METHODOLOGY

for using the theory of STAMP safety model by the Civil Aviation Authorities

Project TA ČR Program DOPRAVA 2020+ No. CK01000073

Department of Air Transport
Faculty of Transportation Sciences
Czech Technical University in Prague

Lališ Andrej
Grötschelová Kateřina
Stojić Slobodan

Program **Doprava 2020+**

Methodology for using the theory of STAMP safety model by the Civil Aviation Authorities

Contents

Introduction

Aviation safety oversight is one of the pillars of safety management of modern air transport. The role of oversight institutions is crucial, particularly because they are tasked with meeting the public's demand for safe air transport. Due to the impartiality requirement, the Civil Aviation Authorities are responsible for this. Over the course of their mandate, they have developed their own system by which they oversee safety in aviation organizations. It is a combination of compliance monitoring based on regulatory requirements with the experience of officials gained from the oversight activities who interact with the organizations. In some respects, the monitoring of safety performance, to which aviation has been moving for a long time, plays a role.

Assessing the actual level of safety of a particular organization is a non-trivial task. Compliance with requirements does not guarantee a high level of safety, and the identification of problematic aspects of air transport often depends on the experience of the officials. However, several approaches and methods have emerged recently in safety engineering to address this problem. These are methods designed both to identify hazards and risks, as well as to support safety performance measurement, including subsequent audits and inspections. These methods belong to the so-called *systemic* approach to safety, which, unlike the previous approaches to safety, aims at a holistic (the so-called "system-wide") approach.

This methodology works with one of the current solutions – the Systems Theoretic Accident Model and Processes (STAMP). This safety model interprets safety as a control problem. Consequently, the focus is on how organizations are set up in terms of roles, their interactions, and responsibilities. In STAMP, safety is as a system-level property, which exists only if organizations operate safely as a whole. Moreover, in air transport, by using the terms *whole* and *system* we refer to all organizations and their interactions, including the Civil Aviation Authorities. Ensuring aviation safety in this setting it involves a dynamic process of continual setup and adjustments to aviation organizations inside and among themselves, where the Authorities are not just observer or impartial entity monitoring the operations, but they play an active role of an industry participant.

The presented methodology is the product of a research project that aimed to find a practical way to apply new theoretical discoveries of a systemic approach to safety to the practice of Civil Aviation Authorities. The goal was to answer some challenging questions from the practice about the new approach to safety, and to formalize a procedure for its application, which is presented in this document. In addition to that, it contains few practical and illustrative examples, which were verified with the Civil Aviation Authority of the Czech Republic.

In result, the document describes new methods that increase the ability of officials to identify and actively work with aviation safety issues, based on the actual level of safety performance achieved by aviation organizations. It also leads to further digitization, modernization, integration and streamlining of the processes of the Civil Aviation Authorities.

1 Goal

The methodology aims to disseminate and support the results of the research carried out by the Czech Technical University in Prague in cooperation with the Civil Aviation Authority of the Czech Republic within project No. CK01000073 funded by the Technology Agency of the Czech Republic. The methodology is a summary of the key knowledge gained in the project. It contains base procedure for safety data processing and analysis at the level of Civil Aviation Authorities with a procedure for creating audit questions for audits based on the systemic approach to safety. The methodology aims at digitization, modernization, integration and streamlining of the processes of the Civil Aviation Authority while reducing the administrative burden borne by subjects of the state safety oversight.

2 Dedication

The methodology is primarily intended for aviation state safety oversight institutions interested in improvement of safety issues identification and targeting of audits and inspections in supervised service providers. The document contains practical examples from aviation, including useful references and citations related to the domain. The methodology can be applied to other transport modes where state safety oversight is carried out, however, it may be necessary to consider modification or adaptation of respective procedures to the selected environment.

3 Methodology

This section describes the use of the STAMP model within the civil aviation authorities in the form of standalone procedures that address respective problems of STAMP application within the authorities, including practical examples. This section also describes the foundations of the STAMP model, their connection to the presented procedures and useful references to related methods.

3.1 STAMP

Systems Theoretic Accident Model and Processes (STAMP) is an accident causality model that interprets the problem of safety as a control problem. This means that both in general and in aviation in particular, the determinative is how effective controls we have over the operational processes and whether the effectiveness of our controls do not get out of hand with time. Processes in socio-technical systems need to be controlled actively or passively to achieve our goals. By control we mean any change in the status of the controlled processes that in STAMP can be made by the management of the organization, front-line personnel, automation or by physical, passive barriers.

Ensuring safety as a system-level property is therefore a matter of establishing an overall control system over the entire operations, as well as a matter of maintaining such system over time. For the purpose, STAMP uses systems theory and the concept of

control-feedback loops (Fig. 1). Establishing a control system therefore implies organizing people and technology into the hierarchy of controllers and controlled processes, distributing responsibilities among them, and setting up interactions to ensure each controller will have the necessary information about the current state of the controlled processes they control (by sensors) and means to change the state (by actuators). This is the core idea that distinguishes STAMP from other safety models (such as SHELL or Reason's model) and that enables a holistic, system-level approach to safety.

A properly established control system must be able to recognize controlled processes getting out of hand and actively intervene against the complete loss of control, which usually leads to an accident and entails the loss of something valuable. In extreme cases, such events may necessitate modification of the entire system or its respective parts if these are no longer able to effectively control the processes. The role of oversight institutions in this respect is to monitor the main features and performance of the currently operated systems. The goal is to detect undesirable degradation in a timely manner and demand corrective measures.

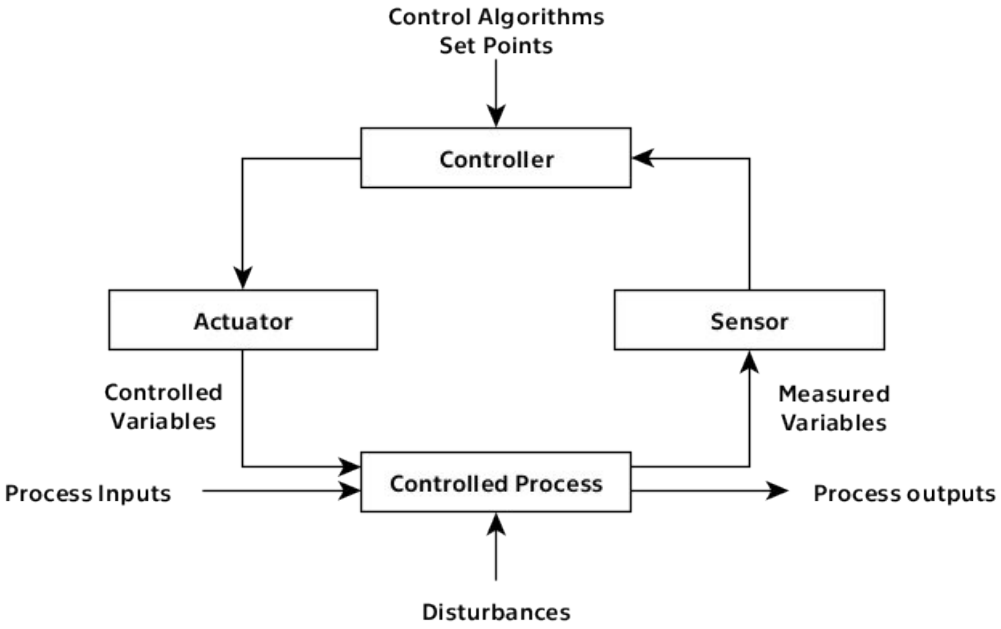

Fig. 1 – A standard control loop [1]

Real-world systems consist of a set (usually dozens or hundreds) of interconnected control loops, where it is not trivial to identify safety issues. The STAMP therefore provides methods designed to address specific safety issues using the STAMP perspective in practice. System-Theoretic Process Analysis (STPA), a hazard analysis method, and Causal Analysis based on System Theory (CAST), an accident analysis method, provide the basics. Both are introduced in separate handbooks [2, 3]. In particular, the STPA and its extension known as Active STPA [4] are key from the point of using the STAMP safety model in aviation oversight processes.

STPA is inherently a proactive method, because it allows prediction of all possible safety issues using only the description of how a particular system is designed. The input for this method can be the routinely available certification documentation of a particular service provider and specification of how they intend to operate. No historical safety data, which often does not even exist, is needed to predict possible safety issues. Nor is there a need for a deeper expert knowledge of the supervised organization, as from the point of its supervision only the principle of how the organization ensures control over its processes is relevant, not the nature of the processes as such. Should the nature of the processes be crucial, however, it can be discussed to the extent necessary directly with the service provider as part of the audits. The STPA method thus provides the oversight institution with a unique opportunity to identify problems much earlier than they would manifest from the acquired operational safety data.

The STPA outputs can be used not only to identify potential safety issues, but also as classifiers for the reported safety data, or as a basis for creating audit questions. Active STPA is an extension of the STPA designed to support such use-cases for the purpose of safety management in everyday operations. Here, the authors of STAMP point out how the STPA outputs can be used in typical processes of safety data collection and analysis, within the safety management system (SMS). Because states manage aviation safety and supervise organizations using the same SMS principles [5], Active STPA can also be used for state safety oversight functions.

In the presented procedures of this methodology, STPA is used as a base method for hazard identification and subsequent tasks, while Active STPA is used for safety data processing and analysis. Therefore, at least a basic knowledge of STPA, which can be obtained from respective handbook [2], is necessary for proper execution of the procedures based on it. Similar holds for Active STPA for the procedures which are based on the extension.

3.2 Formalization of oversight processes

This procedure is recommended when the oversight institution itself is subject to hazard analysis. As already mentioned, civil aviation authorities play not only the role of an observer and impartial entity, but in fact they play an active role as a participant of the air transport system. They can contribute to accidents by losing control of the supervised organizations and either allowing or directly supporting the emergence of hazards in air transport.

The main objective of oversight institutions is to certify and supervise aviation organizations (service providers such as airports, maintenance organizations, air carriers, etc.) to ensure an acceptable level of safety at the state level. However, the oversight institution itself is no exception and shall actively work with its processes as well. This implies, for example, internal audits to ensure that the state safety oversight functions are effective and contributing to an acceptable level of aviation safety.

Process management starts with process documentation, where individual processes are described in detail, including responsibilities and relevant references. However, the process documentation may suffer from shortcomings, e.g., the process may be described in a fragmented way and the reader (the responsible person or organizational unit) may obtain incomplete understanding or misunderstand the original intention. Another problem that may occur is the absence of responsibility assignment, simplified or merged responsibility. For example, in case of simplified responsibility a service provider or an organization can be held responsible for certain activity. If such responsibility occurs frequently in a process documentation, it quickly becomes unclear who is responsible for what and to whom the reader should refer in case of a problem.

The oversight institution, just like any other organization, can also use graphical (schematic) representation for process management, which may supplement text description. Graphical representation is particularly useful for achieving a correct understanding of the relationships between activities, especially if the processes are more complex. At the same time, it facilitates finding deficiencies in the process text description. For example, it is easy to detect if some activities have not clearly assigned responsibility or when the flow of activities is ambiguous.

For the graphical representation of processes, there are methodologies that can be followed when modeling own processes. Such a methodology that addresses this issue comprehensively and that can be used in the context of the STAMP application in oversight institution is, for example, the Methodology for Modelling and Analysis of Business Process (MMABP) [6]. The MMABP was designed for modeling and analyzing business systems and processes, but its principles apply as well to an oversight institution, especially because the methodology uses standardized modeling frameworks and languages such as the Business Process Model and Notation (BPMN) and The Open Group Architecture Framework (TOGAF) Event Diagram.

BPMN, as its name suggests, is a notation created in accordance with the current trends in business systems. The primary goal of BPMN is to standardize the description of processes throughout their life cycle, i.e., the overall workflow. Graphical notation is well understood by project managers or business analysts who actively work with processes (monitor and manage them), while it is also a technical notation that can, for example, be used by developers who implement software solutions to support process management in an organization. Business Process Diagram is the output of a process description by BPMN and it consists of a network of graphical objects, such activities and flows that define the order in which the activities should be performed.

Because the BPMN describes processes in detail, the so-called process map may be necessary to integrate several Business Process Diagrams. For example, the Eriksson-Penker process diagram or the TOGAF Event Diagram are used for the purpose. The process map then provides a global view of processes that is not available in BPMN. The BPMN, together with the process map, thus forms both a global and a detailed view of the business processes of the organization and it allows users to easily understand them. However, it is not always necessary to model business processes at both levels.

Each organization understands its own processes and typically knows best what is needed for the given purpose.

3.2.1 Process mapping with BPMN

The first step in creating process diagrams is to analyze the text documentation of the modeled process. This is done manually by the analyst reading (going through) the documentation and marking important parts that will be used to create the diagrams. It is important that the analyst is familiar with modeling elements used in process diagrams, so that they are able to find corresponding inputs in the process documentation. In certain cases, the text analysis could also be done automatically or semi-automatically with existing tools (e.g. [7] or [8]) that allow the analysis to be performed according to user's requirements to find the relevant information in the text. An example of the text analysis performed manually is shown below, with a sample extract from internal directive of an oversight institution. Important parts have been identified and marked in yellow, and subsequently used them for modeling the process into the graphical form.

1. *Should an employee of the Authority identify or suspect a safety issue when performing state safety oversight functions, they will report this without unnecessary delay to the head of the respective unit. The head of the unit will evaluate the information and if they also suspect the safety issue, they will take adequate measures to resolve it.*
2. *Part of the considered measures to resolve the safety issue must be informing other subjects, who may be influenced by the safety issue – including the EASA and other EU member states Authorities, in line with the procedure described in Section 8.*
3. *If the nature of the safety issue requires it (head of respective unit does not possess the necessary competence to take adequate measures, they cannot evaluate whether the matter is a safety issue, or the safety issue is severe enough and decision about it shall be taken at the level of higher-level management), the head of the unit will forward such information to the responsible manager, alternatively (in case of the division director), they will share the information with the board of directors, which will decide about further measures.*

Fig. 2 shows an example of TOGAF Event Process Diagram - an oversight institution process "Response to Safety Issue". The blue rectangle "Response to Safety Issue" shows the core process while the other two "Informing other subjects" and "Record keeping" are supplementary processes. Each process has its own input and output. The input for the core process is "Safety Issue detected" and the output is "Actions Taken/Decisions". The input can be provided by an external ("Other Authority or EASA") or an internal agent ("CAA Employee").

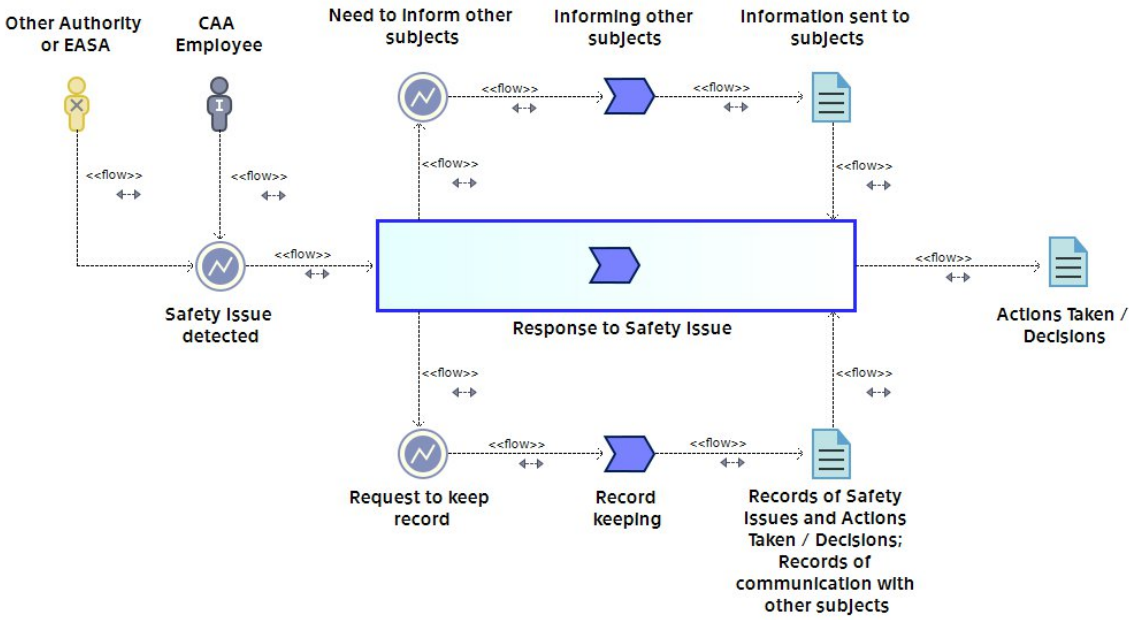

Fig. 2 - TOGAF Event Diagram of the "Response to Safety Issue" process

After the analyst creates a process map or TOGAF Event Diagram, they can proceed with modeling BPMN diagrams. Note that it is not always necessary to proceed in this order. Sometimes it may be more convenient for the analyst to model a more detailed BPMN diagrams first and then create a process map or TOGAF Event Diagram as an abstraction of the more detailed diagrams. In some cases, it may be difficult for the analyst to extract the main processes or their inputs and outputs from the text without deeper knowledge of the process details. If this is done when new processes are created, however, the recommended approach is to start from general, high-level diagrams, which help separate the core processes from the supporting ones and create an overview of their relationships.

Fig. 3 shows example BPMN diagram consisting of activities that have been highlighted yellow in the text above. From the process documentation, decision-making and alternatives for different types of problems need to be identified and captured in the BPMN diagrams. These are shown as yellow diamonds (gateways) in fig. 3 that allow branching or merging process flows. The entire BPMN diagram is divided into the so-called pools. The first part of the diagram (the first pool) is a breakdown of the aforementioned core process. Activities in the first pool have their own sub-activities or sub-processes, which are further described by other pools. This abstraction can be recognized by the small "+" character at the bottom of the rectangle (activity, see Fig. 3). Each final (atomic) activity should have a role assigned to it, which is responsible for its execution. If no role is assigned, it is usually an evidence that this information is missing in the documentation.

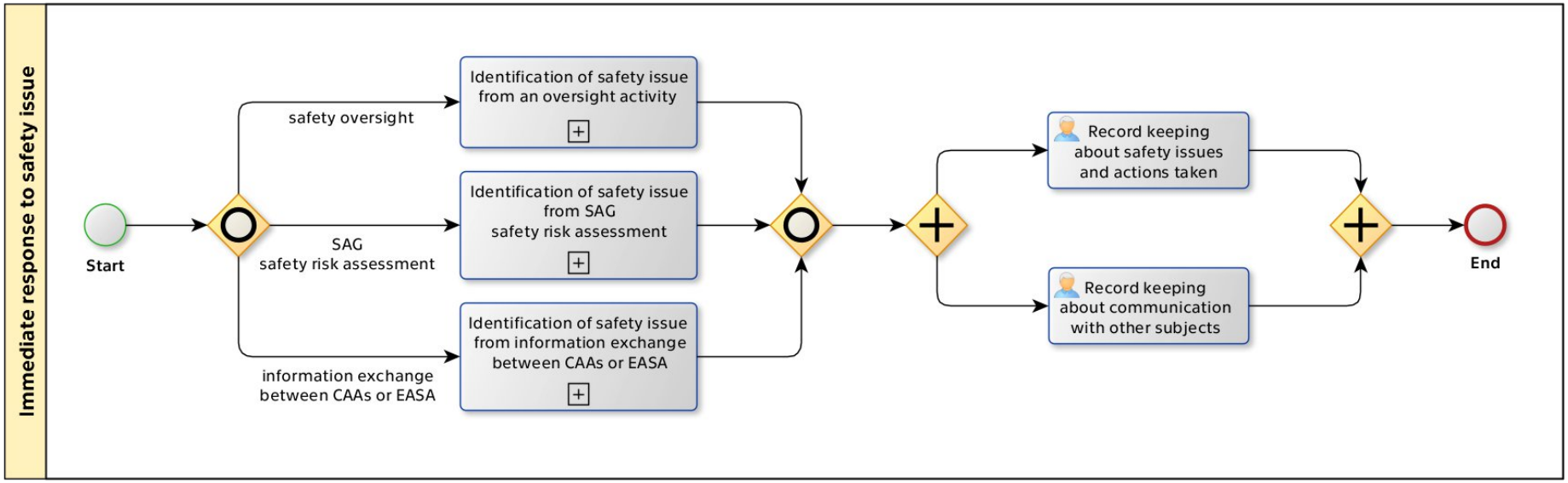

Fig. 3 – First pool of the BPMN diagram of the „Response to Safety Issue“ core process

There are many tools that can be used to create BPMN diagrams and process maps. In our research, we have used open-source tools for both BPMN and TOGAF Event Diagrams - Bonita Studio[1] and Modelio[2] respectively. There are several other tools available, including the commercial ones, so users are encouraged to make their own choice by considering their needs.

3.2.2 Safety control structure modeling

As was explained in section 3.1, the STPA is a hazard analysis technique based on STAMP. Because the systemic approach to safety considers systems in a very broad sense, the oversight institutions can perform hazard analysis with their own processes. The STPA analysis includes, among other things, modeling of a safety control structure (the second step of STPA), which forms the basis for the next steps of the analysis. The control structure, however, may serve other purposes than just the hazard analysis. For example, it enables the oversight institution gaining a better overview of its organizational structure, processes and internal or external relationships.

Modeling a safety control structure is very similar to that of creating process maps or BPMN diagrams. It is therefore important for the oversight institution to analyze internal documentation and highlight important inputs for the control structure. Normally, the modeling itself would follow. However, if the oversight institution already has the process maps and BMPN diagrams created, it is advisable to use them together with the process documentation. Information about the controllers, controlled processes as well as about control actions or feedback are often easy to find and learn from the diagrams. For this reason, the modeling of the control structure is easier and the process documentation serves as a supplement for learning additional details.

The modeling of the safety control structure in oversight institutions should involve similar thinking as when creating the process maps and BPMN diagrams. This means that the oversight institution should start by creating a more general control structure and progressively proceed with more details. Therefore, it is good to start with the organizational structure and the core processes of the oversight institution. An example of the abstracted safety control structure (based on real-scale Civil Aviation Authority) is shown in Fig. 4, where individual colors indicate different levels of management.

After the oversight institution establishes the basic structure, it can proceed with details of individual processes and organizational units related to each other. A process map (e.g. TOGAF Event Diagram) can help with this because the core processes and their links to the supplementary are listed here. This provides a basic overview of the relationships between processes on the basis of which additional details of the control structure can be modeled. In this way, iteratively, the greatest level of detail of the control structure showing all the activities of individual persons (roles) can be achieved.

[1] https://www.bonitasoft.com/
[2] https://www.modelio.org/

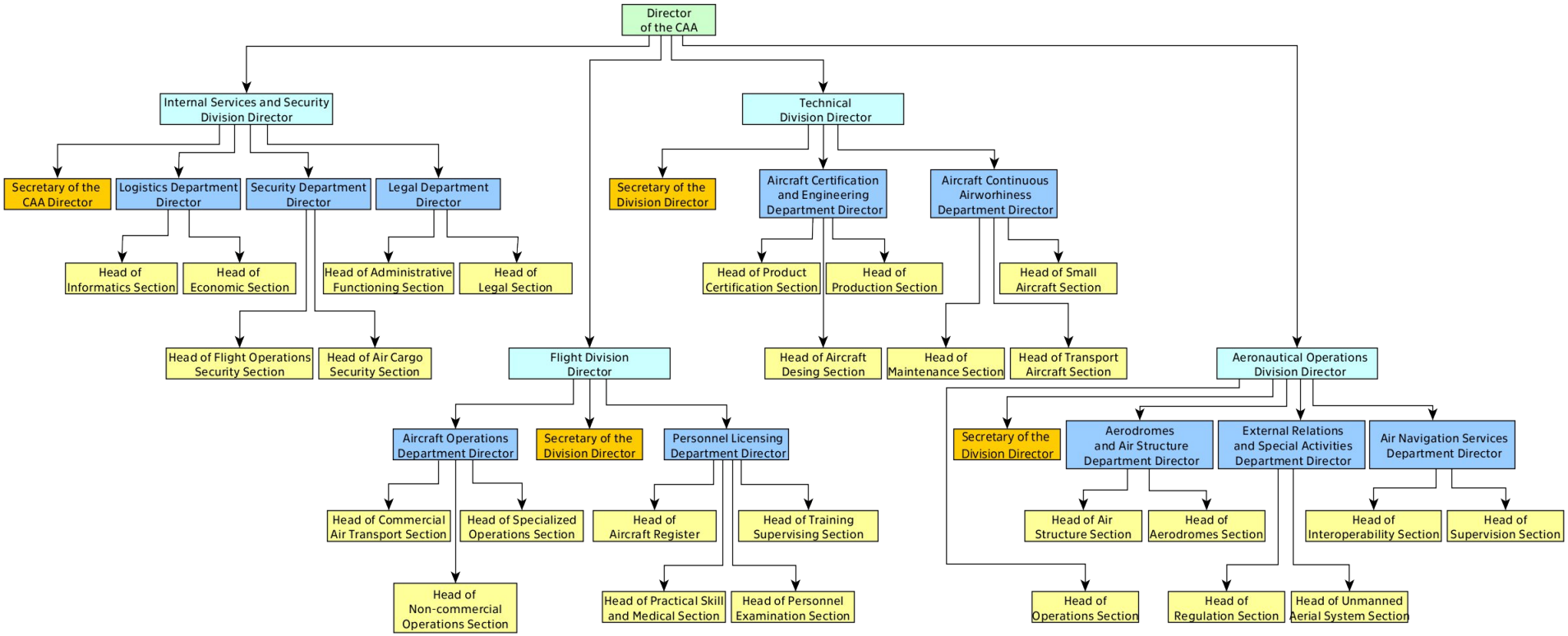

Fig. 4 – General safety control structure of an oversight institution

BPMN diagrams can well support achieving this, because they map individual roles and the activities for which they are responsible. Because activities are interconnected all over the system, it is easy to learn whether the links between individual roles (or controllers in the language of STPA) are control action, feedback or coordination.

The abstraction of the safety control structure subsequently serves the user (oversight institution) in further utilization of the control structure. The user may choose the level of detail they need at the moment. As an example, a detail of the safety control structure is in Fig. 5 (detailed from Fig. 4), showing the detailed control structure for the certification process which takes place in the Aerodromes Section of the Civil Aviation Authority. Arrows down represent control actions, arrows up the feedback. Dashed lines then show the coordination interactions.

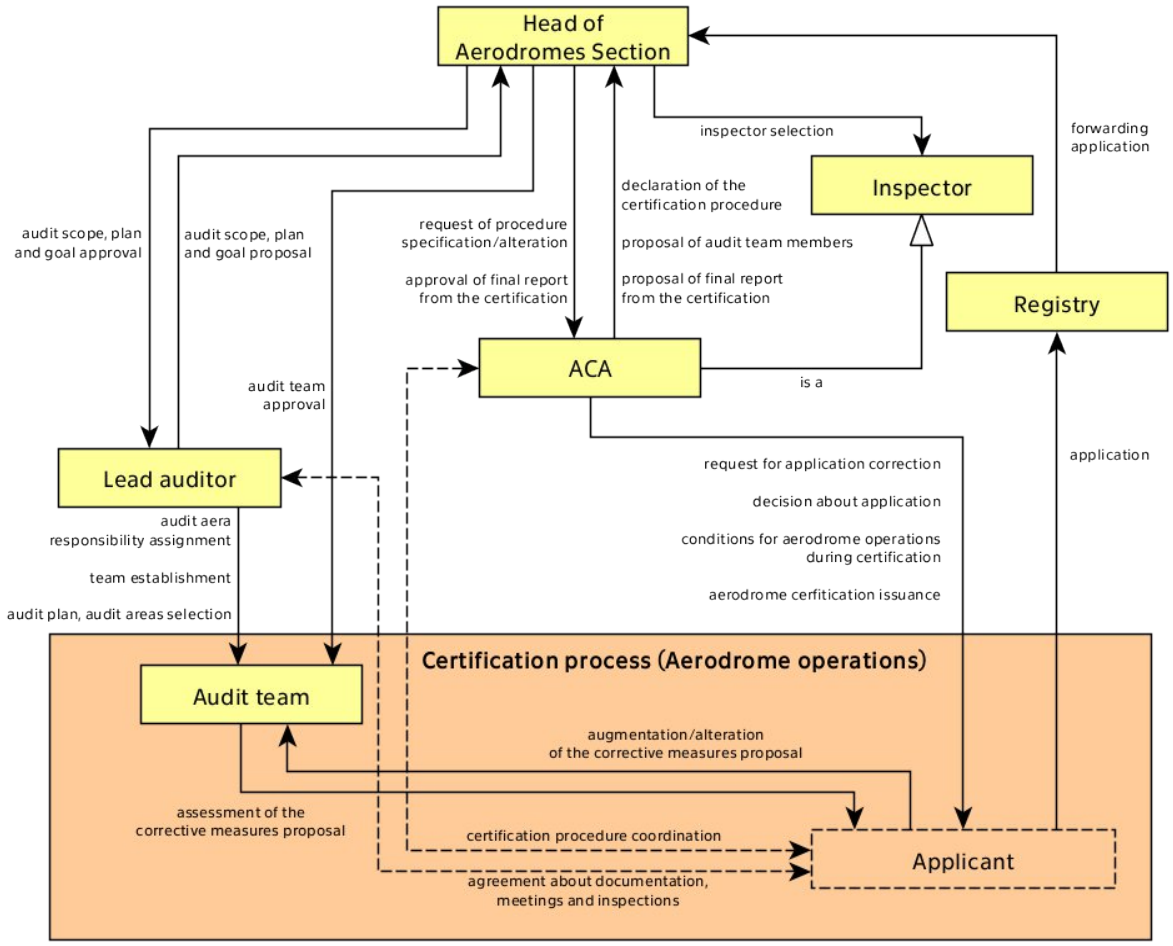

Fig. 5 - Detail of the example safety control structure – aerodromes certification process at the Aerodromes Section

For a complete hazard analysis, the oversight institution must also perform other steps of the STPA. It is therefore necessary to identify losses, system-level hazards and safety constraints (first step of STPA), unsafe control actions and controller constraints (third step of STPA) and finally the loss scenarios (fourth step of STPA). The last part is then identification of potential assumptions based on the safety constraints, according to

Active STPA. With a complete analysis, the supervisory authority learns its weak spots that enables taking measures to prevent them. Such an analysis could also be used for internal auditing and similar purposes.

3.3 Formalization of the knowledge about aviation organizations

The oversight of aviation organizations performed by an oversight institution can be divided into the area of certification and change management and the area of ongoing oversight. Ongoing oversight includes the carrying out of audits and inspections. It aims to ensure that organizations and natural persons comply with their obligations at all times. If, as part of ongoing oversight, an organization or natural person is found to be performing a function in breach of regulatory requirements, then such situation demands adequate measures.

Ongoing oversight in organizations is carried out by a system of planned and unplanned audits and inspections. These help to ensure an acceptable level of safety by verifying that all activities of the organization are performed safely. Audits carried out by the oversight institution in this respect often focus on the procedures of the Safety Management System (SMS) and verifying its performance and effectiveness.

In order to oversee aviation organizations, the oversight institution needs to be familiar with the legislation relating to the respective type of organization and, at the same time, have the certification documentation of specific audited organization available. If necessary, the oversight institution may also request more detailed internal documentation of the organization.

In the case of application of this methodology (and the systems thinking based on the STAMP model), it is necessary to progressively establish a formalized base for all types of overseen organizations, in some cases even specifically for individual organizations. The following steps can help an oversight institution with creating such a base.

As a first step, relevant regulations or standards that relate to the respective type of aviation organization are needed. To form a formalized basis for a particular organization rather than a type of organization, respective organization's certification documentation would be more appropriate. In the certification documentation, the information is typically more detailed (specific), so using it can make the formalization easier for the oversight institution. The procedure is then identical for both cases.

The documentation is usually a file (most commonly PDF) that contains a textual description of, among other things, the required inputs for STPA. The oversight institution must therefore first analyze the document and look up the control structure elements, i.e., controllers, controlled processes and their interactions. In practice, this can be done by reading the documentation and marking all the relevant information (see example in Fig. 6). The next step is the creation of the safety control structure. In this step, a diagram is created according to the second step of the STPA. The diagram will thus show the annotated information, as described in the input documentation.

Fig. 7 shows an example of the safety control structure for maintenance organizations, which was created according to the regulation and therefore shows a generic structure for a type of organization, rather than a specific organization.

The person creating safety control structure typically starts with the most general structure, which is based on the organizational structure of a specific organization or a given type of organization. In most cases (especially in the control structure of specific organizations) the more general control structure may not suffice and it is then necessary to go into the details. The more detailed safety control structures expand selected parts of the more general ones, showing detailed controllers and controlled processes of the respective organizational unit or department.

AMC1 ADR.OR.D.015(a) Personnel requirements

ED Decision 2014/012/R

ACCOUNTABLE MANAGER

(a) Accountable Manager — General

(1) The accountable manager should:

(i) ensure that all necessary resources are available to operate the aerodrome in accordance with the applicable requirements and the aerodrome manual;

(ii) ensure that if there is a reduction in the level of resources or abnormal circumstances which may affect safety, the required reduction in the level of operations at the aerodrome is implemented;

(iii) establish, implement, and promote the safety policy; and

(iv) ensure compliance with relevant applicable requirements, certification basis, and the organisation's safety management system, as well as its quality management system with regard to aeronautical data and aeronautical information provision activities.

Fig. 6 - Sample of legislative text with highlighted important parts for creation of the safety control structure of the selected aviation organization

As part of the first step of the STPA, losses (loss events) and system-level hazards must be defined. Then, the second step of the STPA, additionally to the safety control structure diagram, should include a table listing the controllers with their responsibility (actions that the controller will do themselves), authority (control action), accountability (feedback) and coordination (interaction with elements at the same level in the hierarchy). In result, the table (see example in Tab. 1) will show the same information as the control structure diagram (see Figs. 4, 5 and 7), enabling consistency check and providing the oversight institution with a sound basis for identification of unsafe control actions (third step of the STPA).

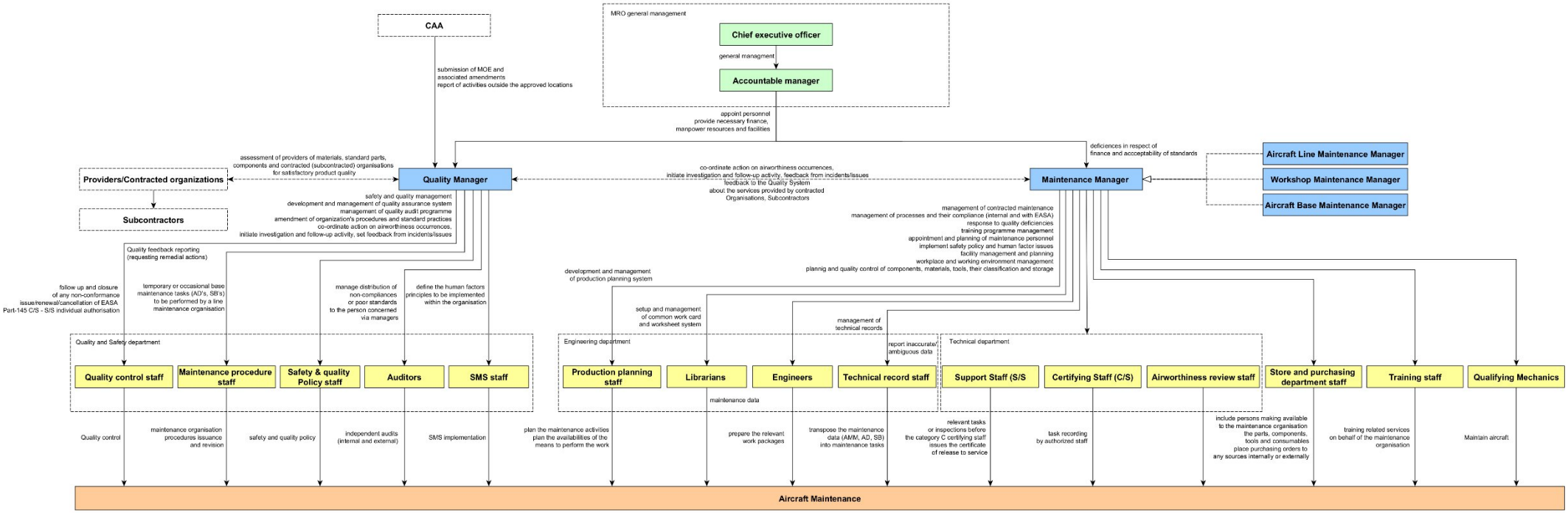

Fig. 7 - Sample safety control structure for maintenance, repair and overhaul organizations created from legislative requirements

Tab. 1 – Table of controllers

Controller	Responsibility	Authority	Accountability	Coordination
Controller 1				
Controller 2				
Controller 3				

Lastly, loss scenarios (STPA step 4) should be identified. The table of unsafe control actions created under the previous step serves as an input. Finally, the person establishing the formalized base should determine the safety constraints, based on existing system-level hazards, unsafe control actions and loss scenarios. Based on the previous knowledge and primarily the safety constraints, the oversight institution can specify additional assumptions for the given type of organization or individual one that should never be violated. If the oversight institution creates such basis, it can simply build on it when preparing audits (specifically when preparing audit questions) or also when processing and analyzing safety occurrence reports.

3.4 Occurrence reports processing and analysis

One of the main and important sources for maintaining aviation safety at the state level is the occurrence reporting system. The system is typically divided into a mandatory occurrence reporting (MOR) and a voluntary occurrence reporting (VOR) systems. In European environment for example, the system is specified in Regulation (EU) No 376/2014 of the European Parliament and of the Council, together with Commission Implementing Regulation (EU) 2015/1018.

For an oversight institution, important are all information contributing to the clarification of the actual situation in the overseen organizations (including mandatory and voluntary occurrence reporting) and to the support of planning audits, including other activities targeted at improving safety in those organizations.

Anytime an oversight institution receives an occurrence report, whether the report is mandatory or voluntary, it records the information in a predefined form to obtain a set of structured data which can be easily searched and filtered, as needed. Reports may be received in various data formats, including e-mail, PDF or E5X files, etc. It is up to each institution to decide how the data will be collected and recorded. For the purpose, it is possible to use both dedicated software tools as well as common spreadsheet editors such as MS Excel.

After receiving an occurrence report, the initial step is to create a new record in the occurrence database and identify the basic information that can be retrieved from the report. Basic information may include items shown in the blue part of Tab. 2: Event ID, occurrence name, date and time, occurrence category, occurrence class and event type, all based on the ECCAIRS taxonomy. In addition, occurrence location and narrative may be used. Tab. 2 then illustrates an example of a reported occurrence with anonymized Event ID, occurrence name and date/time. The remaining data fields include event type classification according to ECCAIRS, followed by the location and the occurrence narrative.

Next follows classification of the reported occurrence by means of Active STPA (see yellow part of Tab. 2). The first step is to identify the involved stakeholders. This is an expert assessment where the user identifies specific organizations that participated in the reported occurrence. It is possible that a single occurrence is reported by several persons or organizations. In such cases, the user stores and aggregates reports related to single occurrence. In Tab. 2, the "1-LKPR" organization is recorded as an example participant, where only one organization participated in the occurrence. If more organizations would be involved in a single occurrence, these would be recorded with consecutive 2-XXX, 3-YYY etc.

Once all the the stakeholders (participants) are identified, more information needs to be identified from the received report. To identify the information, the oversight institution will use existing STPA artifacts created for respective organizations or organization types.

The next step is to identify the losses (loss events) and system-level hazards that occurred in the reported event. The classification assumes the use of existing STPA artifacts created for all participating aviation organizations. The person recording the event (the user) simply selects one or more losses as well as system-level hazards that occurred in the event. In Tab. 2, the loss "Damage to Infrastructure" is recorded. In case the reported occurrence was just an incident, i.e., with no fatalities, injuries or damage, there will be no losses recorded.

After the losses and system-level hazards are classified, the user continues with controllers that were involved in the event. The controllers most often include specific persons in charge or entire organizational units. This means that it is necessary to select from the existing control structure elements of the participating organizations those components that participated in the occurrence, i.e., the manifestation of system-level hazards and losses. The user may simply select one or more control structure elements available in the respective STPA artifacts.

Tab. 2 – Sample of a processed occurrence report

Event ID	Occurrence name	Date/time	Occurrence category	Occurrence class	Event type	Location	Narrative
314.....587	Fire XXX/027/20XX	Fri Mar XX 19:28:00 CET 20XX	24 - ADRM: Aerodrome	300 - Incident	5020800 - Main power	LKPR	Fire T2 on main transformer station. Power cut during fire fighting resulted in switching off apron lights at T1. Full power restoration at 19:51 LT.

Active STPA categorization							
Stakeholder	**Loss event**	**System-level hazard**	**Responsible controller**	**Controlled process**	**Violated assumptions**	**Trend**	**Causal factors**
1-LKPR	L-3: Damage to Infrastructure	H1.1: Airport infrastructure with obstacles / operational limitations	OJ HZS: Fire Rescue Service	Supervisory of electronic system of fire detection Fire fighting	A1 – Airport infrastructure is secured against external influences (e.g. weather) A3 – Airport infrastructure and systems provide service according to the requirements (e.g. time, technical parameters, etc.)	-	-

Following the identification of controllers, the controlled processes that relate to their activity and to the reported occurrence can be identified. Only controlled processes that fall within the responsibility of the participating organizations and respective controllers should be selected. The user would again select one or more controlled processes already available in respective STPA artifacts or, alternatively, search for the controlled processes in the organization's documentation (if such processes are missing in the STPA artifacts), adding it to the list of controlled processes.

Next follows a selection of safety constraints and related assumptions, specifically those violated in the occurrence. The user again simply selects one or more safety constraints and assumptions available in the relevant STPA artifacts, where the selection is already limited by the selected controllers, controlled processes and system-level hazards selected before.

The last part of Tab. 2 are the "Trend" and "Causal factors" data fields. These data fields can be filled in if the information is available. The "Trend" field captures information about similar events occurring repetitively in one organization or in the same type of organization to draw attention to the fact. To fill in such information, it is necessary to have a sufficient amount of data over a longer period of time. The "Causal factor" field may be used if information about specific causal factors is available in the occurrence report. It may be filled retrospectively after the occurrence is investigated. Otherwise, both data fields remain empty.

Tab. 2 shows an example of a single occurrence. If the oversight institution processes and classifies each occurrence report in the same way, a safety database will be established enabling a safety dashboard with statistical overviews of the entire database. Example in Tab. 3 provides an overview of how many loss events occurred in respective organization over a given period of time. Similar overview is provided in Tab. 4, which shows how many times a particular assumption has been violated over a given period. Similar overviews can be created for any category from Tab. 2 and oversight institutions may use other representations as well (e.g. graphs). It is important to regularly update the overviews and use them in the preparation of safety audits and inspections, as well as other relevant activities of the oversight institution.

Tab. 3 - An overview of the number of loss events in an organization for a given period

ID	Loss Events (Losses)	Count
L-1	Loss of life of injuries	0
L-2	Damage to aircraft	11
L-3	Damage to infrastructure	5
L-4	Loss of reputation	0
L-5	Environmental loss	1

3.5 Audits

The oversight institution carries out regular audits of the organizations it supervises under the compliance monitoring system. Compliance-based audits are carried out by verifying whether the monitored organization complies with the legislative requirements by directly comparing the current state of the organization with the specific requirements. In addition to these, there is also the possibility to complement such audit with the so-called "performance-based" questions, i.e., questions targeted on actual performance derived from occurrence reporting data and, where appropriate, previous audits and inspections.

Tab. 4 - Overview of the number of violated assumptions in an organization for a given period

ID	Assumption	Violation count
A1	Airport infrastructure is secured against external influences (e.g. weather)	19
A2	The planned workload will not exceed employees capacity	3
A3	Airport infrastructure and systems provide service according to the requirements (e.g. time, technical parameters, etc.)	12
A4	Increase in traffic on the airport infrastructure will not exceed its capacity	0

3.5.1 Audit preparation and execution

Once the auditor decided which organization to audit, they can start preparing audit questions. If there are already STPA artifacts for the organization or for its type created, the auditor will use the already completed STPA and choose only those parts of the safety control structure that are in the audit scope. However, if they lack the necessary detail or part of the safety control structure, then it must be created.

The auditor will normally use regulatory documentation during an audit, which will also serve them well in the creation of the safety control structure (the second step of STPA). The auditor goes through the documentation, which they also use for the preparation of a typical compliance-based audit. In the documentation, they highlight important parts and then convert them into the safety control structure (see Fig. 8). After the safety control structure is established, it is necessary to proceed in the same way as during a normal STPA analysis, i.e., identify unsafe control actions, controller constraints and loss scenarios. If the STPA analysis is already completed, e.g., from a previous audit, the auditor only checks its currency and modifies some parts of the analysis accordingly.

Next follows the definition of safety constraints related to individual loss scenarios (see Tab. 5). These may also be prepared in advance, but then it is necessary to verify their currency and adjust, if necessary. Similarly, assumptions for the given type of organization should be documented or updated. After the safety constraints and assumptions are defined or updated, audit questions can be created. For safety constraints (and subsequent audit questions) prioritization, it is also good to check the achieved safety performance of the given organization in advance, e.g., by means of the number of safety occurrences, types of problems or corrective actions from the previous audits.

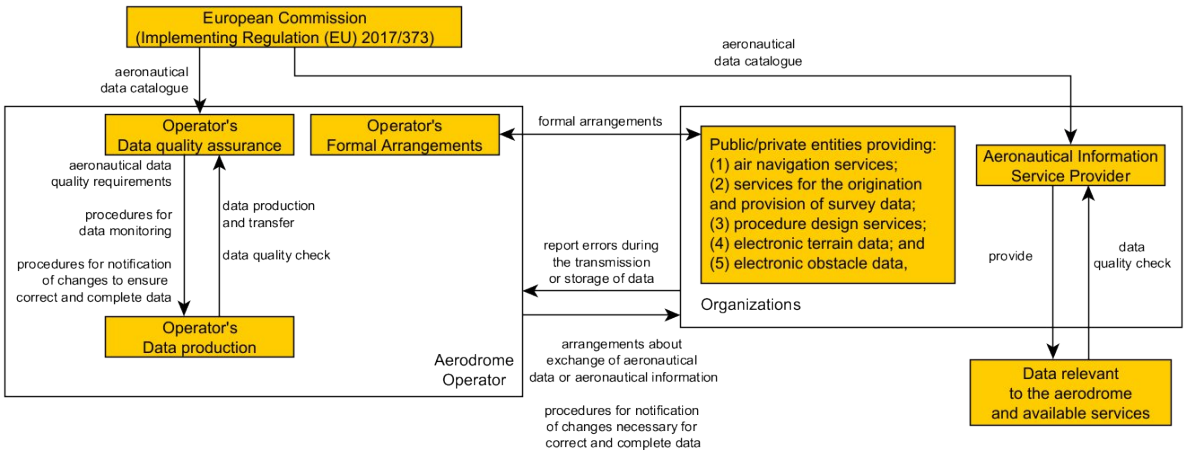

Fig. 8 – Example of a safety control structure created from a regulatory documentation related to data quality requirements

The next step is preparation of audit questions. Here, the auditor translates documented assumptions and safety constraints into audit questions and in this way sets up an audit checklist (see Tab. 5). The translation is done directly by the auditor and the goal is to achieve an organized list of questions and sub-questions. Alternatively, this step could be automated by means of software, however, it is advisable for the auditor to adapt the questions to the specific audit needs. Automatically generated questions may not be accurate or self-explanatory without the auditor providing the necessary context. Context can be added by linking the question (created from the safety constraints and assumptions based on loss scenarios) to a more specific constraint related to the controller and its responsibilities. As shown in Tab. 5, the red constraint is the basis for the audit question while the blue constraint provides respective context in which the auditor should query the organization. The creation of audit questions is largely based on the experience and knowledge of the auditor, and this is why full automation of the audit questions creation is not yet advisable.

Fig. 9 shows a schema of the preparation of audit questions, the follow-up audit in the supervised organization, the responses recording and their subsequent evaluation.

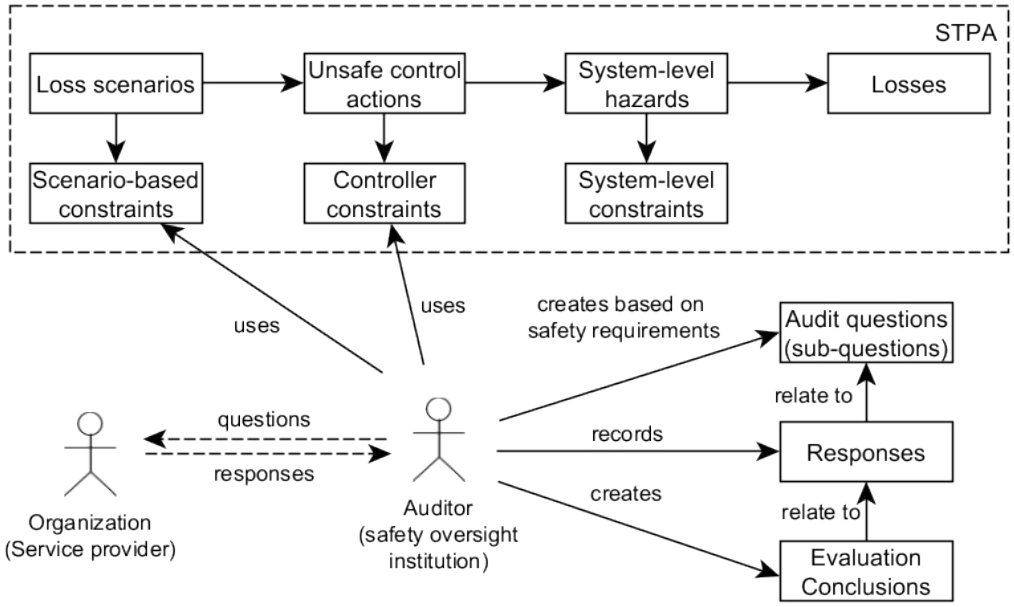

Fig. 9 – Audit preparation and execution based on the STPA

3.5.2 Audit recording

During an audit, the auditor asks prepared audit questions and must be ready to provide additional explanation, should anything be unclear to the audited organization. The organization then responds to the questions and the auditor records the responses and, where appropriate, enquires about the detail of interest or prepared sub-questions (see Tab. 5). After the audit is complete, the auditor must evaluate the individual responses to indicate whether the organization fulfills, does not fulfill or only partially fulfills respective requirement (implemented, not implemented or partially implemented), as can be seen in the last column of Tab. 6.

The recording of responses during an audit is thus primarily used for the final evaluation. However, the recorded responses serve also well the subsequent audits, when the auditor performs the audit again after a given period of time and they need to verify whether the organization improved its procedures or put in place effective corrective actions.

Tab. 5 – Example of safety constraints translation into audit questions

Loss scenario	Scenario-based constraint	Controller constraint		Audit question
Aerodrome operator does not define aeronautical data quality requirements when they are the data originator [UCA-1a] because of lack of personnel.	- Aerodrome operator must have sufficient personnel.	CC-1a Aerodrome operator must define aeronautical data quality requirements when they are the data originator.		Has the aerodrome operator sufficient personnel (for definition of aeronautical data quality requirements)?
Aerodrome operator does not implement procedures for risk assessment and mitigation related to data protection when they are the data originator [UCA-5a] because they are unaware that they shall implement such procedures.	- Aerodrome operator must be aware that they shall implement procedures for risk assessment and mitigation related to data protection.	CC-5a Aerodrome operator must implement procedures for risk assessment and mitigation related to data protection when they are the data originator.		Has the aerodrome operator available necessary documentation for procedure implementation (risk assessment and mitigation related to data protection) - What are the procedures? - How they work in practice?
Aerodrome operator implements procedures for monitoring of data and available services with delay, when data collection already takes place [UCA-2c], because additional change to the procedures was needed.	- Aerodrome operator must implement procedures so that any change is incorporated before its planned introduction.	CC-2c Aerodrome operator must implement procedures for monitoring of data and available services before the data collection starts.		Has the operator sufficient time to implement new procedures and are final changes/modifications considered before the planned introduction? - How are handled additional changes to procedures? - How are the employees notified to changes?

Tab. 6 –Audit responses and evaluation

Loss scenario	Scenario-based constraint	Controller constraint		Audit question	Response	Evaluation
Aerodrome operator does not define aeronautical data quality requirements when they are the data originator [UCA-1a] because of lack of personnel.	- Aerodrome operator must have sufficient personnel.	CC-1a Aerodrome operator must define aeronautical data quality requirements when they are the data originator.		Has the aerodrome operator sufficient personnel (for definition of aeronautical data quality requirements)?	Detailed record of the response	not implemented
Aerodrome operator does not implement procedures for risk assessment and mitigation related to data protection when they are the data originator [UCA-5a] because they are unaware that they shall implement such procedures.	- Aerodrome operator must be aware that they shall implement procedures for risk assessment and mitigation related to data protection.	CC-5a Aerodrome operator must implement procedures for risk assessment and mitigation related to data protection when they are the data originator.		Has the aerodrome operator available necessary documentation for procedure implementation (risk assessment and mitigation related to data protection) - What are the procedures? - How they work in practice?	Detailed record of the response	partly implemented
Aerodrome operator implements procedures for monitoring of data and available services with delay, when data collection already takes place [UCA-2c], because additional change to the procedures was needed.	- Aerodrome operator must implement procedures so that any change is incorporated before its planned introduction.	CC-2c Aerodrome operator must implement procedures for monitoring of data and available services before the data collection starts.		Has the operator sufficient time to implement new procedures and are final changes/modifications considered before the planned introduction? - How are handled additional changes to procedures? - How are the employees notified to changes?	Detailed record of the response	implemented

4 Application of the methodology

The methodology can be applied in several ways, in terms of scope and form of application. It is recommended that oversight institutions applying the methodology consider both aspects when implementing the procedures described in this document.

In terms of scope, the methodology can be applied as a whole or some of its parts individually. All procedures are linked to each other and offer synergy effect with their application as a whole, but technically some can be applied separately and for other purposes that are not subject of this methodology. For example, the creation of a safety control structure according to STAMP can be used as a type of organizational chart for understanding of the oversight institution or supervised organization functioning. However, some procedures depend on others and cannot be applied separately. These are mainly procedures for processing and evaluating occurrence reports from organizations, creating audit questions and recording responses to them. These procedures require the existence of STPA artifacts, which are the product of other procedures, and it is therefore necessary to apply them together. The decision on the application of the methodology in terms of scope should be made in cooperation with qualified personnel who are able to assess the applicability and potential benefits of specific procedures in a given oversight institution and its specific environment.

In terms of the form of application, there are also several options. As a baseline, it is assumed to implement the procedures mentioned in this methodology into the existing software infrastructure and related procedures of a given institution. Such application assumes that the existing infrastructure and procedures of the oversight institution allow the implementation of the methodology either directly or by its adaptation to the existing infrastructure and procedures. A more extensive application would include the implementation of additional software tools mentioned in this document. In such case, the oversight institution adopts an external software tool set for selected procedures and considers the issues of incorporating such tool set into the existing software infrastructure. It is also appropriate to make the decision on the form of the methodology application with an expert assessment by qualified personnel.

To achieve maximum synergy effect in the application of the methodology, it is recommended to apply all the procedures specified in this document while using dedicated software tools to support the creation of process diagrams (editors working with BPMN and other types of process diagrams) and STPA artifacts (graphic editors for creating block diagrams, Microsoft Office or equivalent applications for storing tables etc.). Microsoft Office or equivalent applications can be used for storing data from occurrence reports, audit questions and audit results.

5 Economic aspects

The application of the methodology entails several costs to consider. The procedures of the methodology as a whole are more time-consuming than the usual procedures of oversight institutions and they require additional qualification of personnel working with safety data. This is mainly due to the maintenance of STPA artifacts that represent the actual functioning of the oversight institution as well as the functioning of supervised organizations. By contrast, an opposite effect can be expected for procedures that formalize the oversight institution's process documentation, because once such procedures are in place, the time required to maintain the process documentation will be smaller, despite the improvement of the documentation quality. This is because the text documents will not need to be analyzed as a whole to identify the parts that need to be updated and no specific efforts will be needed to retain the documentation integrity and cross-references. Schemes and diagrams-based process documentation only requires modification of the relevant parts of the modeled artifacts, which are more easily traceable by software tools designed to manage such artifacts, compared to text editors such as Microsoft Word. This balances the potentially negative impact of the increased work requirements related to managing STPA artifacts. The resulting time required for the full application of this methodology, however, depends on the number of supervised organizations and the complexity of the processes of respective oversight institution and cannot be assumed to be the same for each institution.

Concerning the implementation of procedures of this methodology, the training of the personnel in charge of processing safety data and the modification or extension of the software infrastructure should be considered. In terms of the training, approximately three-day workshop will be needed to ensure sufficient qualification of all staff working with the STPA and the related artefacts. In terms of the modification or extension of the software infrastructure, the costs will depend on the form of application of the methodology. To reduce the costs associated, it is advisable to use the tools listed in this methodology, most of which are available free of charge. The more extensive implementation in form of modification of the existing software infrastructure additionally offers the potential of automation, e.g. by reusing the data and taxonomy from one artefact (e.g. BPMN model) with some the other artefact (e.g. the safety control structure of the oversight institution). This will be a more expensive option due to the need of programming, but in the long term it will be advantageous by saving the working time of employees of the oversight institution. The costs associated with the software infrastructure also depend on the number of supervised organizations and on the complexity of the processes of the respective oversight institution thus it is not possible to make a general recommendation for all institutions.

In terms of the economic benefits, the use of STAMP safety model and its methods brings new possibilities for oversight institutions to identify hazards, assess risks and measure safety performance, leading to a better identification and assessment of safety issues. Compared to the current procedures, better identification regards the time (i.e. early identification) and the nature of safety issues owing to explaining safety as a control

problem. Only the description of the normal functioning of aviation organizations is needed, i.e. there is no need for historical safety data or expert knowledge in the domain of an organization to identify safety issues. Early identification of safety issues and greater control over ensuring safety brings savings in the costs of prevention and elimination of the consequences of safety occurrences, with consequent increase in the availability and competitiveness of air transport.

Economic benefits can also be found in the area of safety oversight process management. The procedures using the STAMP safety model, owing to its holistic approach, create models that, in addition to safety management and oversight activities, can also be used to optimize the processes of the oversight institution, e.g., by adjusting responsibilities and distributing work across individual organizational units or roles of employees. This can result in a workload reduction of respective work procedures and, as a result, in respective personnel costs savings.

References

[1] LEVESON, N. Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. ISBN 978-0-262-01662-9.

[2] LEVESON, N. a J. THOMAS. STPA Handbook, 2018. Dostupné z: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[3] LEVESON, N. CAST Handbook: How to Learn More from Incidents and Accidents, 2019. Dostupné z: http://sunnyday.mit.edu/CAST-Handbook.pdf.

[4] CASTILHO, D. Active STPA: Integration of Hazard Analysis into a Safety Management system Framework. Dissertation, Massachusetts Institute of Technology (MIT), 2019.

[5] ICAO. Doc. 9859: Safety management manual (SMM). 4th edition. Montréal, Quebec: International Civil Aviation Organization (ICAO), 2018. ISBN 978-92-9258-552-5.

[6] ŘEPA, Václav. Podnikové procesy: procesní řízení a modelování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2007. Management v informační společnosti. ISBN 97880-247-2252-8.

[7] LEDVINKA, M., P. KŘEMEN, L. SAEEDA a M. BLAŠKO. TermIt: A Practical Semantic Vocabulary Manager. In: Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 1: ICEIS. 22nd International Conference on Enterprise Information Systems (ICEIS 2020), Prague. Porto: SciTePress - Science and Technology Publications, 2020. s. 759-766.

[8] STRIPPEL, Christian, Laura LAUGWITZ, Sünje PAASCH-COLBERG, Katharina ESAU a Annett HEFT. BRAT Rapid Annotation Tool. Medien & Kommunikationswissenschaft [online]. 2022, 70(4), 446-461. ISSN 1615-634X.

Publications preceding the methodology

GRÖTSCHELOVÁ, K., A. LALIŠ a N. GUSKOVA. Systemic Safety Data Collection and Processing in Aviation Safety Oversight. In: 2021 International Conference on Military Technologies (ICMT). Brno, 2021-06-08/2021-06-11. Praha: IEEE Czechoslovakia Section, 2021. ISBN 978-1-6654-3724-0. DOI 10.1109/ICMT52455.2021.9502826. Dostupné z: https://ieeexplore.ieee.org/document/9502826/

KAFKOVÁ, M., S. STOJIĆ a A. LALIŠ. Improving Safety Studies through Application of Deviation Concept. In: HANÁKOVÁ, L. a V. SOCHA, eds. Safety & Security Conference Prague 2019. Praha, 2019-11-20/2019-11-21. Praha: IRIS - Rudolf Valenta, 2019. s. 49-55. ISBN 978-80-907724-0-3.

KŘEMEN, P. et al. Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems. Journal of Aerospace Information Systems. 2017, 14(5), 279-292. ISSN 1940-3151. DOI 10.2514/1.I010441.

LEDVINKA, M., A. LALIŠ a P. KŘEMEN. Toward Data-Driven Safety: An Ontology-Based Information System. Journal of Aerospace Information Systems. 2019, 16(1), 22-36. ISSN 1940-3151. DOI 10.2514/1.I010622.