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.

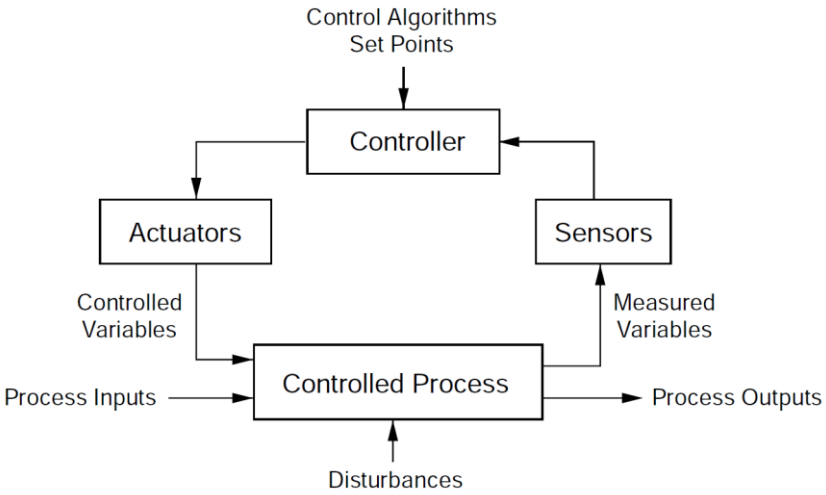


Fig. 1 Control loop as a basic concept of feedback control [4]

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.

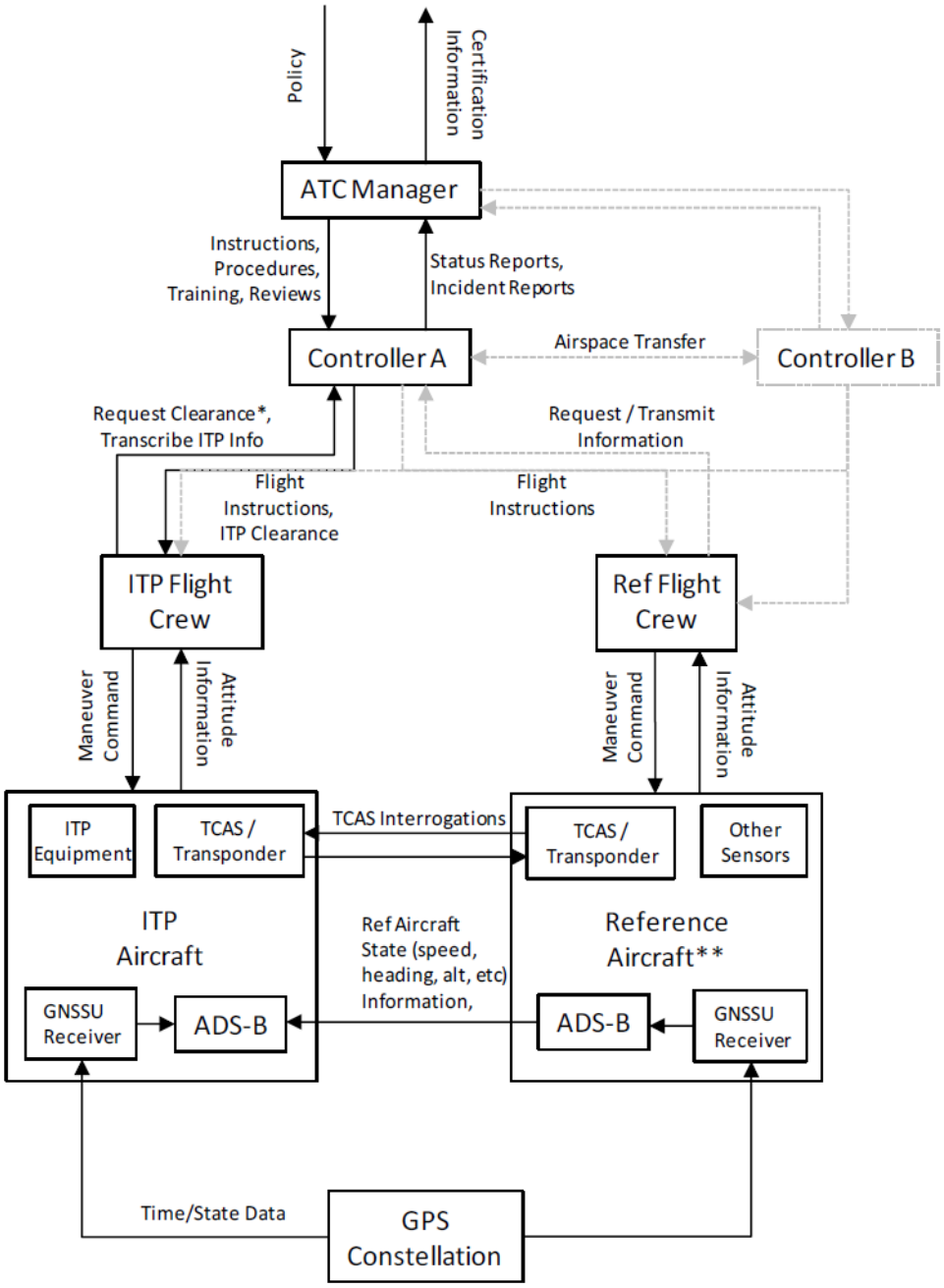


Fig. 2 Example safety control structure in aviation according to STAMP - the situation depicts two aircraft controlled by an air traffic controller [5]

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

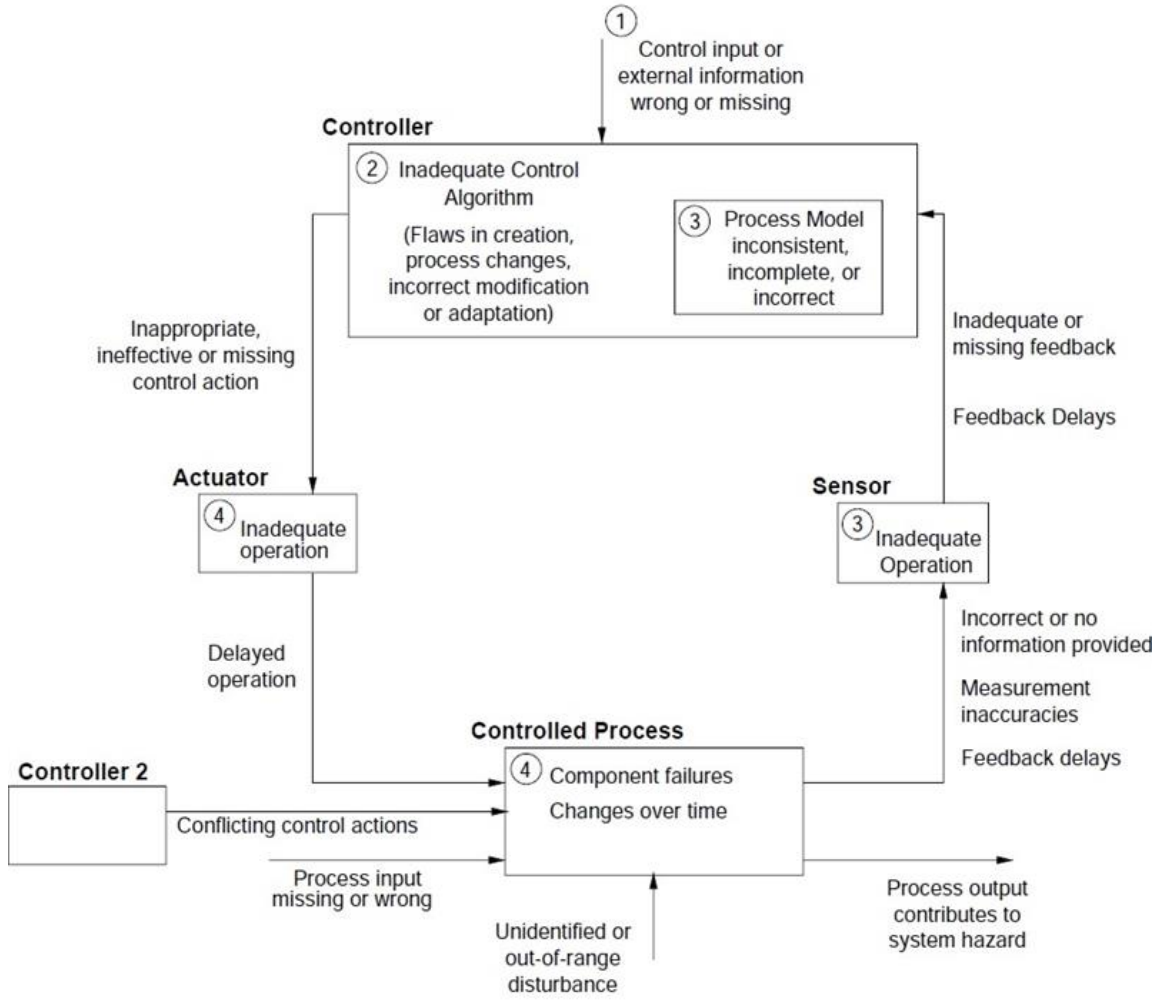


Fig. 3 Basic causal control model for scenario generation for identification of hazards and safety issues taxonomy based on the theory of STAMP [4]

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.

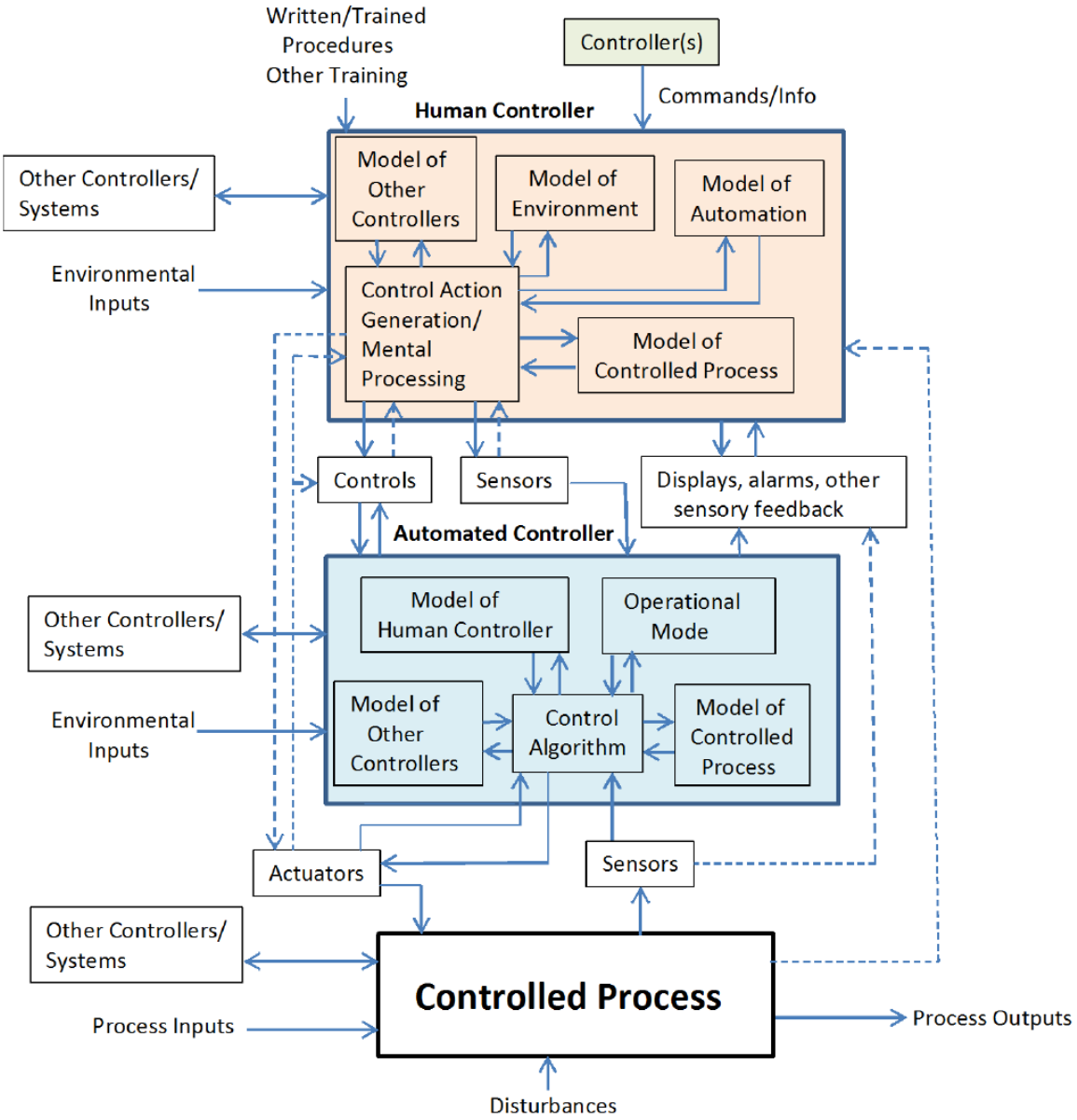


Fig. 4 Extended causal control model for scenario generation for identification of hazards based on the theory of STAMP. Combination of the causal control model with basic taxonomy of safety issues from Fig. 3 provides extended taxonomy of safety issues according to the theory of STAMP. Intermittent 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

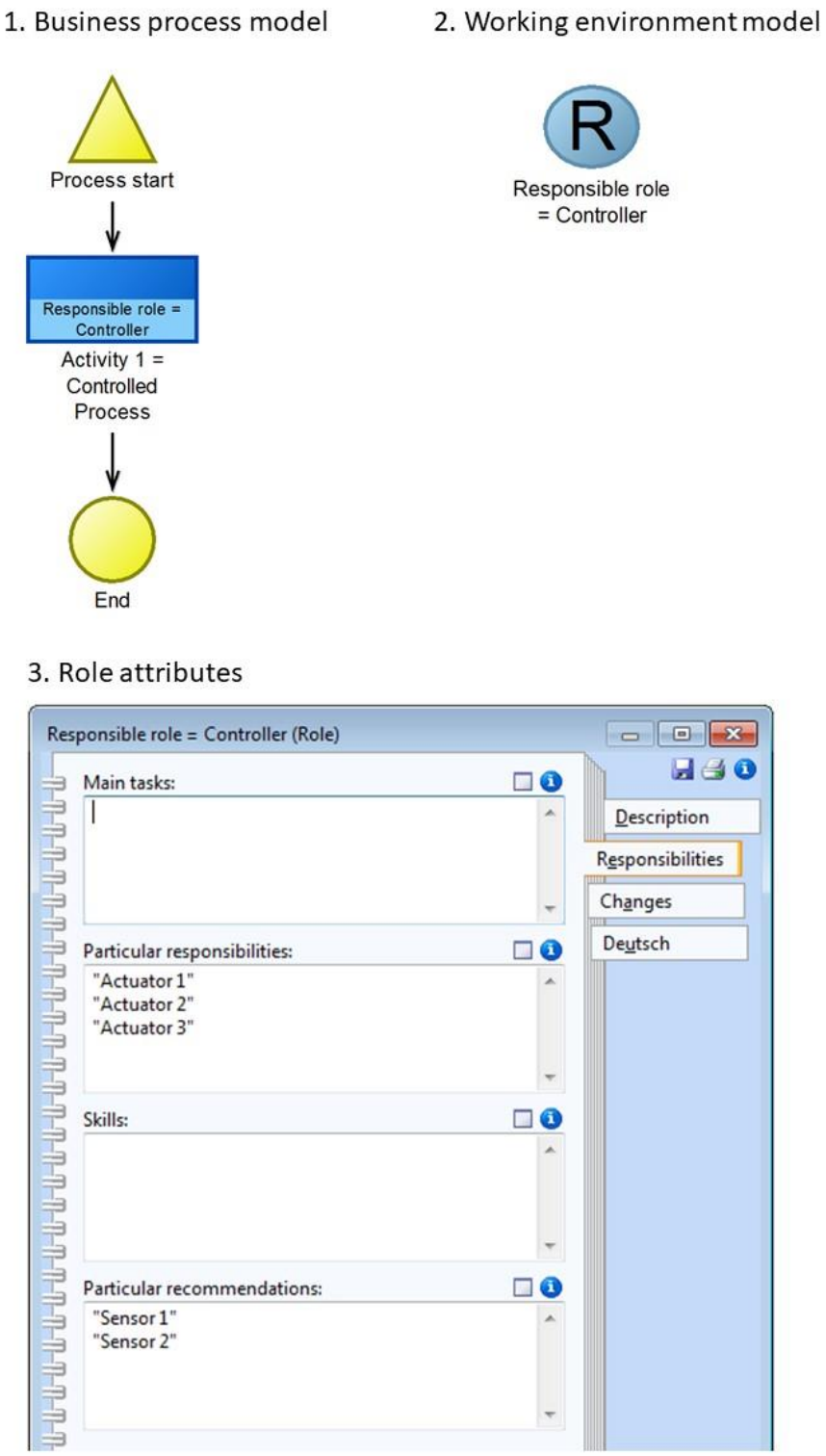


Fig. 5 Utilization of a tool for process modeling to insert information necessary for analyses based on STAMP

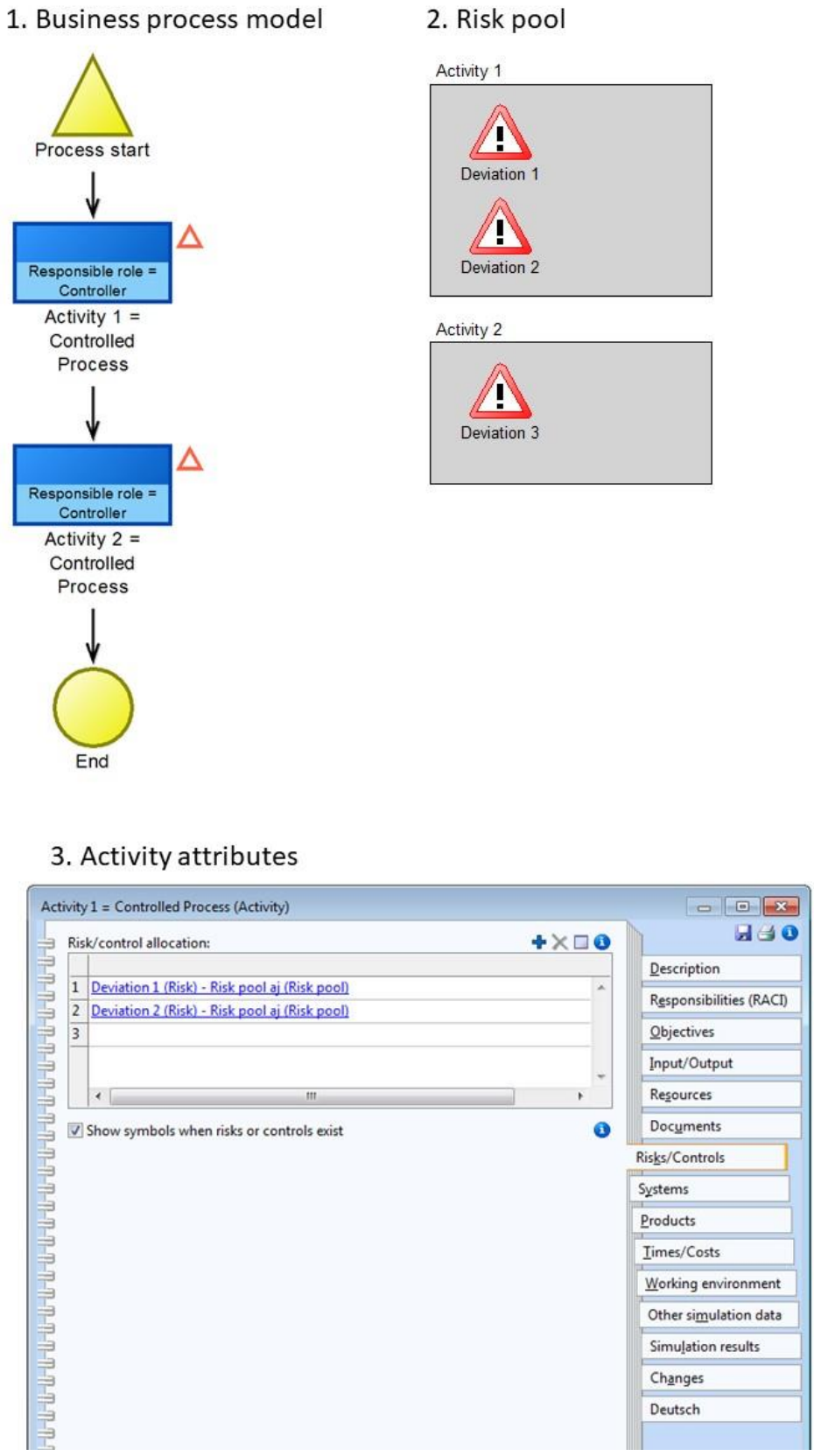


Fig. 6 Utilization of a tool for process modeling to insert information about deviations from defined activities in a process

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.

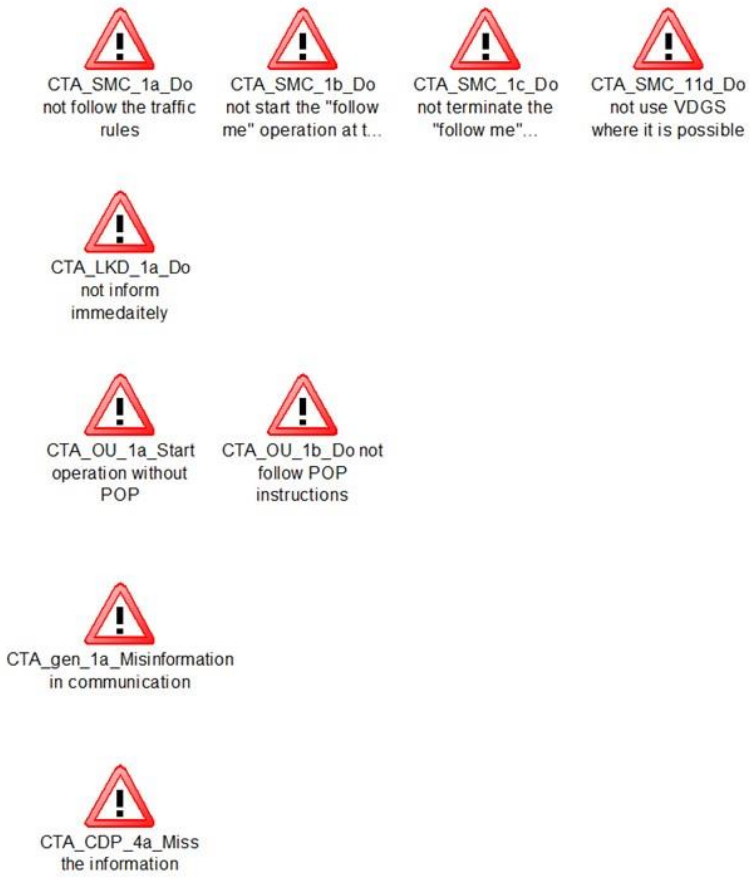


Fig. 7 Example of a list of deviations extracted from a process model

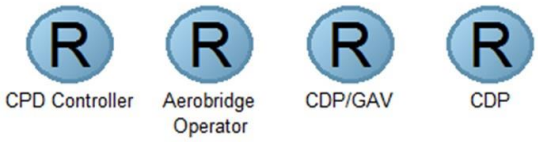


Fig. 8 Example of a list of controllers extracted from a process model

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

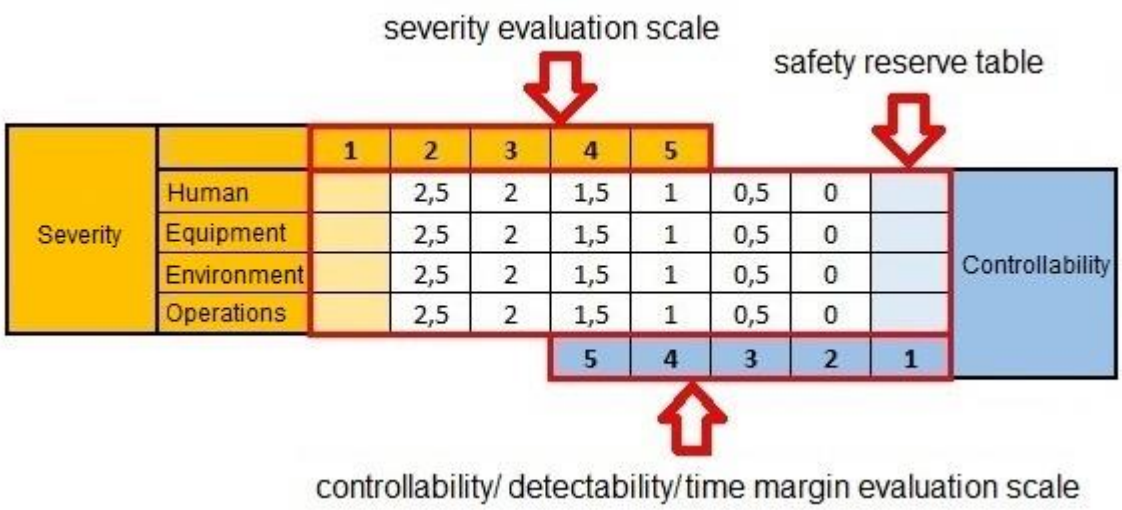
be evaluated during risk assessment. This is a main reason why the criteria are evaluated in one matrix.

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)

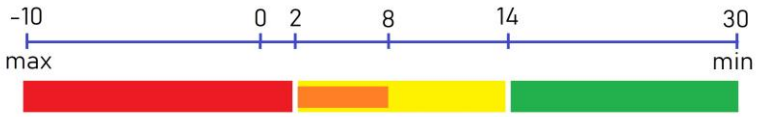


Fig. 9 - New scale of risk acceptance

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

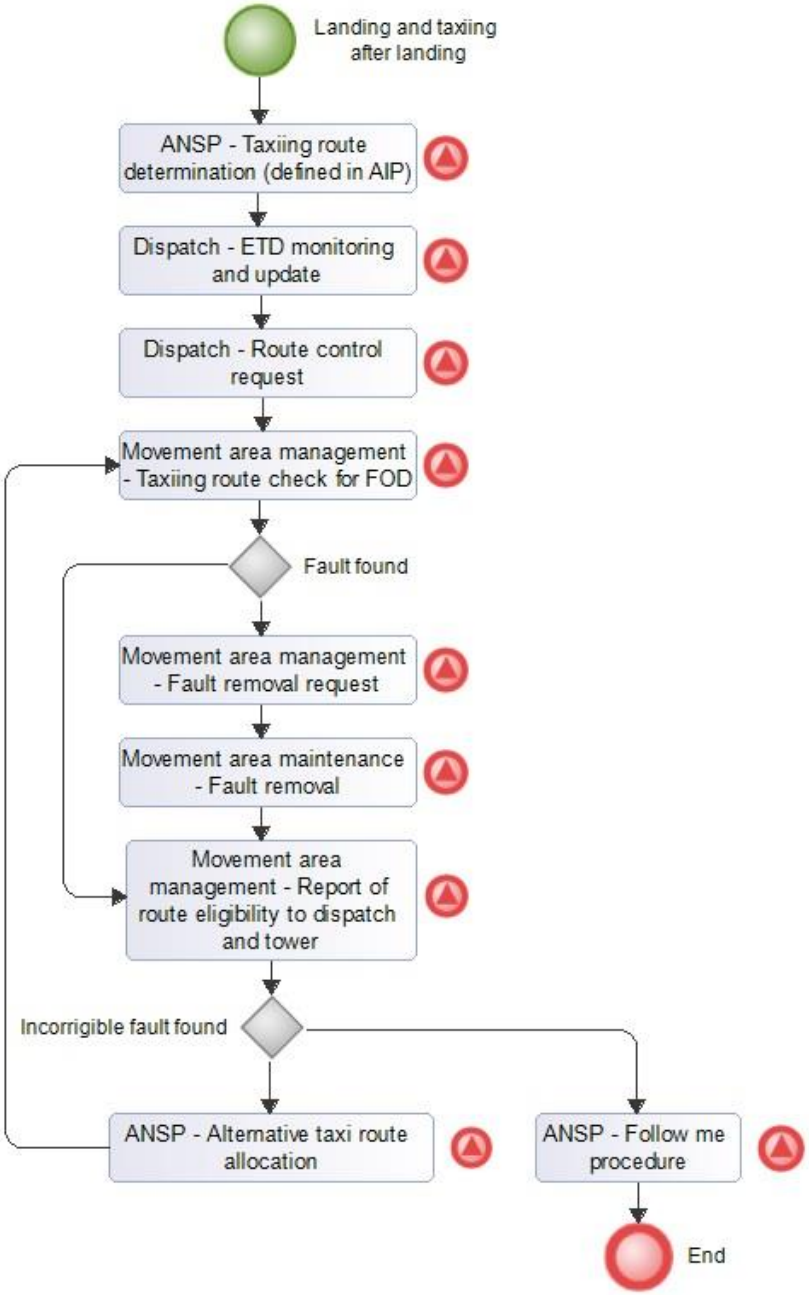


Fig. 10. Process map - taxing of the critical aircraft type

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.