way introduced in this chapter.

Processes of an organization or a company can be divided into three basic groups: main, supporting and control processes. A model of such division provides an overview of a system for analyst. The groups can be further elaborated and detailed to a higher level of resolution because every activity in a process may represent a whole other process at the higher level or resolution. Eventually, every single action within an activity can be described, even though

such resolution is typically not needed. It is very important, however, to record the work as done rather than work as imagined when documenting the processes.

The following figure (Fig. 20) shows a diagram of a basic process. Its elements are start, i.e. beginning of the process activity, individual activities arranged into required structure and interconnected with relations, and finally an end where process activity finishes. The figure shows a process of vehicle parking used in examples from the previous chapters. It specifies two parallel activities as per the responsible person, here the vehicle driver and a positioning coordinator.

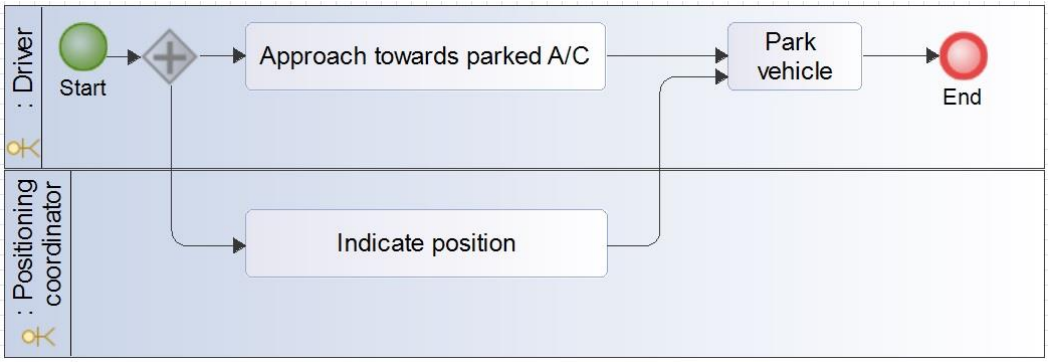


Fig. 20 Example of process diagram according to the BPMN notation produced with Modelio

As can be seen from Fig. 20, the process diagram provides functional documentation of a system, i.e. a documentation of what the system does rather than what it is (from the object-based perspective). This is very useful when applied in the context of CAST methodology execution since it can guide safety analyst to avoid extremely detailed description of a system that could eventually be limited to analysis of failure modes of individual components rather than systemic issues.

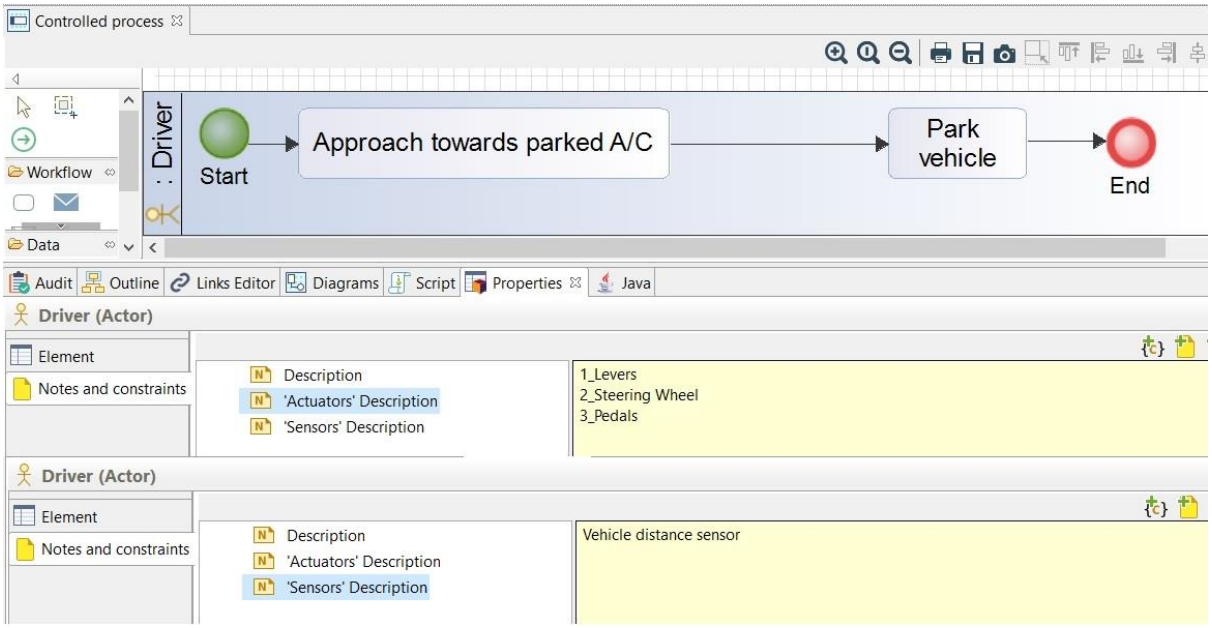
Available tools for process modelling can be used for documentation of a system (safety control structure), as discussed in chapter 3.3.1, since they allow for storing all necessary information to be used with the ontology application. Following subchapters provide some details about how to use the tools for this purpose.

3.4.1 Documentation of a control loop

Control loop according to the feedback control theory and as used by STAMP consists of four basic elements: controller, actuators, sensors and controlled process. In BPMN, a controlled process is every activity arranged in a process diagram. Every activity must have precisely one responsible role assigned as responsible for its execution. From the perspective of STAMP, such role is the controller. The list of actuators and sensors used with the role can be added using attributes of the role. Example of implementation of a control loop description according to feedback control with BPMN is shown in Fig. 21. The figure shows specification of available actuators (‘Actuators’ Description) and sensors (‘Sensors’ Description), namely “1_Levers”, “2_Steering Wheel”, “3_Pedals” as actuators and “Vehicle distance sensor” as sensor. This way it is possible to add part of the information needed for STAMP analysis directly into a process documentation of an aviation organization.

3.4.2 Library of controllers

Roles of the employees who are responsible for individual processes can be displayed in a library of responsible roles. For the purpose of the described methodology, roles are defined by actuators and sensors available to a controller in respective activity. Example of a preview of a library of controllers is shown in Fig. 22. The library shows two roles - namely the vehicle *driver* and *positioning coordinator*. As already mentioned in chapter 3.3.3, establishing a library facilitates process documentation management with regard to provision of the information required by STAMP analysis. It is sufficient to establish library of controllers by means of standard available tools for process modelling, nevertheless depending on the specifics of respective tool it may be useful to consider establishing other libraries, which may facilitate process documentation management in respective cases. Establishing such libraries then follows the same principles as for library of controllers.



Obr. 21 Example of a control loop description with BPMN produced with Modelio

4. Novelty of the methodology

The novelty of the methodology can be defined in two contexts: (a) in comparison with CAST methodology based on the theory of STAMP and (b) in comparison with current industrial standards of aviation safety data collection and processing. The following subsections provide the highlights from both contexts.

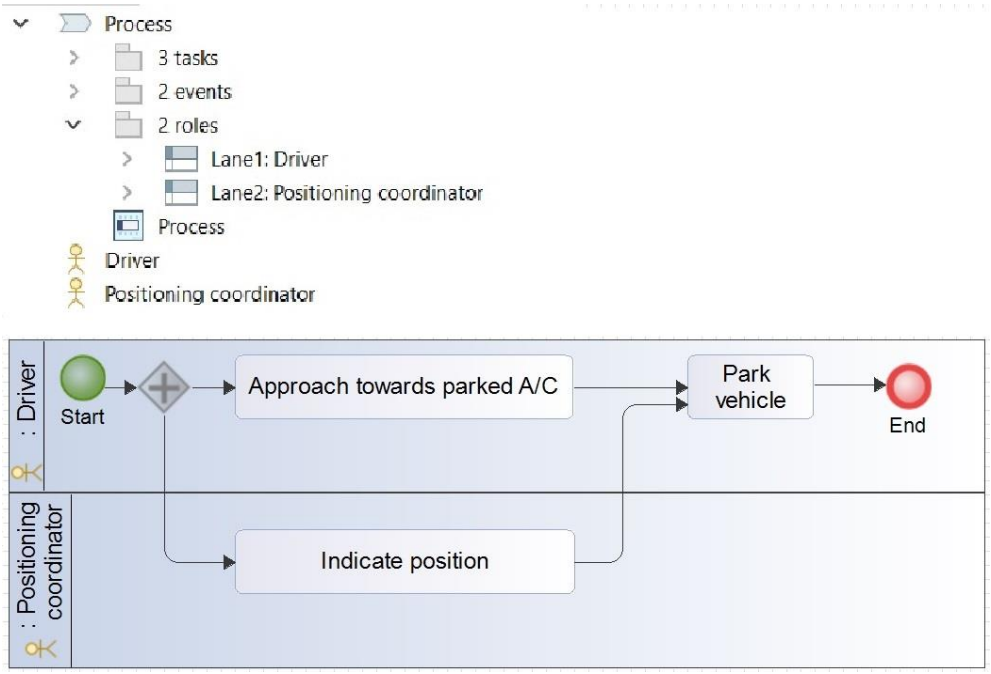


Fig. 22 Example of utilization of library of controllers according to the BPMN notation produced with Modelio

4.1 Comparison with CAST methodology

The methodology already includes direct comparison with CAST methodology based on the theory of STAMP. CAST is founded on the theory of STAMP so is the developed ontology in this methodology. Both methodologies are compatible, however, this document describes new technical possibilities for how to support specific steps of CAST by the developed ontology and how to achieve practically exploitable results in the aviation industry, especially in the context of current safety management standards in the industry. In addition, the application of ontology brings new possibilities for integration of the safety data collection and processing with company and industrial processes, which is out of the scope of CAST. The developed ontology allows for utilization of standard process documentation as a source of necessary information for carrying out safety data collection and processing and, vice versa, it allows for storing data in the context of the very same documentation. Apart from the benefits of the integration, this brings also few other possibilities: (1) CAST methodology can be executed with complete and up-to-date documentation of a system, which produced the data and not only with ad-hoc representation (snapshot) of a safety control structure of interest, which is necessary to be established with every safety analysis; (2) storing safety data in the context of process documentation allows for better and more effective support for identification of problematic parts of a system so as preventive measures, which have the potential to mitigate the problems; (3) in case the ontology modeling technology is applied in other then safety domains, it enables partly automated identification of correlations between safety data and data about quality, reliability, cost-efficiency and similar and consequently the possibility to propose system-level measures in the context of standard process documentation.

4.2 Comparison with aviation industrial standards

In the context of current standards for safety data collection in the aviation industry, the main novelty regards application of the theory of STAMP in the aviation industry and support for carrying out CAST methodology which is now (owing to proposed technical solution) more accessible from the perspective of the systems already in use for safety data collection and processing.

Current industrial standards for these systems are defined by ICAO Doc. 9859 Safety Management Manual, issued by the International Civil Aviation Organization, now in edition 4 from 2018. This document requires aviation organizations and states to establish a system for safety data collection and processing and it lays down principles for which data and how to collect and process. These principles are until today based on SHELL and Reason's model, i.e. based on identification of accidents and incidents with linearly ordered contributory factors, in line with the core ideas of the models. The industry focuses of event classification according to current safety taxonomies available, in the aviation especially the ICAO ADREP taxonomy and in Europe the ECCAIRS taxonomy, or its filtered version known as RIT (Reduced Interface Taxonomy). Safety data collected and processed according to the taxonomies are subjected to analysis by means of safety performance indicators, which are analyzed for trends or correlations with other safety performance indicators. Other processes defined by ICAO with respect to the safety data collection and processing regard data completeness or security and they are not innovated by this methodology.

The novelty with respect to the mentioned industrial standards in the aviation regards the shift in safety model used to explain safety occurrences and safety issues. This methodology uses STAMP prediction model of safety, which aims at system-level assessment of safety and for identification of safety issues at the level of a system as a whole, by means of feedback control theory. This methodology brings key innovations and technical possibilities owing to which it is possible to close the gap between the theory and industrial processes of data collection and processing and so it facilitates application of STAMP in the aviation industry. The methodology guides the user to create safety occurrence records mapped to the documentation of a system, which generated the data, and so it allows for the system-level safety analysis. The goal is not to monitor pre-defined set of safety performance indicators over some time periods, as is the current practice in aviation, but to monitor the behavior of individual parts of a system with analysis focused on which parts of the system or which safety measures are correlated, eventually providing for the understanding of how to effectively manage safety from the perspective of the whole system. In this respect, the methodology with its technical solution based on ontology engineering creates new functionalities, which allow for faster, simpler and more accurate analysis and management of risk in the context of current safety management systems in the aviation.

5. Application of the methodology

This methodology describes the possibility for increasing efficiency and effectiveness of analysis and management of risks by means of conceptual modeling, i.e. by means of the developed STAMP ontology, and based on customized safety data collection and processing. It is dedicated to aviation organizations, which can implement its content into their safety

management systems, and for which it offers technical and methodological solution for integration of standard process documentation activities with safety management. It is possible to apply the methodology in several contexts detailed in the following paragraphs. Even though the methodology is based on innovative solutions, which are not required by any current law of aviation standard in force, it offers potential for improvement in areas where the law and standards aim to govern industrial practice and its application eventually supports meeting the goals of applicable law and standards.

The methodology can be applied in the context Czech aviation standard L19 and ICAO Annex 19 provisions, so as in the context of specific provisions of ICAO Doc. 9859 Safety Management Manual regarding the establishment and management of Safety Data Collection and Processing System - SDCPS.

The methodology can be applied in the context of European legislation regarding the aviation safety data collection and processing, especially in the context of Commission Regulations No. 996/2010, No. 376/2014 and No. 2015/1018.

The methodology can be applied also in the context of EUROCONTROL Safety Regulatory Requirement ESARR2 about safety occurrence reporting by the European Organisation for the Safety of Air Navigation.

6. Economic aspects

Application of the methodology induces several implementation costs. If the methodology is implemented into own custom software solution, then the costs are induced for such implementation. Further, there are costs regarding the training of relevant personnel and update of respective processes in a company. In some cases, it may be needed to increase the number of employees of a safety management unit of respective company, nevertheless such measure is not considered necessary for the methodology implementation. If the methodology is implemented independently from existing software solutions in respective company, especially by means of free available tools, then the implementation costs are reduced but, on the other hand, an opportunity of integrated solution is lost.

Potential economic benefits cannot be precisely quantified, but these are primarily related to the improvement of safety management processes, namely with increased effectiveness and efficiency of the safety management system. Effective safety management brings improvement in financial health of a company, because it leads to less safety occurrences in the operations and the occurrences can be better anticipated, i.e. adequate resources can be planned for potential remedy in advance [14]. Standalone economic opportunity is the realization of integrated solution, which offers the potential for limitation of the workload of safety management employees in the context of safety data collection and processing. It also improves the capability of identifying system-level opportunities for improvement of respective company operations and so to increase the capability of a company to adequately allocate resources to priority issues from the perspective of maintaining its safe and efficient operations.

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

List of publications preceding the methodology

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

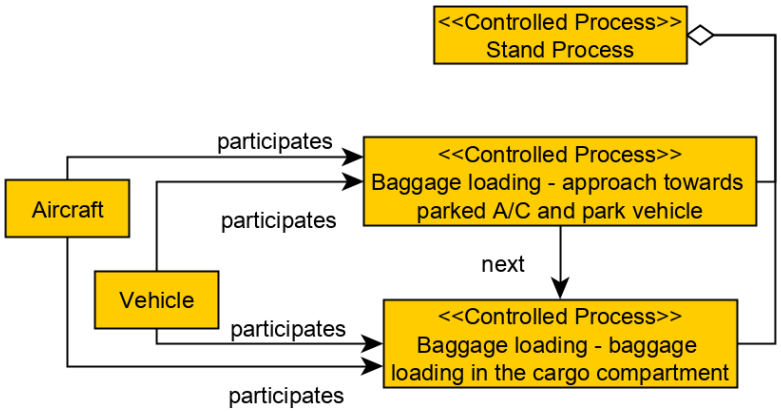
Křemen, P., Kostov, B., Blaško, M., Ahmad J., Plos, V., Lališ, A., Stojić, S. and Vittek P. Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems. *Journal of Aerospace Information Systems*. 2017, 14(5), 279-292. DOI: 10.2514/1.I010441. ISSN 2327-3097.

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

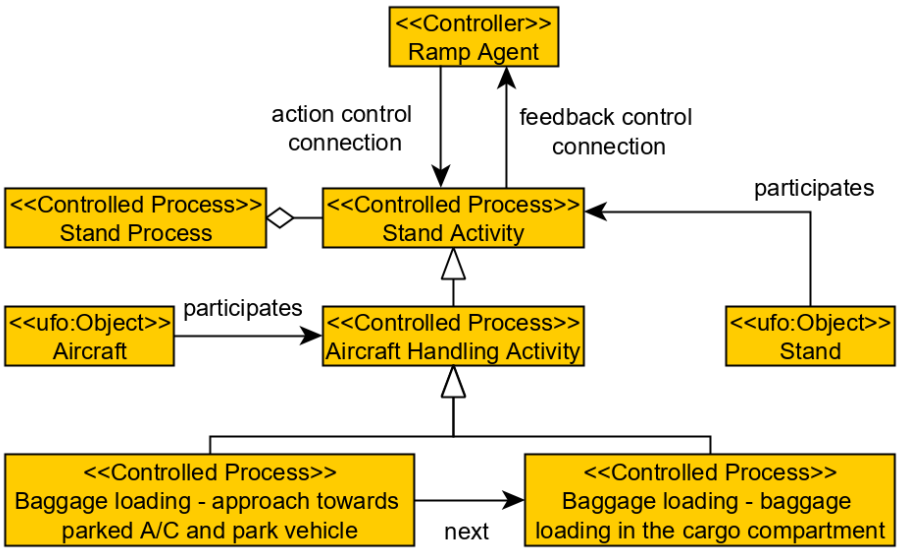
Saeeda, L. Iterative Approach for Information Extraction and Ontology Learning from Textual Aviation Safety Reports. Blomqvist, E., Maynard, D., Gangemi, A., Hoekstra, R., Hitzler, P. a Hartig, O. ed. *The Semantic Web*. Cham: Springer International Publishing, 2017, 2017-05-07, s. 236-245. Lecture Notes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

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

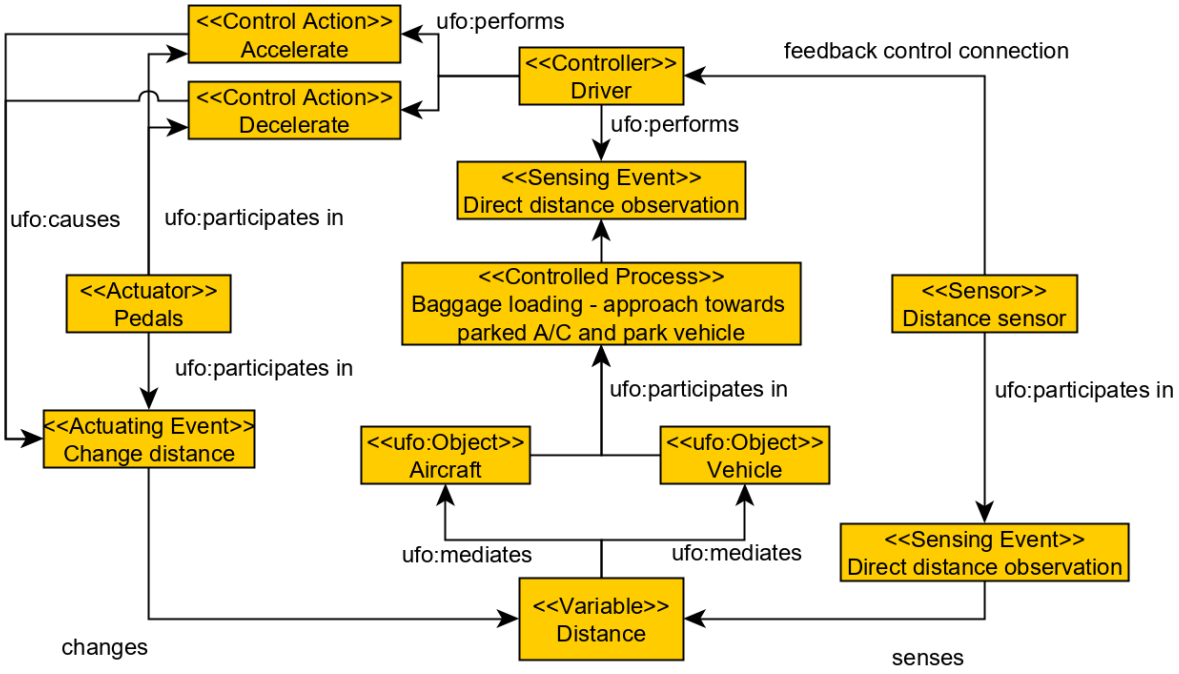
Appendix 1: Examples of STAMP ontology application on industrial situations from the domain of airports



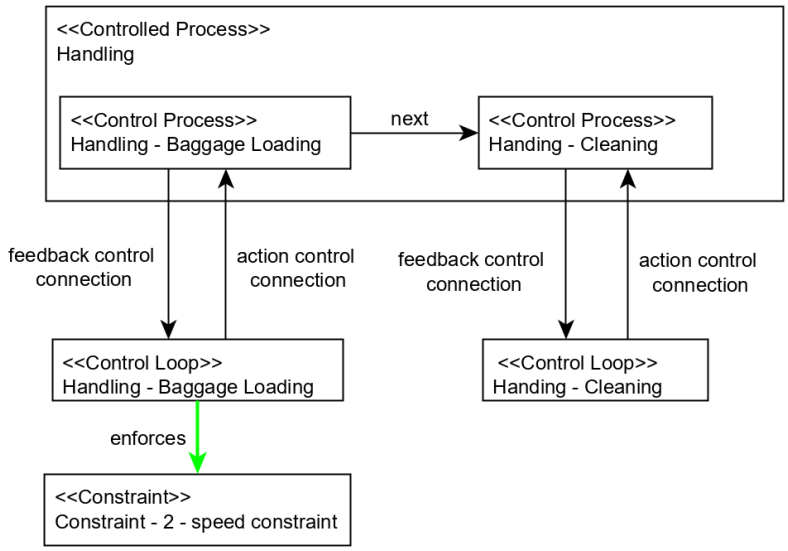
P1: Description of a baggage loading process during ground handling of an aircraft



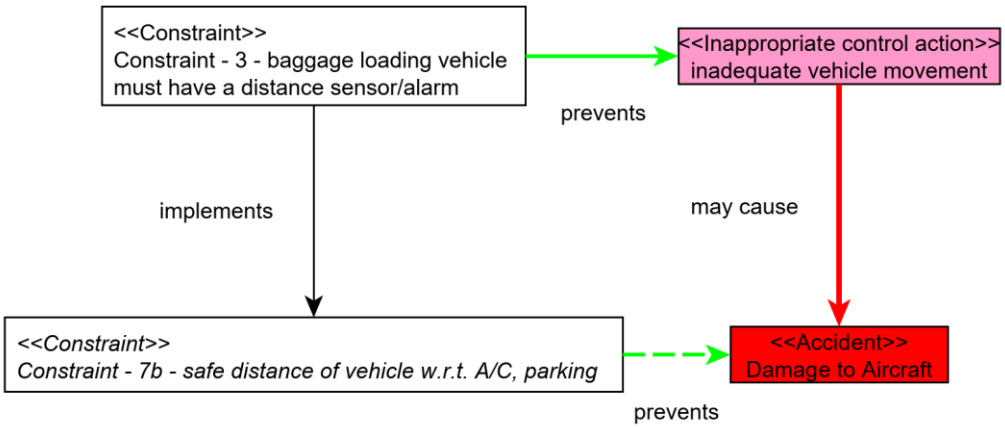
P2: Specification of participants and relations of feedback/control in the context of describing aircraft baggage loading process



P3: Modeling of control and events related to the conveyor belt driver



P4: Modeling of relations between safety controlled process, safety control structure and safety constraints in the context of aircraft ground handling



P5: Modeling the relations between safety constraints in the context of unwanted events they are designed to prevent

Appendix J

LALIŠ, Andrej, Slobodan STOJIĆ, Markéta KAFKOVÁ and Oldřich ŠTUMBAUER. *Methodology for performing safety studies in the aviation by means of quantitative methods.* Certified methodology by the Ministry of Transport, Czech Republic, 2019.

METHODOLOGY

for performing safety studies in the aviation by means of quantitative methods

Research project TA ČR Zéta No. TJ01000252

Department of Air Transport
Faculty of Transportation Sciences
CTU in Prague

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

Prague Airport, Ltd.

Kafková Markéta, Ing.

CTU
CZECH TECHNICAL UNIVERSITY IN PRAGUE

Prague Airport

T A
Č R
Technology Agency of the Czech Republic

Program Zéta

Methodology for performing safety studies in the aviation by means of quantitative methods

Contents

Introduction

Safety studies undoubtedly belong to the key activities which are necessary to carry out in all high-risk industries, with the aviation being no exception. The main purpose of these studies is an assessment, whether specific system (technology, infrastructure, procedures and similar) has the potential to perform acceptably safe in the operations. The task of the safety studies regards not only assessment of newly developed systems with no history of operation, but also assessment of changes to existing systems, which need to be modified due to various reasons. This task is especially challenging in the modern age since current technology is becoming ever more complex and more dependent on non-trivial interactions with its user and environment [1]. In the aviation, this issue is formulated in the latest (fourth) edition of ICAO Doc. 9859 Safety Management Manual [2] by the International Civil Aviation Organization, as the problem of total system era, which is manifested in the aviation in form of mutual dependency of individual industry components. Following the issue, it is important to emphasize system-level aspects also in the context of safety studies and, as much as possible, to limit the impact of subjective evaluation of individual safety analysts on the overall result of safety studies. This issue of the modern age is addressed by this methodology.

The methodology offers basic guidelines for the analysis and evaluation of risk in the aviation processes, with the focus on airports. Its content corresponds to the risk management processes and its novelty stems from incorporating current safety engineering knowledge and the theory of safety. The methodology is fully compliant with international standards and recommendations in the aviation, especially the mentioned ICAO Doc. 9859 [2]. Further, it is based on the current practice of safety studies execution in the aviation, which are mostly implemented as a variation or full application of SAM (Safety Assessment Methodology) [3] published by EUROCONTROL (European Organisation for the Safety of Air Navigation). The main novelty is extension and alignment of SAM base process, namely its steps regarding hazard identification and risk assessment, with the STAMP (Systems-Theoretic Accident Model and Processes) [4] systemic model of safety. In this way, the methodology addresses current challenges of interconnection and systemic dependency of modern high-risk industries such as the aviation. The methodology, on the other hand, does not propose any change of the SAM principles, but uses some of its parts as the baseline for extension. Separate extension is addition of quantitative evaluation which regards customization of some steps of safety studies for the sake of increasing objectivity of overall safety studies execution, especially in the context of risk level evaluation. In this respect, the methodology aims especially at the issues of risk matrix. In the aviation, ICAO still suggests the two-dimensional (severity and probability) risk matrix to be used with risk assessment. According to the research of selective mathematical properties, the matrix has significant limitations such as poor resolution, inherent flaws, suboptimal targeting of resources and ambiguous inputs and output [5]. Even according to the theory of STAMP, the risk matrix as a tool is questionable when used for risk assessment towards future operations of modified or new systems [4].

The following chapters detail the new methodology for safety studies execution with the focus on the aviation industry, specifically on airports. In a standalone chapter, theoretical foundations of systemic approach to safety studies so as the STAMP model with STPA methodology [6] (originally designed for hazard analysis by the authors of STAMP) are

described in detail. Detailed description of the methodology follows with instructive examples of its application.

1. Goal of the methodology

The methodology aims to disseminate the results of executed research project No. TJ01000252 by the Czech Technical University in Prague, in cooperation with Prague Airport, funded by the Technology Agency of the Czech Republic. The methodology is a summary of the knowledge gathered in this project and it contains procedure for carrying out safety studies in the aviation, with the focus on airports and utilization of systemic approach and quantitative methods for analysis and evaluation of risk. The goal of the newly created method is to increase objectivity of risk evaluation in the context of safety studies, focused on the domain of airports, and with provision of a methodology that follows systemic approach to safety.

2. Dedication

The methodology is primarily dedicated to airports, which are interested in improving the process of carrying out safety studies and so to increase the level of safety on their infrastructure. The methodology can be applied also in other types of aviation organizations or other high-risk industries, such as nuclear power plants, chemical industry etc. Even though the procedure described in this methodology is general, in case of application in other types of aviation organizations or in other industrial branches, the methodology does not guarantee full correspondence to the specifications of these domains and possible modification should be considered.

3. Methodology description

This section contains core description of the new process of carrying safety studies in the aviation, with the focus on the airports and utilization of systemic approach to safety and quantitative methods for the risk evaluation and analysis. The new process follows STAMP prediction model of safety and so the first subsection introduces relevant parts of the theory. The subsection provides base description with all relevant links that the user should familiarize with in order to fully understand the methodology. The next subchapters follow with detailed description of the new process for carrying out safety studies, with several practical examples of its application.

3.1 Theory of STAMP [4]

STAMP is modern systemic model of safety, which interprets the problem of safety as a control problem. The model adopts the concept of feedback control [7] representing how modern systems are controlled, both from social and technical perspective. Even though feedback control originates in computer science, it can be used to describe also a purely social system, where the controller is human and the controlled process is an activity of another human. The basic concept of feedback control is a control loop depicted in Fig. 1. According to the theory

of STAMP, any accident or incident can be explained in the context of feedback control and the feedback control theory can be used for identification of causes why a system failed as a whole. The theory of STAMP claims that if there is an accident or incident (so as regular safety occurrences), the so-called safety control structure, i.e. a web of interconnected control loops, must have failed in some way to either cause or to allow the occurrence to happen. The theory moves the attention of safety analyst away from basic interpretation of safety data by means of descriptive statistics (mean, trend or deviation regarding number of occurrences in a time frame) and encourages him or her to document description (representation) of a system which generated the data. In result, this allows safety analyst to consider the entire system as a whole. The produced documentation of a system simultaneously supports analysis of how to prevent recurrence of similar situations.

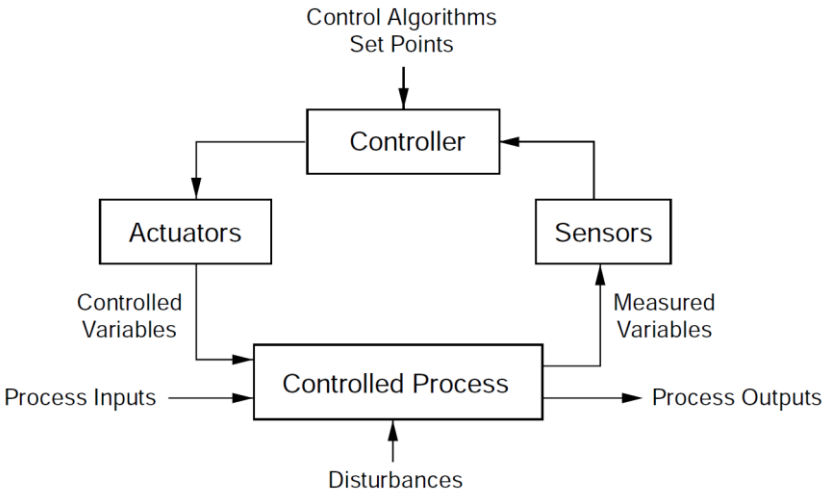


Fig. 1 Control loop as a basic concept of feedback control [4]

Following the afore-mentioned, it is apparent that all methods based on the theory of STAMP require each safety analysis documenting parts of a system of interest, which is then to be evaluated on safety by means of control loops. As the Fig. 1 shows, this leads to a creation of an object-based diagram describing the evaluated system from the perspective of roles and responsibilities (controllers) and tools (actuators, sensors) used to manage safety. By progressively specifying and connecting sets of control loops, it is possible to produce detailed description (representation) of a system, i.e. the overall safety control structure, that can be abstracted to provide for functional description rather than merely object-based description. Simple example of a safety control structure from the domain of aviation is depicted in Fig. 2.

As a next step, the combination of documented system description with general causal control model for scenario identification, i.e. taxonomy of safety issues provided by the theory of STAMP (shown in Figs. 3 and 4), is used to execute safety analysis. This document includes both variants of the general causal control model for scenario identification (both basic and extended) so as the basic taxonomy for classification of safety issues by STAMP. This way the theory of STAMP ensures completeness of a safety analysis since all safety issues, which cannot be excluded as not possible in real conditions, should be considered in the context of the documented system, its safety control structure and possible causal scenarios that can lead to losses. In some cases, the very documentation of safety control structure suffices for identification of safety issues.

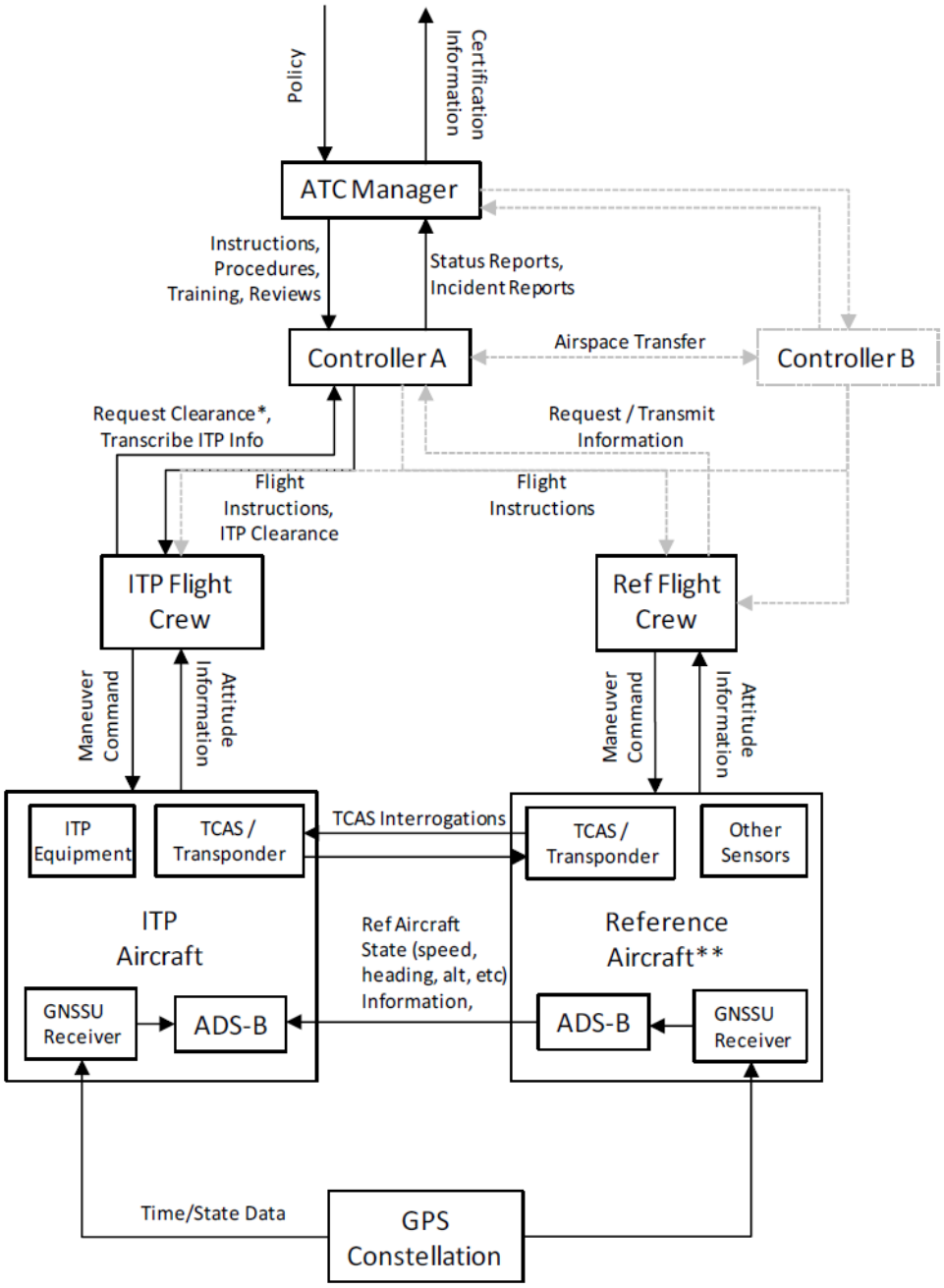


Fig. 2 Example safety control structure in aviation according to STAMP - the situation depicts two aircraft controlled by an air traffic controller [5]

In the context of safety studies, the authors of STAMP developed STPA (System-Theoretic Process Analysis) methodology for hazard analysis, which is aimed at practical utilization of the STAMP theory by industrial users. This methodology requires documentation of the system (safety control structure) of interest and its subsequent analysis. STPA methodology consists of the following steps:

1. Definition of the analysis purpose
2. Modeling of the safety control structure (diagrams of safety control loops)
3. Identification of unsafe control actions
4. Identification of loss scenarios

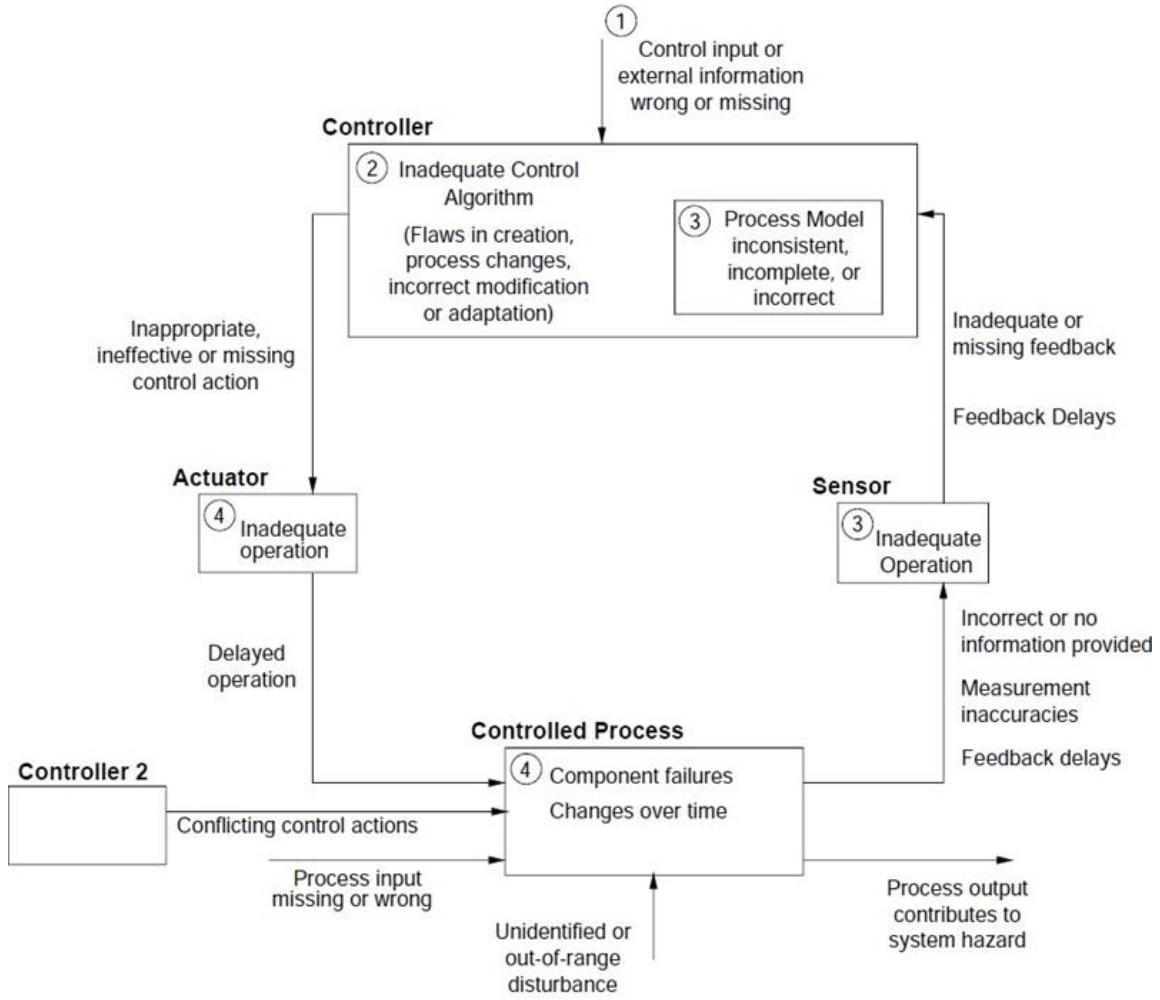


Fig. 3 Basic causal control model for scenario generation for identification of hazards and safety issues taxonomy based on the theory of STAMP [4]

Step 1 of the methodology ensures correct selection of the analyzed system or parts of several systems and their interfaces. Due to practical reasons it is advisable that step 2 produces only diagram of selected part of a system or systems and their interfaces, because complete description of reality may be very demanding and in the context of the safety study rather unnecessary. Step 3 follows with analysis of all elements and relationships in the diagram of control loops created in step 2 to identify unsafe control. The last step - step 4 then supports analysis of the entire diagram with the focus on failure of the system as a whole in specific scenarios.

Apart from hazard identification, which in STAMP is based on the explanation of safety as a control problem, there is also the question of risk. STAMP also uses the risk matrix as a starting point, even though authors of the theory suggest not to use probability parameter if it cannot be precisely estimated (whether qualitatively or quantitatively). The parameter is

considered especially problematic if estimated in cases where non-existing system is the scope of analysis, in the context of which there are no history data that could serve as a basis for probability estimation. In that case, any probability estimation is considered unfounded and very unlikely to match reality.

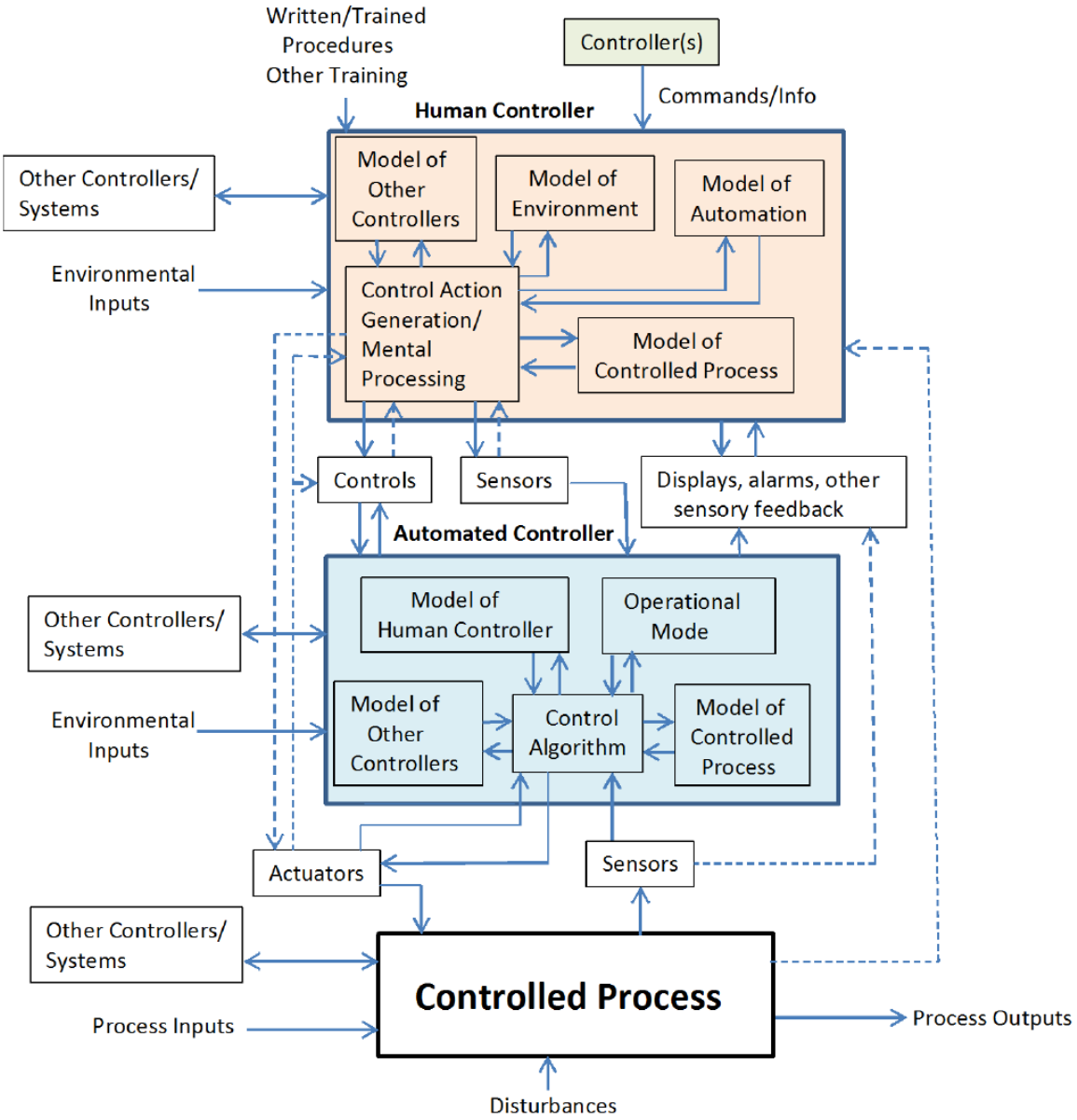


Fig. 4 Extended causal control model for scenario generation for identification of hazards based on the theory of STAMP. Combination of the causal control model with basic taxonomy of safety issues from Fig. 3 provides extended taxonomy of safety issues according to the theory of STAMP. Intermittent lines represent relationships which do not have to exist in a system but which implementation may be considered for the sake of increased level of safety [5]

As a solution to the problem with probability, theory of STAMP offers two general solutions. The first solution suggests establishment of a set of questions or assessment criteria, which can be better answered than the question “What will be the probability of an occurrence type in future operations?”. An example of such questions is: (1) Will the proposed change lead to

the need of new safety measures to mitigate risk? (2) Will the proposed change lead to new functions, which have the potential to reduce effectiveness of current strategy for risk mitigation? (3) Are related failure modes and hazards in the proposed change the same as in current systems, or are new types of them introduced? (4) What is the extent of the change with respect to skills and knowledge required by controllers? and similar. Such questions should be customized for each safety study so that they fit its context and relevant safety control structure. As it is apparent from the general solution, safety analyst should gain assurance about acceptable level of risk from the overall set of questions and answers in the context of the proposal. The answers should create complete rationale for the assumption that there are no unacceptable risks in the proposed change. However, this does not eliminate the need for subsequent development and operations monitoring, which should both confirm the correctness of underlying assumptions from the executed safety study.

The second general solution is to substitute probability parameter with a new parameter - the so-called mitigation potential [8]. This parameter evaluates each identified hazard from the perspective of options available for its mitigation. The most desired state is when risks can be eliminated or mitigated directly by system design or in operations, with no need for complicated or costly solutions. In such system, risks are controlled easily and the very proposal indicates that accidents and incidents will be emerging very hardly.

The choice of a general solution lies with specific safety study, more precisely with the proposed system to be evaluated. The theory does not exclude utilization of both solutions simultaneously when probability of risk is unknown. In all cases, safety study should be executed repetitively during the entire proposal of a change or a new system to be introduced to operations. The reason for repetitive execution of a study is the risk that, in later stages of development of a new system or proposing modification to an existing system, implementation of effective mitigation measures may be costly, if possible at all. By contrast, in early stages of a development it is practical to choose from several development alternatives and timely select a proposal which will not be considered unsafe in later stages. According to the theory of STAMP, most suitable is repetitive execution of a safety study each time a key milestone is achieved, such as definition of system purpose, definition of system design principles, proposing system architecture or proposing physical representation [4]. Repetitive execution of a safety study, however, always depends on specific project type and the theory does not suggest any general procedure for every project.

3.2 Process model of an airport

The theory of STAMP, so as the methodologies proposed by its authors, work with the assumption that ad-hoc documentation of a system needs to be produced every time an analysis is to be carried out. The reason for this is that there is no practical way of managing real-time and up-to-date documentation of a system that would provide the details necessary for STAMP-based analyses in advance. However, with the development and practical experiences of business process modeling, there are new emerging possibilities that could provide such documentation or at least significant parts of it. This is the key assumption of this methodology, which provides a starting point for a new STAMP-based methodology.

Given the new assumption from previous paragraph, a system becomes delimited by the very process documentation, in this case of an airport. Processes which fall outside what is

documented in detail should be considered a system's environment. By contrast, such system may be robust and further decomposition or filtering shall be considered as per individual safety study or analysis. This is supported by the very definition of processes; every analysis has some scope with processes of interest and all processes outside the interest are then considered background processes, i.e. the environment. This makes each analysis per the proposed methodology flexible.

When looking in details, a process represents logically ordered sequence of activities, which aim to achieve some goal. Business process modeling is a tool that makes it possible to describe logical structure of individual activities inside an organization and as such it provides for functional documentation of a system (i.e. what the system does rather than what it is). The complex view on the activities inside an organization enables their thorough analysis and facilitates understanding of functional correlations and rules in a system.

The advantage of process modeling is the possibility for decomposition, which enables specification of subprocesses, often to the level of individual tasks, with the potential for measurement of their efficiency and effectiveness. Detailed focus on activities and tasks in a process may be very beneficial in a context of a safety study. Other benefit of a process modeling is that it inherently produces suitable inputs for analysis of a system when assessing its possible modification.

As described in the previous chapter, STAMP offers STPA methodology as a technique to analyze hazards, that can be used in safety studies. The proposed methodology in this document takes a different approach which, however, leads to the same results as when STPA is applied. The starting point is to produce process documentation as a complete system functional representation. If this is not possible, then conventional STPA should be applied instead. If such documentation exists or can be produced, then it is necessary to align the process documentation with basic concepts (objects) from the theory of STAMP. The overlap between standard business process modeling and the theory of STAMP is rather straightforward: every (sub)process has a responsible person (role) for each defined activity and task. The responsible person becomes the controller and respective activity or tasks the controlled process. The process model thus needs to be complemented only with the set of available actuators by which the controller manipulates controlled variables so as the set of sensors that provide him or her with feedback. It follows that controllers are delimited by the sets of actuators and sensors, which are available to them to control a process. Concrete example of application of the feedback control principles in process modeling tool is shown in Fig. 5. From the figure it is apparent that for description of sets of actuators and sensors, "Particular responsibilities" and "Particular recommendations" attributes were used respectively. This and all other examples were created with Adonis software[1] for business process modeling and the attributes were selected as most suitable to record the information about actuators and sensors. The examples are by no means aimed to endorse usage of this particular tool, but are used merely for illustrational purposes. In case of other tools or software, it may be convenient to use or create other attributes to record the information.

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

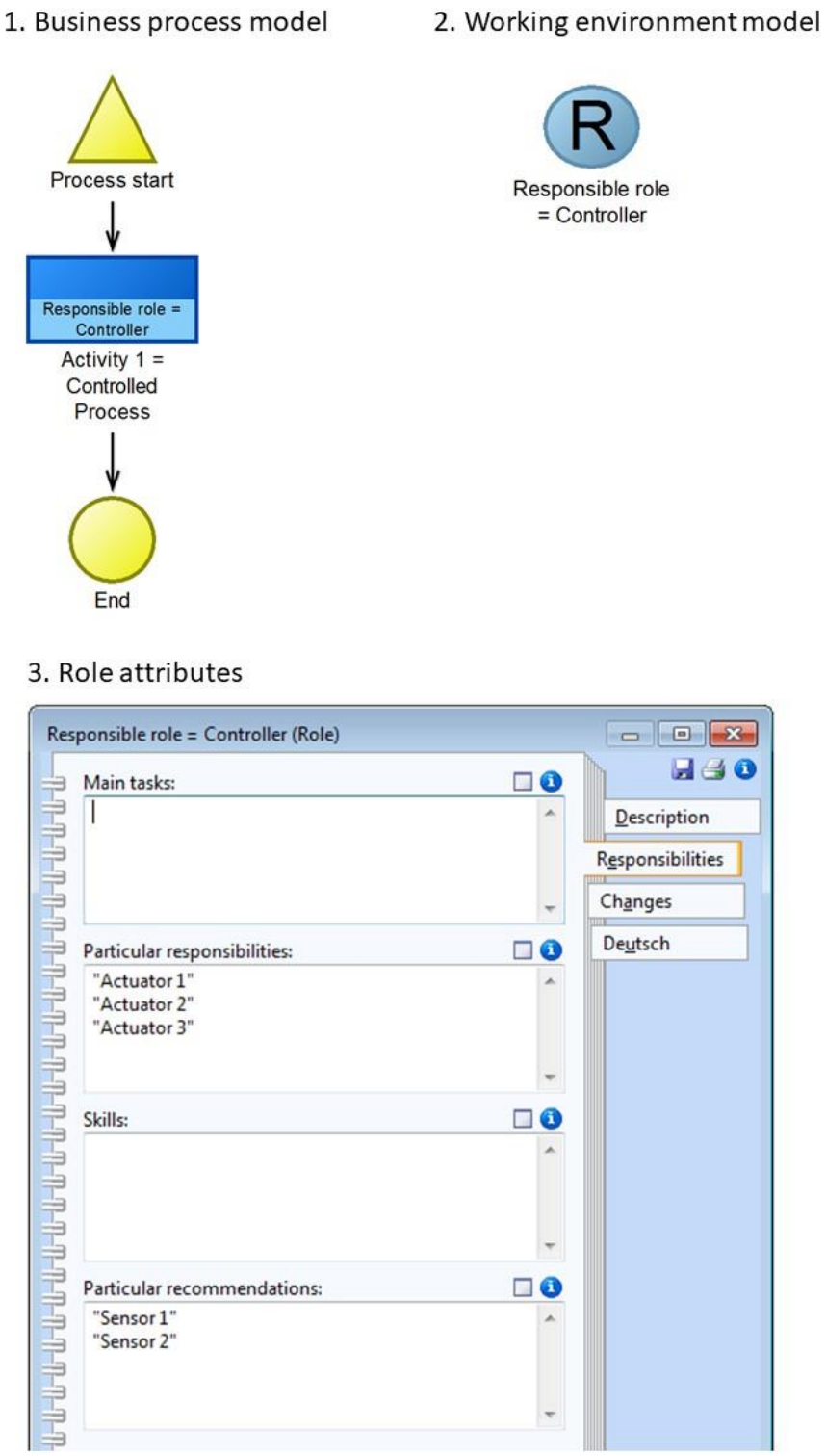


Fig. 5 Utilization of a tool for process modeling to insert information necessary for analyses based on STAMP

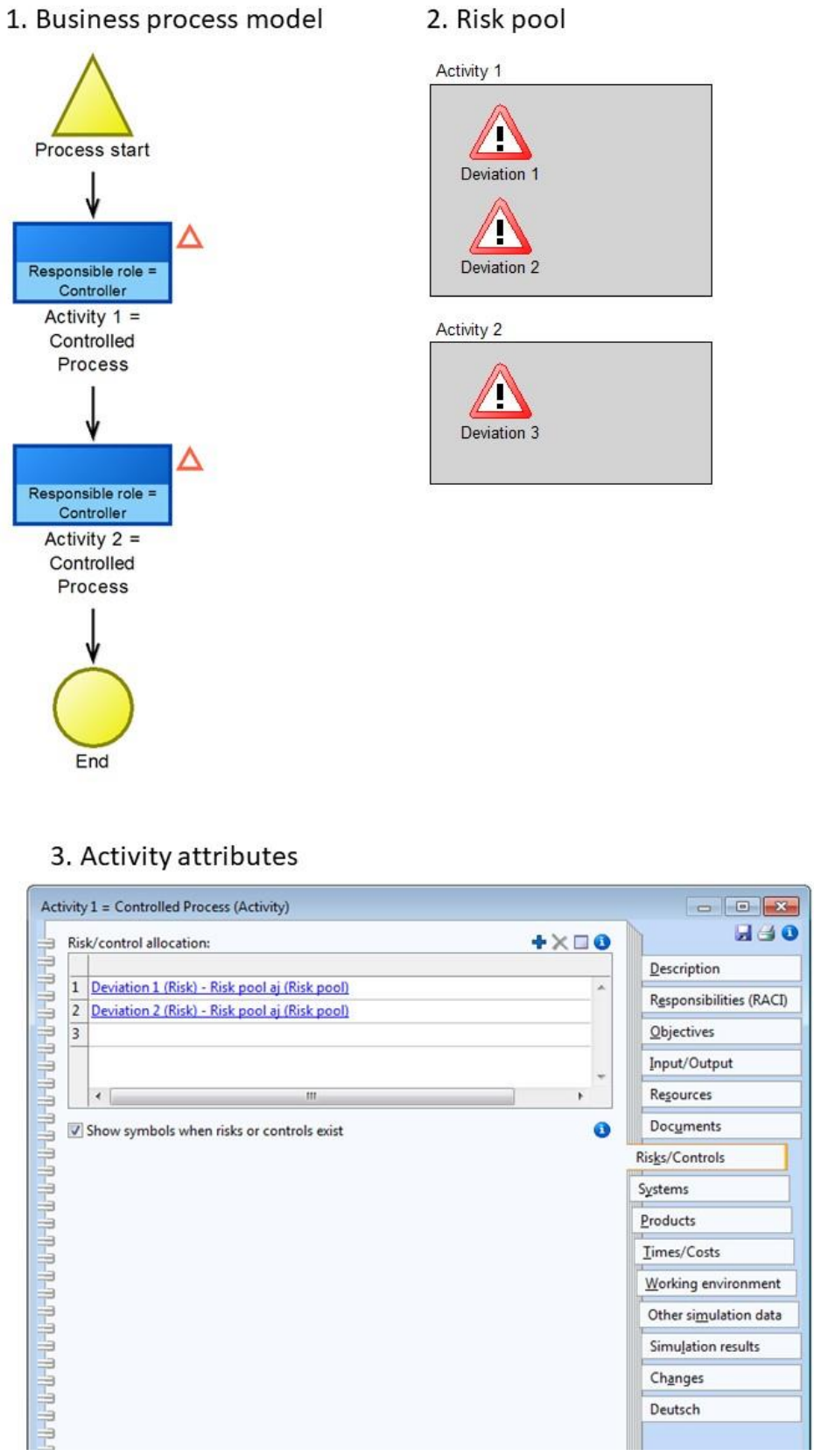


Fig. 6 Utilization of a tool for process modeling to insert information about deviations from defined activities in a process

According to the conceptualization of STAMP, accidents follow from external failures, component failures or dysfunctional interactions between components, if not adequately intervened by safety control structure. Accidents, therefore, follow from inadequate control and safety is considered to be the task of adequately designed safety control structure. Prevention of future accident requires establishing such safety control structure, which can effectively control activities to stay within given margins. Departure from assumed behavior of a controlled system (i.e. the difference between work as imagined and work as done) is considered a deviation in this methodology.

Deviation is key concept in this methodology and it is defined as departure from defined activity which has the potential to contribute to an accident. Deviations should be determined for every activity in a process model, i.e. for every control loop, by an expert who takes into account current system in consideration (which processes are the scope and which environment) and considers what losses (accidents, incidents, occurrences) may happen at the system level. During a safety study, it is necessary to verify that control loops are designed correctly so that they can react to every of possible deviations, i.e. that every deviation is identifiable by some of the sensors available and that the state of controlled process can be controlled by the actuators available. Because deviations are departures from individual process activities, they should be properly linked in a process model. For this purpose, deviations can be listed by means of the activity attributes, which is often a feature of the available modeling tools (see Fig. 6 depicting the example with Adonis software).

List of deviations then supports identification of hazards. Potential hazards are identified through a process analysis, performed by the safety expert, who evaluates individual process steps and defines most severe outcomes from the predefined deviations. Process model consists of logically ordered process steps, representing the workflow of respective process, so an identified hazard cannot strictly relate to single process step, but could be mutual for several of them. A process step or a group of process steps, in which identified hazard is relevant, should be identified based on the predefined deviations. Practical example of proposed hazard identification process is described in chapter 3.6. Identification of such system-level hazard represents a “high-level” analysis, where only severe outcomes are taken into account. For more proactive approach to safety management, the focus should be placed on the deviation level.

The list of applicable deviations can be established systematically by means of process documentation, where individual activities are described in detail and that should be carried for correct and safe process execution. An instruction, if carried out incorrectly or missed, is such a deviation. A suitable aid for establishing a list of deviations is systematic classification and generation of deviations with causal control model for scenario generation, together with the STAMP taxonomy shown in Figs. 3 and 4.

Subsequently, in this way, established libraries in a modeling software provide safety analyst with another view of a system or its part. For example, library of risks can provide for list of all deviations from a process, as the example in Fig. 7 shows. Similarly, library of controllers can be used for an overview of all controllers in a system, as shown in Fig. 8.

3.3 System interfaces

Process modelling is also a tool which helps organizations incorporate own processes in the surrounding environment, especially in the context of interfaces with other organizations. These interfaces are essential for safety management. It is important to realize that airports have a specific role as they are considered responsible for maintaining acceptable level of safety performance but majority of processes taking place on their infrastructure is out of their control. The processes are typically controlled by other organizations operating on an airport infrastructure, such as airlines, ground handling providers, fueling and catering companies and similar. Apart from processes which fall directly under the responsibility of airport operators, there are typically several other processes where airport operator interacts with other subjects and processes where the control is not provided by the operator at all.

Environment processes or some of their activities which fall outside the responsibility of airport operator are also suitable for analysis according to this methodology. They do not differ from description of internal airport operator processes and respective safety control structure fundamentally, but only in the level of detail. Control loops in process activities, for which airport operator is not responsible, can be processes only at generic level according to the theory of STAMP and basic knowledge of respective process or activity.

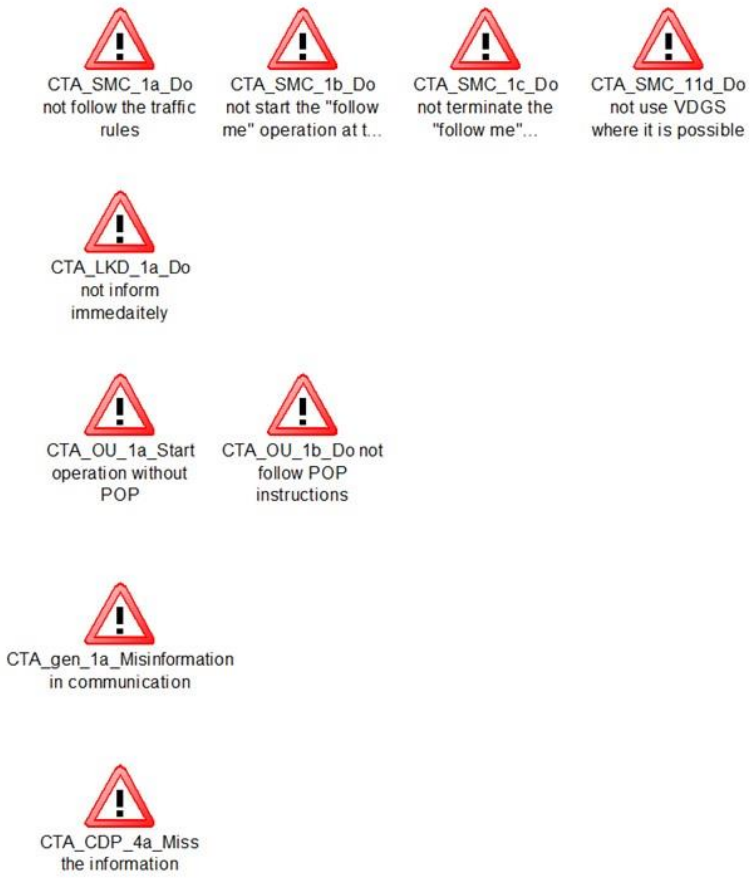


Fig. 7 Example of a list of deviations extracted from a process model

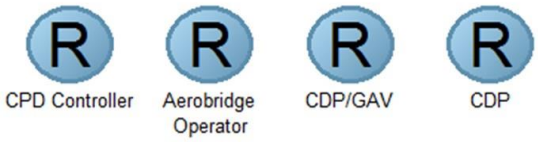


Fig. 8 Example of a list of controllers extracted from a process model

3.4 Deviation evaluation

The list of deviations as depicted in Fig. 7 represents base for hazard identification, and so as the hazards, deviation need also to be evaluated on risk. Hazard identification is here, however, based on STAMP by identification of deviations from the proposed system behavior at the level of controlled processes and individual activities, and so the evaluation of deviation is of greater importance and the main scope of this methodology. In this methodology, risk evaluation is tied to deviations and specific quantification method for the risk evaluation is detailed in this chapter. Risk evaluation of hazards follows similar logic, but with thorough evaluation of deviations, it is inherently covered and needs not to be done separately.

Evaluation of each deviation in this methodology is divided into four criteria: severity, controllability, detectability and time margin. These four criteria are mutually independent. The result of risk evaluation is not a single number expressing the level of risk with respective deviation, but a vector of indices expressing the overall criticality of a deviation in the context of risk, which respective deviation generates. The process of evaluation requires the user to possess detailed knowledge about the system and operations of interest.

Each of deviations is evaluated by vector of indices. Individual elements of the vector depend on assessment criteria and such distribution not only provides a more detailed analysis of weak parts of the evaluated system, but it shows the safety analyst, which particular evaluated system elements should be improved from the perspective of risk.

3.4.1 Evaluation criteria

This chapter details the criteria, which evaluate individual deviations. The next chapters describe overall evaluation of a process so as the entire system. The last chapter of this part provides some practical examples of evaluating deviations from airport processes.

1. Criterion - severity

This criterion assesses the worst potential occurrence which can emerge due to the deviation.

Quantitative evaluation maintains usual way of risk evaluation in the aviation industry. Severity is, however, divided into four groups, namely human, equipment, environment and operations. Each of the groups has different evaluation scale.

Severity evaluation of the worst possible occurrence with respect to its impact on employees and passengers follow the scale in tab. 1 [9,10]. Evaluation of the worst possible occurrence impact on environment and infrastructure is given by the scale in tab. 2 [9]. Evaluation of the impact of the worst possible occurrence impact on aircraft and ground technology is shown in tab. 3 [11]. Evaluation of the worst possible occurrence impact on operations is shown in tab. 4.

Tab. 1 Evaluation scale for worst possible occurrence impact on passengers or employees - human group

No effect	1
Decrease in passengers or employees' comfort	2
Significant decrease in passengers or employees' comfort	3
Potential minor injuries to passengers or employees	4
Hazard scenario with major injury or loss of life	5

Tab. 2 Evaluation scale for worst possible occurrence impact on infrastructure and environment - environment group

No or minimal local impact on the environment, which can be simply removed with little resources	1
Impact on the environment of extensive character, which can be removed with significant resources	3
Impact on the environment which cannot be removed or requires intervention from the outside of the organization	5

Tab. 3 Evaluation scale for worst possible occurrence impact on aircraft and ground equipment - equipment group

No effect	1
Ground technology is serviceable with reduced performance	2
Ground technology is unserviceable but repairable	3
Ground technology is unserviceable and unrepairable or aircraft damaged - no AOG	4
Aircraft damage - AOG	5

Tab. 4 Evaluation scale for worst possible occurrence impact on operations - operation group

No effect	1
Minor effect on ground operations	2
Effect on ground operations leading to delay of several flights	3
Significant delay of several flights	4
Flight cancellation or significant delays of many flights	5

2. Criterion - detectability

Detectability determines the likelihood of correct deviation detection in a system before the deviation impacts a process or a system. The value of detectability expresses the capability of a system to correctly and timely detect failure and departure from safe operations. Evaluation scale is shown in tab. 5.

Tab. 5 Evaluation scale for deviation detectability

High likelihood of deviation detection before it happens	1
Likelihood of deviation detection immediately before it happens	2
Deviation is detected when it happens	3
Deviation is detected during or after it happens	4
Deviation is not detected or is detected too late	5

3. Criterion - controllability

Controllability expresses the property of a system to timely react to a deviation and control the process within safety margin by means of available inputs, i.e. active control of emerging situations. It encompasses the existence of effective and suitable measures for control or stopping a deviation, or for limiting the consequences to a minimum, i.e. to acceptable level [12]. Evaluation scale is shown in tab. 6.

Tab. 6 Evaluation scale for deviation controllability

Deviation is automatically controllable - use of automation	1
Deviation is easily controllable	2
Deviation is hardly controllable	3
Only deviation consequences can be controlled	4
Deviation is completely uncontrollable	5

4. Criterion - time margin

This criterion aims to evaluate the difference between time available and the actual time needed for correct execution of a process. This difference is referred in this methodology to as a time margin. Sufficient time margin, i.e. situation where an employee is not stressed, has no influence on the deviation, which can emerge during operations.

Low, no or even negative time margin leads to stress situation, which increases the likelihood of a deviation. Given the goal conflict, where an activity is to be carried out despite insufficient time, an employee is subconsciously pushed to value efficiency more than thoroughness and that implies lower quality of his or her work. This leads to deviations in a controlled process. Evaluation scale for time margin in depicted in tab. 7.

Tab. 7 - Evaluation scale for time margin

Process has no time limitations	1
Process provides comfort time margin	2
Process provides minimal time margin	3
Process provides no time margin	4
Process provides negative time margin (time needed is more than time available)	5

3.4.2 Deviation evaluation

Deviation evaluation requires the establishment of three indices that are part of the resulting deviation evaluation vector. The determination of these indices is based on a functional correlation of the criterion severity with other criteria. Severity, as a criterion is given by the nature of the deviation similar to standard risk matrix. On the contrary, the other three criteria are capabilities of the control system employed to avoid or control the deviation. Therefore, severity is compared with other criteria in order to put both of them in a single context, i.e., potential effects of the deviations and possibility of their prevention. This supports the basic idea of the methodology and the theory of STAMP, that safety is also a system control issue. Consequently, the ability of the control system to adequately detect and control issues, should

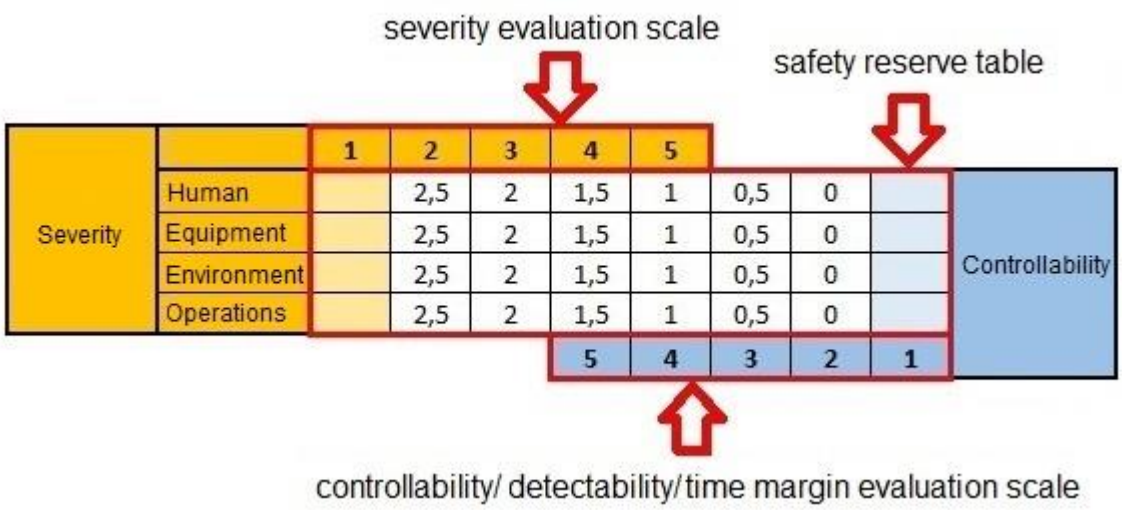
be evaluated during risk assessment. This is a main reason why the criteria are evaluated in one matrix.

Three resulting indices are needed for evaluation of ability to control deviations:

- Controllability index
- Detectability index
- Time margin index

The following table represents an illustration of the functional correlation, here with controllability index (Table 8).

Tab. 8 Functional correlation between severity and controllability criteria



The severity criterion with individual groups (human, equipment, environment and operations) is shown in the left part of the table and the direction of the evaluation table goes from left to right. The right scale represents a controllability criterion, where the evaluation goes from right to left. Evaluation for the other two criteria (indices), i.e. detectability and time margin is done in the same way. The central part of the table is called safety reserve. The safety reserve is determined by the sum of values from the white color (unused) fields of the central part of the table and thus represents an imaginary safety reserve in the management of a particular deviation. The value of the calculated reserve now becomes the value of a particular index, in this example the index in controllability. The values within safety reserve table range from 0 to 2.5. Such setting is only a recommendation and the users can adjust these according to their own needs. However, the proposed table (Tab. 8) was calibrated in an airport environment and provides accurate results.

While setting the values of the safety reserve table, the basic rules must be followed:

- Values from the left (severity) to right (other criterion) side always have a downward trend, in this methodology an arithmetic progression. - This ensures that in case of low severity and low controllability there is still sufficient safety space left. Such value setting gives a higher weight to the severity criterion.

- The lowest value in the safety reserve table is 0
- The maximum value of the safety reserve is the sum of all reserves when both correlated criteria have the value 1
- The minimum safety reserve is the negative value of the overlapping fields of the two correlated evaluations
- If there is an overlap in any part of the table, only the negated values from the overlaid table cells are counted as the resulting index
- If the difference of the values between the one or more evaluated severity groups are two or more units, the values in the lower units are multiplied by the so-called factor (coefficient)

For clarity and better understanding, various calculated scenarios are shown in the following tables and the retention of these rules is explained.

Tab. 9 The maximum index values in case of the highest severity of all groups and the best controllability

Severity		1	2	3	4	5				Controllability
	Human						0,5	0		
	Equipment						0,5	0		
	Environment						0,5	0		
	Operations						0,5	0		
					5	4	3	2	1	

Tab. 9 shows an example of a situation where for the given deviation, which has the highest severity value for all groups and at the same time the highest value of controllability, the resulting value of the safety reserve, i.e. the controllability index is evaluated as 2. Yellowed-colored fields represent the "used" fields of the safety reserve by the high severity of a particular deviation (assessed with the value 5 for all groups). On the other hand, the high controllability (evaluated with the value 1) preserves the central table fields, i.e. there are 8 fields with the cumulative sum of all values equal to 2, which form the resulting index value. This value is borderline in terms of risk management, as it points to a very problematic deviation in terms of severity, but also includes information about a well-set deviation management.

The following table (Tab. 10) shows the lowest value of the safety reserve. The lowest value is the sum of the negated safety reserves in the overlapping area. In this example, severity is evaluated as the highest for all groups. Low controllability is evaluated with the rating 5. The red-colored area represents overlapping fields. This shows a lack of the safety reserve, which is expressed by the cumulative sum of the negated values of the original reserve table (in this case the cumulative value is -10).

Tab. 10 The lowest index value

Severity		1	2	3	4	5				Controllability
	Human				1,5	1				
	Equipment				1,5	1				
	Environment				1,5	1				
	Operations				1,5	1				
					5	4	3	2	1	

The following tables show the principle of the index value decrease and multiplication of the de-emphasized values with a factor, i.e. a coefficient that increases the relevance of the most problematic value of severity.

Tab. 11 Difference of the severity evaluation for one group is higher by one evaluation unit

Severity		1	2	3	4	5				Controllability
	Human			2	1,5	1	0,5			
	Equipment		2,5	2	1,5	1	0,5			
	Environment		2,5	2	1,5	1	0,5			
	Operations		2,5	2	1,5	1	0,5			
					5	4	3	2	1	

Table 11 shows that in the case of severity assessment, where the values for individual groups differ by only one unit, this value is just subtracted.

Tab. 12. Difference of the severity evaluation for one group is higher by two evaluation units

Severity		1	2	3	4	5				Controllability
	Human				1,5	1	0,5	0		
	Equipment		0,75	2	1,5	1	0,5	0		
	Environment		0,75	2	1,5	1	0,5	0		
	Operations		0,75	2	1,5	1	0,5	0		
					5	4	3	2	1	

In the case where the difference of one or more severity values are two or more units, the values in all unused fields of the previous column are multiplied by a factor that is set to 0.3. The reserve values in the respective column are multiplied by a factor once, if the difference of severity between any two groups is two units, twice if difference is three units, and three times if the difference is four units. Tab. 12 shows that the values in the first column are multiplied by 0.3, while the values in the following columns remain the same (difference less than two units).

Tab. 13. Difference of the severity evaluation for one group is higher by two or more evaluation units

Severity		1	2	3	4	5				Controllability
	Human					1	0,5	0		
	Equipment				1,5	1	0,5	0		
	Environment		0,07	0,6	1,5	1	0,5	0		
	Operations		0,07	0,6	1,5	1	0,5	0		
					5	4	3	2	1	

Tab. 13 shows factor multiplication when the severity value is two or more units higher in more than one evaluated group. In the model situation, the value of severity for a human group is three units higher and for a equipment group it is two units higher than the values of the other two groups. The values in the unused fields of column 2 are three times multiplied by a factor. They are multiplied twice because the value of the first group is three units higher, and once more, because the value of the second group is two units higher than the remaining two groups.

The result of overall deviation assessment is a determination of the safety reserve for each criterion. These values are the components of the final evaluation vector. The resulting evaluation of the deviation in question is composed of the size of the determined indices for the criteria of detectability - v_1, controllability - v_2 and time margin - v_3.:

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

If necessary, the parameters that play an important role in given situation, such as weather, inappropriate process frequency, where deviations could occur, or increased safety importance of the given deviations, could be included in order to reduce or increase the size of the safety reserve. These are represented through additional coefficients, multiplying the values of the safety reserve table. In this case, the parameter coefficients would be set by the users in accordance with their requirements.

3.4.3 Limit values of deviation evaluation

After the deviation evaluation process is completed, the results are compared to the new scale (Fig. 10), which sets significant thresholds. The scale follows similar logic as the risk matrix, used in current safety management systems. Four colors are determined for each segment, which represent the level of risk acceptance. For better compatibility with the current risk matrix[2], descriptions of the color segments are similar (red - unacceptable risk, orange - undesirable risk, yellow - tolerable risk, green - acceptable risk). Since the final evaluation consists of three indices, each is evaluated individually and may have a different level of risk.

[2] For the sake of practicality, this methodology retains basic compatibility with risk representation in a risk matrix (color-coded zones) to facilitate its implementation in the aviation industry.

It is important to note that the standard risk matrix consists of three colors. In this case, the orange color is added to refine the scale as an example of a more detailed description of the risk and can be used according to the users' needs.

Threshold values of individual segments are based on calculations of problematic scenarios (see Fig. 9):

- Value 2 - all severity criteria groups are evaluated as 5, second criterion has value 1 or 2 (indicates satisfactory level of management of safety mechanisms, however highlights the seriousness of possible deviation impact)
- Value 8 - all severity criteria groups are evaluated as 2, second criterion has value 5 (indicates poor control of safety mechanisms and at the same time relatively low but not minimal severity)
- Value 14 - all severity criteria groups are evaluated as 2, the second criterion has value 4 (points to the state where all criteria are at the acceptance limits and any deterioration is not considered as acceptable)

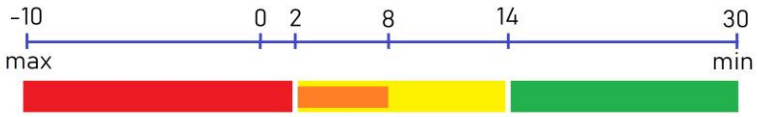


Fig. 9 - New scale of risk acceptance

3.4.4 Process evaluation

In case of a process with sets of deviations, the process is evaluated as a whole by the most critical values of all evaluated indices (even in case the indices classify each a different deviation from the sets of deviations in the process) and simultaneously by arithmetic average of all safety reserves in the process (i.e. safety reserves of all deviations), expressing the room for process improvement.

The most critical deviation is the one with least cumulative sum of all criteria safety reserves.

3.5 System level evaluation

The result of all previous steps is list of deviations and their evaluation by means of vector of indices of safety margin. The evaluation requires no estimation of likelihood as in standard risk matrix, only evaluation of criteria from chapter 3.4.1. The result is also an evaluation of processes, i.e. sets of deviation which can emerge in a process, e.g. fueling of an aircraft. The last step is analysis of all deviations in the context of a system as a whole.

This methodology proposes in this respect simultaneous utilization of both general solutions according to the theory of STAMP, i.e. evaluation of mitigation potential so as evaluation of set of questions regarding the safety study as a whole.

3.5.1 Mitigation potential

As already mentioned in chapter 3.1, this potential evaluates identified hazards from the perspective of possibility of mitigating risk, which relates to them. Here, it is important to distinguish hazards (deviations), which require mitigation measures from those, which are already considered acceptably safe. Further, it is necessary to distinguish, which type of mitigation measure is taken. Deviation evaluation in this respect follows the scale from tab. 14.

Tab. 14 Evaluation of mitigation measures from the perspective of risk mitigation potential

1. Deviation requires no mitigation
2. Deviation mitigation aims at hazard (deviation) elimination
3. Deviation mitigation aims at improvement of controllability, detectability of time margin
4. Deviation mitigation aims reducing severity, i.e. exposure to the deviation
5. Deviation mitigation aims at damage reduction

Evaluating the overall mitigation potential is given as a statistics of individual types of measures distribution as per the tab. 14. By means of distribution evaluation, safety analyst gains complete overview about respective safety study, especially indirect overview of possible likelihood of unwanted consequences of hazards.
The most desired is a state where all deviations can be classified from the perspective of mitigation by 1. or 2. type from tab. 14. Increasing the ratio of measures from 3. type and then especially 4. and 5. indicates safety limitations in the proposal for system change. Overall, measures of 5. Type should not be present in a safety study at all, nevertheless acceptable level of individual types distribution is to be considered in a context of particular safety study.

3.5.2 Evaluation of a set of system-level questions

In this step it is necessary to consider the evaluated proposal of change of specific safety study in the context of its impact on broader environment of the system, including parts of the system, which are not directly evaluated in the safety study. This methodology proposes as a basic set of system-level questions those included in tab. 15.

These system-level questions comprise only a check-list at the end of a safety study and responses to the questions should help safety analyst to conclude the assumptions and arguments for final decision about implementation of the assessed proposal from the perspective of safety. In a combination with all previous steps of this methodology, complete evaluation of a change is achieved. Ideally, several alternatives for change implementation should be assessed are evaluated, if alternatives exist, and safety study should be performed repetitively with all the steps in this methodology during the development of a change proposal. This way the overall proposal can be optimized with regard to safety.

Tab. 15 System-level questions

1. Does the proposed change require implementation of new type of measures for risk mitigation?
2. Can the proposed measure reduce the effectivity of some currently implemented measures for risk mitigation?
3. Can the proposed change negatively affect controllability of some deviations in the system?
4. Can the proposed change negatively affect detectability of some deviations in the system?
5. Can the proposed change negatively affect time margin of some deviations in the system?
6. Can the proposed change negatively affect severity of some deviations in the system?

3.6 Example of risk evaluation in airport processes

For better comprehension of the risk assessment according to this methodology, an example of deviations from the airport environment will be analyzed. Taxing of a critical aircraft type will serve as the example process for analysis. The process is shown in Fig. 10.

The created process map enables basic safety analysis and definition of the individual deviations, which are then used for hazard identification. The result of identifying the deviations from this process is the following list:

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

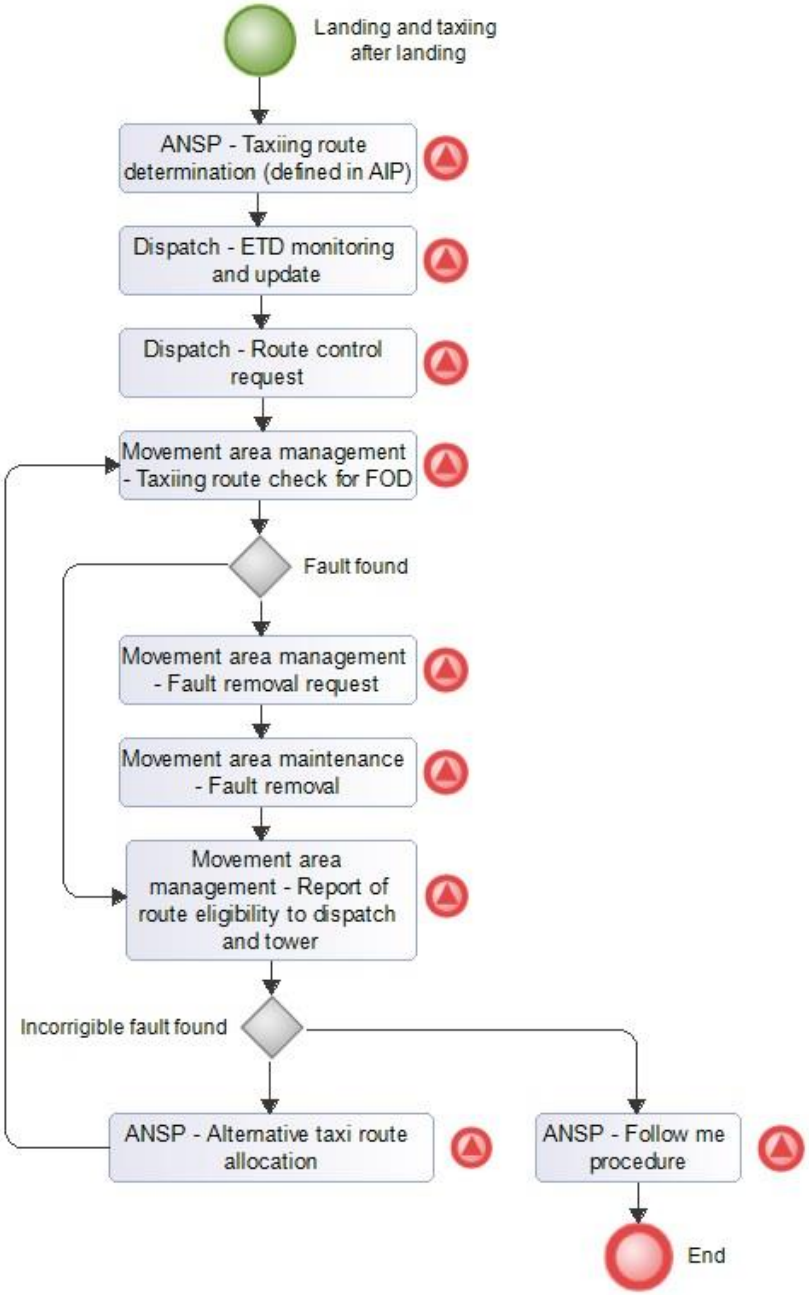


Fig. 10. Process map - taxing of the critical aircraft type

The following step includes hazard identification. As explained in the chapter 3.2, hazards are identified for individual process, as a worst possible scenario according to the predefined deviations. Tab. 16 shows a list of identified hazards related to particular process steps from Fig 10.

Tab. 16 System-level hazards

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

The next step is a risk assessment. An example will be conducted for two selected deviations, namely:

1. Do not check the entire area (from the TWY axis to the taxiway strip boundary to both sides)_Movement area Management
2. Do not pass the information_Movement area Maintenance

Risk assessment for the first of the deviations is performed by a qualified safety expert for all severity criteria groups. The given deviation achieves the following values:

Human - 2 (Decrease in passengers or employees' comfort - it does not have direct impact on passengers or other personnel included in the process. Delay or operation change could be expected in case of outcome related to the collision of the aircraft and FOD on the TWY)
Equipment - 3 (Ground technology is unserviceable but repairable - direct impact on the aircraft or vehicles after collision with the FOD. Aircraft landing gear damage possible and require closure of the TWY and aircraft towing procedure)
Environment - 1 (No or minimal local impact on the environment, which can be simply removed with little resources - environment not endangered in the majority of possible outcome scenarios)
Operations - 3 (Effect on ground operations leading to delay of several flights - Closed TWY and ground equipment engaged for the towing operation)

The evaluation severity will be the same for determining individual indices. Other criteria were evaluated as follows:

Controllability - 3 (Deviation is hardly controllable - procedure already performed, no revision process defined or checking equipment used)
Detectability - 2 (Likelihood of deviation detection immediately before it happens - possibility for the flight crew to react in case of obstacle on the ground)
Time margin - 2 (Process provides comfort time margin - 30 minutes allocated for the whole procedure)

Utilization of the functional correlation table with these example values is shown below:

Controllability index

Severity		1	2	3	4	5				Controllability
	Human			2	1.5	1				
	Equipment				1.5	1				
	Environment		0.2	2	1.5	1				
	Operations				1.5	1				
					5	4	3	2	1	

Detectability index

Severity		1	2	3	4	5				Detectability
	Human			2	1.5	1	0.5			
	Equipment				1.5	1	0.5			
	Environment		0.2	2	1.5	1	0.5			
	Operations				1.5	1	0.5			
					5	4	3	2	1	

Time margin index

Severity		1	2	3	4	5				Time margin
	Human			2	1.5	1	0.5			
	Equipment				1.5	1	0.5			
	Environment		0.2	2	1.5	1	0.5			
	Operations				1.5	1	0.5			
					5	4	3	2	1	

The overall deviation risk assessment is represented by the vector:

v = (**14.2; 16.2; 16.2**)

According to the established risk acceptance scale, the values of this deviation fall into the acceptable risk category, all indexes are higher than 14, thus falling into the green zone.

The evaluation of the second deviation is shown in the tables below.

Controllability index

		1	2	3	4	5			
Severity	Human			2	1.5	1	0.5		Controllability
	Equipment		0.75	2	1.5	1	0.5		
	Environment		0.75	2	1.5	1	0.5		
	Operations				1.5	1	0.5		
					5	4	3	2	1

Detectability index

		1	2	3	4	5			
Severity	Human			2	1.5	1	0.5		Detectability
	Equipment		0.75	2	1.5	1	0.5		
	Environment		0.75	2	1.5	1	0.5		
	Operations				1.5	1	0.5		
					5	4	3	2	1

Time margin index

		1	2	3	4	5			
Severity	Human			2	1.5	1	0.5		Time margin
	Equipment		0.75	2	1.5	1	0.5		
	Environment		0.75	2	1.5	1	0.5		
	Operations				1.5	1	0.5		
					5	4	3	2	1

The overall deviation risk assessment is represented by the vector:

v = (**19,5**; **19,5**; **19,5**)

According to the new risk acceptance scale, this is an acceptable risk, all indices fall into the green rating zone.

4. Novelty of the methodology

In the context of current standards of safety studies execution in airports, there are two key novelties. First novelty regards application of the theory of STAMP with standard business process modeling, which facilitates STAMP application in aviation industry. Second novelty regards implementation of comprehensive framework of quantitative methods, which complement the theory of STAMP and its methodologies, such as the STPA and some steps which relate to it.

4.1 Comparison with STAMP and STPA methodology

This methodology is founded on the theory of STAMP and it provides alternative approach to achieve the results of STPA methodology. The main difference is that the proposed methodology can be directly applied with other, managerial processes of an airport operator (if they exist), by means of business process modeling. In this sense it supports application of the theory of STAMP and it is fully compatible with it. Where process documentation does not exist and where it is highly impractical to establish such documentation with sufficient level of detail, STPA is more suitable. Even in such cases, the quantitative framework from this methodology can be combined with conventional STPA to achieve both hazard and risk analysis Apart from the base concepts of feedback control and system theory, the methodology works with several additional ideas from the theory of STAMP, especially the problematic nature of probability estimation in the context of risk evaluation in safety studies, which it interconnects with specific domain in the aviation and so it also brings the theory of STAMP closer to practical industrial application.

4.2 Comparison with aviation industrial standards

Current industrial standards for management of change are laid down by aviation standard L19 in the Czech Republic [13], and ICAO Annex 19 [14] and also ICAO Doc. 9859 Safety Management Manual by the International Civil Aviation Organization (ICAO) [2] globally. Provisions of these standards are, however, rather generic and require no specific method which should be applied to the process of change management. In the aviation, however, the Safety Assessment Methodology (SAM) [3] by the European Organisation for the Safety of Air Navigation (EUROCONTROL) with its variations is used most often for the purpose. Despite the details provided by the SAM methodology, it does not strictly specify method to be used for hazard identification and the user typically selects one of listed methods in the SAM documentation at own discretion. This is usually based on various prediction models of safety, such as Swiss cheese model or older methods such as Hazard and operability study (HAZOP), Fault Tree Analysis (FTA) and its variations. Risk matrix is then used for risk evaluation.

This methodology brings novelty with respect to the mentioned industrial standards by utilizing STAMP prediction model of safety for hazard identification but also as an input for risk evaluation. The methodology demonstrates how to practically employ the theory of STAMP in airports and timely identify safety issues, that cannot be identified with older prediction models and methods. Through implementation of the theory, processes related to risk analysis given by the SAM methodology are customized and do not rely on the combination of older prediction

models of safety, which SAM recommends. The process of risk evaluation is then modified to limit subjective evaluation, especially in terms of the problematic aspects of probability evaluation.

5. Application of the methodology

This methodology describes new procedure for executing safety studies in the aviation, with the focus on airports, and it corresponds to the processes of management of change in a Safety Management System (SMS) of aviation organizations. The methodology can be applied in several contexts described below. Even though it contains innovative solution, which is not required by current legislation or aviation standards, application of the methodology conforms to the current legislation and industrial standards, it positively affects processes of management of change and increases awareness of current and priority safety issues of airports. Overall, it contributes to further improvement of operational level of safety.

The methodology can be applied in the context of implementing provisions of L19 Czech aviation standard or ICAO Annex 19 so as specific provisions of the ICAO Doc. 9859 Safety Management Manual pertaining management of change of the industrial SMS systems.

The methodology can be applied in the context of current European legislation regarding administrative procedures for airports, which are subject to Commission Regulation No. 216/2008 [15], especially in the context of Commission Regulation No. 139/2014 [16].

The methodology can be applied in the context of SAM methodology by the European Organisation for the Safety of Air Navigation (EUROCONTROL) in case safety study is executed according to this methodology.

6. Economic aspects

Application of the methodology induces several costs related to its implementation. These regard new procedures for safety studies execution, which are more demanding for execution than current industrial standards in the aviation, especially regarding airports. Safety analyst should be familiarized with process documentation of respective organization, identify relevant procedures and draft future changes, i.e. also provide necessary inputs for updating process documentation. In some cases, it may be beneficial to increase the number of employees with the responsibility for safety studies execution in respective organization, even though this methodology does not consider such measure necessary for its implementation.

Implementation of the methodology does not require special IT tool to be developed. From the engineering perspective, the methodology does not require further systemic changes, which eliminates additional engineering and production costs. Process description needed for the methodology is performed with the existing BPMN solutions, while risk analysis can be performed with standard MS Office software. This process, including the establishment of the hazards and deviations list, is a task of the safety experts within the given organization. Estimated time for carrying the tasks depends on the size of the respective organization. For

the training and methodology implementation into the safety assessment process approximately a 3-days workshop would be needed.

Potential economic benefits relate to the increased level of operational safety, which can be assured in the management of change processes of airports. The methodology brings new way how to effectively identify and further manage larger amount of safety issues than with current safety studies, thus it has the potential to allow for timely and usually also less expensive mitigation measures related to the issues. The methodology is also focused on risk evaluation; it assumes quantitative procedures by which it decomposes some merely subjective aspects of current procedures for executing safety studies. This way it positively influences prioritization of safety issues and eventually enables better resources allocation for assuring acceptable level of safety in operations.

As an additional point, the methodology has the potential to improve other domains than safety, despite originating in safety. These domains regard for example quality and process management or security management in airports. Versatility of the procedure is grounded with the utilization of BPMN, thus integrating the methodology with standard business processes and their management, so as the theory of STAMP, which has the potential to provide support for other domains.

References

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

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

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

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

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

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

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

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

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

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

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

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

[13] Ministry of Transport, Czech Republic. Letecký předpis L19 - řízení bezpečnosti. Číslo jednací 166/2013-220-LPR/1, 2013.

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

[15] Regulation (EC) No 216/2008 of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, OJ L 79 http://data.europa.eu/eli/reg/2008/216/oj

[16] Commision Regulation (EU) No 139/2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council. OJ L 44. Available from: http://data.europa.eu/eli/reg/2014/139/oj

List of publications preceding the methodology

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

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

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

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

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