http://dx.doi.org/10.14311/MAD.2016.19.02 ISSN 1805-7578

Safety Study in Aviation

Marek Štumper
Department of Air Transport
Faculty of Transportation Sciences, Czech Technical University in Prague
Horská 3, Praha 2, 128 03, Czech Republic
e-mail: stumpmar@fd.cvut.cz

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

Abstract— **The objective of this article is to provide a brief look at safety studies, which are a necessary part of every change of system or a new system in aviation. The main focus is put on the area of air traffic management, because it affects most of the aviation stakeholders. The article begins with a description of safety and safety assessment of changes in systems. Then it discusses analysis of processes, hazard identification and risk assessment. Main part focuses on Safety studies and briefly describes the elements of the study. At the end, possible ways of safety study evaluation are mentioned.**

Keywords - Safety study, hazard identification, hazard effect, risks, change, new system, Safety Assessment Methodology

I. INTRODUCTION

The aviation sector employs about 58 million people worldwide and engages in activities worth of approximately 2,4 trillion dollars. 3,3 billion passengers were transported in 2014 and some estimates talk about 16 billion passengers in 2050 [1]. Those are huge numbers and it will be impossible to reach them without focusing on operational safety and its increasing.

The EUROCONTROL Safety Regulatory Requirement (ESARR 4) defines safety as "freedom from the risk of unacceptable harm" [2]. Harm means death or a serious injury and/or structural damage to an aircraft. In other words, safe situation exists when the risk of an accident is acceptably low (when acceptably low risk is a risk not higher than tolerable and mitigated as far as reasonably practicable) [3]. Different definition of safety comes from Systems theory. It says that safety is an emergent property arising from interactions between system elements. Such property is managed through setting constraints or requirements on behaviour of elements and interactions between them [4].

Safety is not a one-time event, it is an ongoing, never ending process of identifying hazards and managing risks in order to show that a system or process is safe. This continuous process is performed by utilizing Safety Management System (SMS). [11] However, it is also required to assess a planned change or a new system before it enters service. Method for such assessment is a Safety Study, which focuses on identifying negative events and consequently determine means of prevention of such events.

II. ANALYSIS OF PROCESSES

Analysis of processes consists of dividing the whole process into subparts: actors (hardware, software, human), environment conditions and other. These subparts are then studied both individually and in interactions with each other in order to find various failure modes, interactions and effects of failures on other subparts.

Such analysis is a basis for safety studies as they are based on analysis of processes, their assessment and evaluation, whether they are safe or not. A shortcoming of an analysis conducted before entry into service is the fact, that it is based on the design of a system. Design takes into account specific characteristics of elements, but in real life service, these characteristics are different and the elements might influence their environment in a different way than expected and assessed in an analysis [4]. Furthermore, some systems require an operator, who needs information about the ongoing process. Already at the beginning of designing of a new system, it has to be decided what kind of information has to reach the operator. However, the designer is not able to come up with exactly everything needed, therefore brings a source of mistakes into the system. A way of reducing the number of these mistakes is to conduct analysis of processes over and over again to search for the mistakes and take them out of the system.

There are many methods that can be used for performing the analysis, although two of them stand out. They are called Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). Both of them require identification of a negative event, from which the ETA analyses possible effects and FTA analyses possible causes.

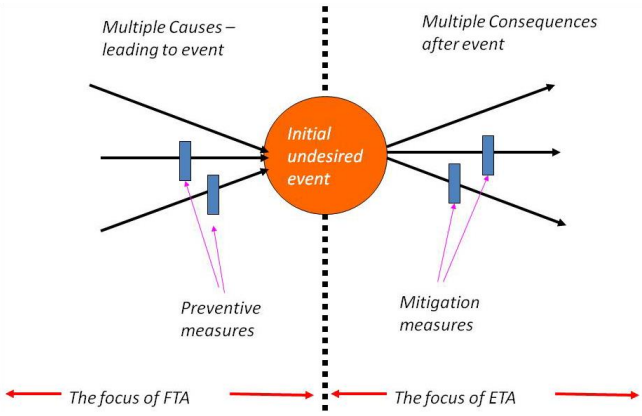

Figure 1. Connection between FTA and ETA [5]

III. Hazard Identification and Risk Assessment

Hazard identification is the alpha and omega of all the efforts related to safety. Without it, it would be impossible to determine what to improve, what to mitigate, what areas to focus on or how to build airplanes. Both hazard identification and risk assessment are processes of SMS, however they were not created together with SMS, they are accompanying mankind for a very long time, only with minimum attention in the past.

It is important to define three terms: hazard, hazard consequence and a risk.

- Hazard – ESARR 4 defines hazard as "Any condition, event, or circumstance which could induce an accident." It is reasonable to make this definition more general: a hazard is anything, that can negatively influence safety [6].
- Hazard consequence – this term describes what is the consequence (effect) of a hazard. For example, if a hazard is an unwanted release of steam, then consequence is burnt worker. It is obvious, that one hazard can have multiple consequences.
- Risk – according to ICAO doc. 9859 [7] risk is a "probability and severity of a consequence of a hazard.

A. Hazard and its consequences

Hazard itself does not necessarily mean something negative or destructive. It gains those attributes only when in contact with operations, that can cause safety affecting situations. A wind could be used as an example. It does not pose any threat on its own, but its speed, runway configuration, pilot experience and airplane characteristics transform this hazard into something, that can affect safety of flight.

Problem of hazard and hazard consequences identification is caused by mixing up these two terms. It is quite common, that an accident is identified as a hazard. It is logical from non-professional point of view, but wrong and confusing from an expert point of view and could lead to insufficient analysis of processes. Accident is a consequence of a hazard and its interactions with operations

B. Risk

Risk is an assessed consequence of hazard in terms of probability and severity. These two attributes can be divided into several categories, such as according to ICAO doc. 9859 [7]. Probability:

- Frequent
- Occasional
- Remote
- Improbable
- Extremely improbable

Severity:

- Catastrophic
- Hazardous
- Major
- Minor
- Negligible

When probability and severity is assigned, the risk is compared to safety risk assessment matrix and then to safety risk tolerability matrix (ICAO doc. 9859 offers possible forms of these matrices).

Current state of risk assessment has several flaws. First of them is in the risk assessment matrix, which should provide firm basis for determining acceptability of risks, their prioritization and funding allocation. Unfortunately, most of those matrices use subjective and sometimes even poorly defined scales that they are almost unusable. It sure is hard to assign numerical values to probability and severity, but it is desirable to do some level of quantification of these scales. Because values such as "maybe so/maybe not" or "great damage/little damage" hardly describe the type of data needed for essential decision making. [8]

When the risks are being assessed by several experts, each of them might use a little bit different matrix, more suitable to their knowledge and experience, which could lead to a different risk assessment. Then, it might be tempting to use those outcomes, that require the smallest amount of effort for further dealing with risks.

IV. Safety Studies

Safety studies are a method of assessing risks related to implementing a change to the aviation system. Execution of such study and following report is used by the regulator to decide whether it will allow start of assessed operations (or use of changed/new system), and also by the organization itself as a way of assurance, that their current and future actions are and will be safe.

Described process of safety study in this article is based on Safety Assessment Methodology (SAM) developed by EUROCONTROL. SAM has three major phases, called Functional Hazard Assessment (FHA), Preliminary System

Safety Assessment (PSSA) and System Safety Assessment (SSA). At the beginning of a project, each of them has set a specific timeline in which it will be conducted, but as the project develops and time goes by, the phases begin to blend together as the last one can have an influence on the first one and vice versa. Following picture shows the timeline.

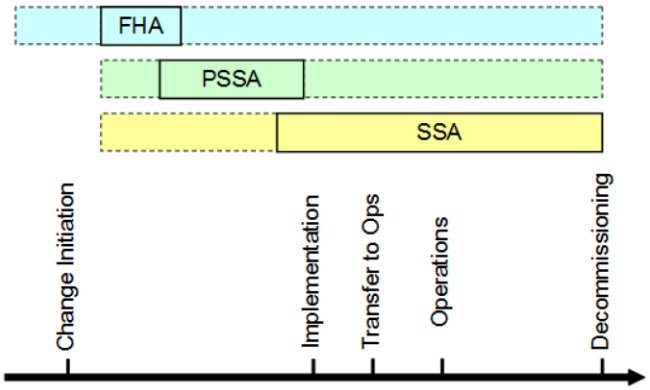

Figure 2. SAM Timeline [9]

A. FHA

FHA is the first phase of a safety study. Its goal is to determine how safe the proposed system has to be. That means setting Safety Objectives – qualitative or quantitative statement, which specifies acceptable frequency or probability of hazard occurrence [6]. Briefly, FHA consists of these five steps:

- Get to know the proposed system design – definition of the system, definition of the environment
- Hazard identification
- Hazard consequence identification
- Assessment of hazard consequence severity – assign severity to consequences, set Safety targets
- Safety Objectives derivation

B. PSSA

PSSA works with deeper description and knowledge of the system architecture. The outcome of this phase are Safety Requirements – means of risk mitigation, which will enable achieving given Safety Objective. Safety Requirements can have various forms – organizational, operational, procedural, functional, etc. [12]

C. SSA

SSA is the last phase and it consists of proving that the proposed system will be safe when implemented and in operation. That is achieved through collecting evidence, that Safety Requirements are being fulfilled. Most of SSA is being performed during operation and it is recommended to use SMS [13].

V. Safety Study Evaluation

The goal of safety assessment is to continuously identify hazards and assess risks, however in the case of safety study, a certain line has to be drawn after conducting FHA, PSSA and part of SSA and before implementing system into operation. The reason is that the outcome of this "first" part is used by regulator to either give or not give an approval for implementation and following operation of the assessed system. It is obvious that the purpose of the safety study is to show, that the system is safe, but that does not mean that the safety study should be bent and twisted and conducted with both eyes closed in order to just get the approval. If the safety study has a positive outcome, then there is no need to not approve the implementation and operation. On the other hand, if the study comes with a negative outcome, the authority then has several options:

- Change/new system will not get and approval and no further activities will be done
- The authority considers the outcomes and grants a limited approval, for example for test trials
- There is overall effort to implement the change. Then, the stakeholders work closely with authorities in order to come up with possible solutions, that would allow for a revision of the safety study (e.g. change of regulations). Of course it cannot be something, that could lower the required level of safety. [10]

VI. Conclusion

Correct and thorough execution of a safety study requires large amount of time, knowledge, expert opinions and many inputs. Crucial parts are identification of hazards and their consequences and risk assessment. Without these steps done properly, the following steps would be a simple waste of time. The SAM methodology is one of a few (maybe the only one), that provides a complex list of inputs a steps needed for conducting a proper safety study.

Acknowledgment

This paper was supported by the Grant Agency of the Czech Technical University in Prague, grant No. SGS14/212/OHK2/3T/16.

References

[1] The Global Aviation Development Summit Aviation Technology: www.aviation-technology.me. Aviation Technology: www.aviation-technology.me [online]. 2016 [cit. 2016-04-19]. Available from: http://www.aviation-technology.me/mod/events/13-The-Global-Aviation-Development-Summit.htmlJ. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] EUROCONTROL Safety Regulatory Requirement (ESARR 4): RISK ASSESSMENT AND MITIGATION IN ATM [online]. EUROCONTROL, 2001 [cit. 2016-04-19]. Available from: https://www.eurocontrol.int/sites/default/files/article/content/documents/single-sky/src/esarr4/esarr4-e1.0.pdf K. Elissa, "Title of paper if known," unpublished.

[3] Safety Assessment Made Easier Part 1, Safety Principles and an Introduction to Safety Assessment [online]. EUROCONTROL, 2010 [cit.

2016-04-19]. Available from: https://www.eurocontrol.int/sites/default/files/field_tabs/content/documents/nm/safety/same_part_1_v1.0_released.pdf

[4] LEVESON, Nancy. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, c2011. Engineering systems. ISBN 02-620-1662-1.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] NEBOSH National Diploma - Unit A | Managing Health and Safety: Element A3 | Identifying Hazards, Assessing and Evaluating Risk [online]. In: . © RRC Training [cit. 2016-04-19]. Available from: http://www.icao.int/SAM/Documents/2014-ADSAFASS/Fault%20Tree%20Analysis%20and%20Event%20Tree%20Analysis.pdf

[6] Safety Assessment Methodology PART I: Functional Hazard Assessment [online]. EUROCONTROL. [cit. 2016-04-19]. Available from: http://www.caa-ks.org/index.php/en/air-navigation-services/157-tp-13-sam-functional-hazard-identification

[7] International Civil Aviation Organization. Safety management manual (SMM) [online]. 3rd edition. Montreal, Quebec: International Civil Aviation Organization, 2013 [cit. 2016-04-19]. ISBN 9789292492144. Available from: http://www.icao.int/safety/SafetyManagement/Documents/Doc.9859.3rd%20Edition.alltext.en.pdf

[8] STEPHANS, Richard A. a Joe STEPHENSON. System safety for the 21st century. Updated and rev. ed. of System safety 2000. Hoboken, N.J.: Wiley-Interscience, c2004. ISBN 0-471-44454-5

[9] Air Navigation System Safety Assessment Methodology-SAM [online]. Civil Aviation Authority of Kosovo [cit. 2016-04-19]. Available from: http://www.caa-ks.org/index.php/en/air-navigation-services/156-tp-12-air-navigation-system-safety-assessment-methodology-sam

[10] SZABO, S., VITTEK, P., LALIŠ, A., ČERVENÁ, V.: Aviation Safety Investment Assessment Utilizing Return on Investment and Bayesian Networks. In Central European Conference in Finance and Economics (CEFE2015). Košice: Technická univerzita v Košiciach, Ekonomická fakulta, 2015, p. 646-652. ISBN 978-80-553-2467-8.

[11] VITTEK, P., LALIŠ, A., STOJIĆ, S., PLOS, V.: Runway incursion and methods for safety performance measurement. In Production Management and Engineering Sciences: Proceedings of the International Conference on Engineering Science and Production Management (ESPM 2015), Tatranská Štrba, High Tatras Mountains, Slovak Republic, 16th-17th April 2015. Bratislava: University of Economics in Bratislava, 2016, p. 321-326. ISBN 978-1-138-02856-2.

[12] Safety Assessment Methodology PART II: Preliminary System Safety Assessment [online]. EUROCONTROL. [cit. 2016-04-19]. Available form: http://www.caa-ks.org/index.php/en/air-navigation-services/158-tp-14-sam-preliminary-system-safety-assessment

[13] Safety Assessment Methodology PART III: System Safety Assessment [online]. EUROCONTROL. [cit. 2016-04-19]. Available from: http://www.caa-ks.org/index.php/en/air-navigation-services/159-tp-15-sam-system-safety-assesment