XLIV Symposium on Operational Research
SYM-OP-IS 2017
Zlatibor, 25-28 September 2017

METHODOLOGY FOR SAFETY RISK ASSESSMENT IN FUTURE AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS

BOJANA MIRKOVIĆ[1], TATJANA KRSTIĆ SIMIĆ[2], FEĐA NETJASOV[3], OBRAD BABIĆ[4]

University of Belgrade - Faculty of Transport and Traffic Engineering, Division of Airports and Air Traffic Safety

[1]b.mirkovic@sf.bg.ac.rs,[2] t.krstic@sf.bg.ac.rs, [3]f.netjasov@sf.bg.ac.rs, [4]o.babic@sf.bg.ac.rs

Abstract: *In future air traffic management (ATM) a significant increase in automation is expected, in order to cope with growing air transport demand. The automation will take more active role in provision of the air traffic control (ATC) services, while future air traffic controller (ATCo) will monitor and/or approve actions performed/proposed by automated ATC Systems. ATCo will need to be trained to safely adapt to new role, with special emphasis on participation in the case of automated system components failure. Designing appropriate training for future ATCo should rely on assessed safety hazards in future ATM. The methodology for risk assessment of future ATM concepts of operations is proposed and applied in AUTOPACE project. This paper presents eight steps that are a foundation for execution of safety hazard assessment. Brainstorming sessions with operational experts are perceived for hazard identification and for safety feed-back, i.e. providing recommendations for future training designers.*

Keywords: *risk assessment, air traffic management, hazard identification, air traffic controller, automation*

1. INTRODUCTION

Growing air transport demand creates constant pressure on the existing and prospective airspace and airports. In order to cope with such development in a safe and efficient way, according to SESAR and NextGEN initiatives, it will be necessary to develop a new generation of the Air Traffic Control (ATC) and Air Traffic Management (ATM) automation, communication, navigation and surveillance facilities and equipment, both airborne and ground-based. In such environment of advanced technology and high level of automation, better understanding of the particular processes and their influence on the human performances, becomes significant.

Based on SESAR's perspective (SESAR, 2014) about future evolution of ATC and ATM, ATM concept for 2050 and beyond is created within AUTOPACE project. A progressive introduction of more autonomous and decentralized systems is expected until full automation is reached. The implementation of such future ATC System will change the human (Air Traffic Controller - ATCo) role since the automated processes will replace significant number of tasks nowadays performed by ATCo.

This paper presents the knowledge arising from the AUTOPACE project (funded by the SESAR Joint Undertaking within the framework S2020 Exploratory Research Programme as part of the H2020 programme). The main objective of the project is to assess how novel automation features would impact on ATCo performances, tasks, skills and competences and training strategies. The AUTOPACE project should suggest training strategy for the future ATCos who will have less active role in regular, everyday operations, but needs to be adequately prepared to take over the given tasks once the ATC System failures occur. This paper addresses safety risk assessment, aiming to provide list of critical hazards that could be mitigated refining ATCo training strategies and/or the automation design.

Methodology for risk assessment proposed and applied in AUTOPACE project is presented in Section 2. Sections 3 to 8 describe each of the eight steps in more details. Concluding remarks are given in Section 9.

2. SAFETY RISK ASSESSMENT METHODOLOGY

In order to identify potential safety effects of the high automation implementation in ATC, the methodology for safety risk assessment of future ATM concepts of operation is proposed. The methodology is based on the fundamental risk management principles. Namely, the ICAO (ICAO Doc. 9859 2006) defines *risk management* as "the identification, analysis and elimination (and/or mitigation to an acceptable or tolerable

level) of those hazards, as well as the subsequent risks, that threaten the viability of an organization". Risk management serves to focus safety efforts on those hazards posing the greatest risks.
Risk management process assumes the following steps: hazard identification, hazard characterisation (severity/criticality, probability of occurrence, acceptability), risk mitigation and risk communication (ICAO 2005; ICAO Doc. 9859 2006; Netjasov 2015).

The methodology applied in AUTOPACE project consists of the following steps:

Step 1. Future ATM concept of operations definition;
Step 2. System boundaries and its components definition;
Step 3. Selection and definition of scenarios to be analyzed;
Step 4. Hazard identification: identify and analyze (qualitatively) safety hazards;
Step 5. Hazard categorization: chose the appropriate criteria (one or several);
Step 6. Hazard characterisation: assign severity and likelihood (in order to assess the risk of each hazard);
Step 7. Risk acceptance: define the risk criteria and list all the critical hazards;
Step 8. Provide safety recommendations for critical risks and propose risk mitigation measures.

3. CONCEPT OF OPERATIONS, SYSTEM AND SCENARIOS

Future ATM will be rather different than ATM we know nowadays. The sectors will evolve to significantly larger geographical areas. Within one large sector ATCo will be in charge for the certain number of flights (Flight Centric ATC). Supported with automation, one ATCo is assumed to take over both current roles: Executive and Planner Controller role. Free routing will apply. Airlines will file their desired trajectories that will pass through de-confliction process on the planning level. Airlines will enter negotiation process with ATC service providers about their trajectories. Once agreed on modified trajectories they will become so called 4D contract i.e. it will be guaranteed that trajectories will be conflict free along the way as long as airlines stick to it. More planning and pre-tactical interventions are expected and less tactical intervention. That, together with evolution in technology – surveillance, navigation, communication, data exchange etc., will enable conditions for higher involvement of automations in ATC processes.

In proposed methodology, future ATCo environment is observed through two main parts. Internal, core part contains ATCo and ATC System and their relations. External part (environment) gathers Local Traffic Manager, System Wide Information Management (SWIM), other ATC Systems/ATCos and traffic (aircraft/pilot) – Figure 1.

Two different visions of automation that could be expected by 2050 are assumed and analyzed in AUTOPACE project (AUTOPACE 2016):

- Scenario 1 – High Automation: ATC System assumes the major ATCo responsibilities. The ATCo takes the role of the supervisor of the ATC System operations (Figure 1, left).
- Scenario 2 – Medium Automation: ATCo has more active role. He/she decides which action to apply. ATC System proposes different alternative solutions of the actions to be performed (Figure 1, right).

For both scenarios, selected non-nominal situations (referring to system's function failure) were analyzed.

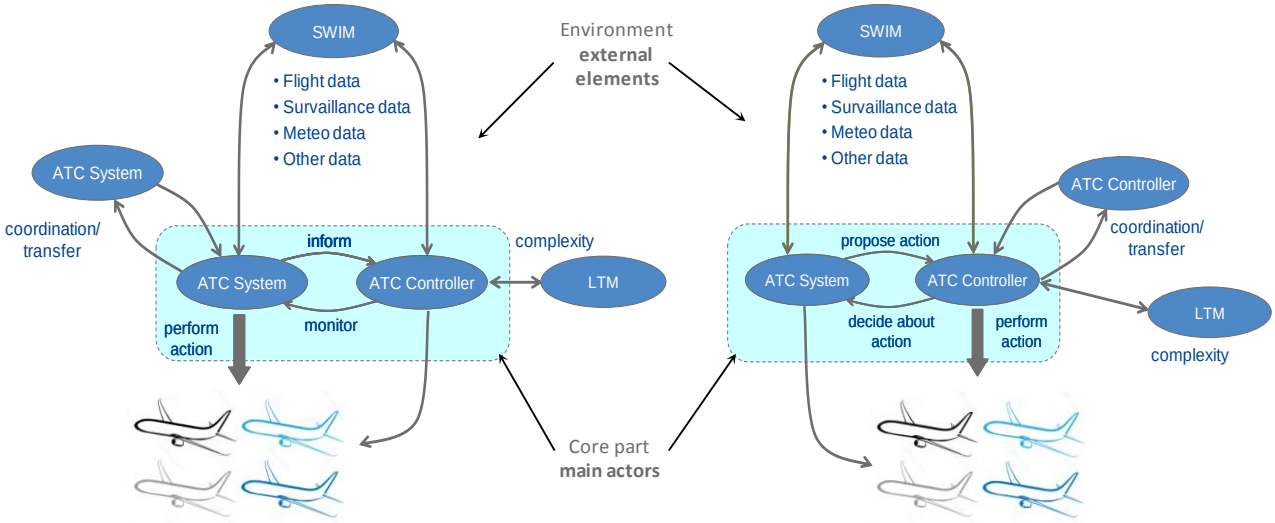

Figure 1: System elements and their interactions (left - Scenario 1, right - Scenario 2)

4. HAZARD IDENTIFICATION

Hazard identification is the most critical stage in safety assessment. “A hazard is an event/state that may: lead to a dangerous situation, or hamper resolution of such a situation, possibly in combination with other hazards or under certain conditions” (de Jong 2004; Netjasov 2015). Hazards may emanate from the operational concept itself (e.g. related to the proposed hardware, software, procedures, and/or human elements), from the external events in the environment (e.g. bad weather), or from failures or events in the system and/or other systems that can affect the system under consideration (FAA/EUROCONTROL 2007; Netjasov 2015).

Generally, hazards may be identified through a quantitative (data-driven) or qualitative process such as discussions, interviews and brainstorming. In order to assess safety hazards, an approach based on hazard identification brainstorming sessions with operational experts, combining advantages of four well known and complementary methods used in aviation is proposed:

- Brainstorming sessions with operational experts (focused on operational hazards) (ECAST 2009);
- Functional Hazard Assessment – FHA (focused on technical hazards) (SAM 2006; Netjasov 2015);
- Future Aviation Safety Team – FAST (focused on areas of change) (FAST 2006);
- Structured What If Tool – SWIFT (carried out on a higher level system description which is case in AUTOPACE project) (ECAST 2009; Netjasov 2015).

Since the far future system is analysed comprising lots of uncertainties, in AUTOPACE the main contribution was from the brainstorming sessions with operational experts. European Commercial Aviation Safety Team - ECAST describes brainstorming as “an unbounded but facilitated discussion within a group of experts.” The brainstorming session facilitator prepares “issues ahead of the group session and then encourages imaginative thinking and discussion between group members during the session.” The main characteristics of this way of hazard identification are that all “contributions are accepted and recorded and no view is challenged or criticized.” This way of working “provides an environment in which the experts feel comfortable in thinking” (ECAST 2009).

Two hazard identification (expert brainstorming) sessions were perceived in this case, both performed based on future tasks and description of nominal and non-nominal situations. The first one, with academic experts (in safety and ATM field) aims to result with initial set of hazards. The second with operational experts (experienced ATCos), aims to validate the initial set of hazards and possibly enrich it with some additional, complementary hazards.

5. HAZARD CATEGORIZATION

Two groups of hazards appeared as relevant: Operations specific i.e. general hazards are associated to the particular scenario/situation in general, and Task specific hazards which are related to the tasks which should be performed during operations.

In order to be consistent and comprehensive in hazard identification and, later, with hazard characterisation, for all observed scenarios/situations and types of tasks, hazards should be categorized with respect to several criteria. In AUTOPACE project three criteria for categorization are used:

I. Responsibility share;
II. Nature of hazard;
III. Origin of hazards (Internal/External).

The categorization is important for the risk assessment. Rules to assign severity and likelihood for hazards are connected to hazard characterization.

In the first group three levels of responsibility share between ATC System and ATCo are recognized. With respect to their origin hazards are split to those related to the core part of the system (ATC System and ATCo) and external components (belonging to environment). Nature of hazard is the most relevant categorization for hazard characterization. Eight categories are recognized in this project (e.g. Reduced situation awareness, Incorrect input, Uncertain traffic evolution, etc.)

6. HAZARD CHARACTERISATION

Hazard characterisation is a process in which for each hazard a severity and likelihood are assigned based on expert judgement.

Based on ICAO recommendations (ICAO 2005; ICAO Doc. 9859, 2006; Netjasov 2015) and some examples from industry and previous studies five category scale (1 - lowest to 5 - highest) for both severity and likelihood is considered as the most appropriate for AUTOPACE project. Each quantitative value holds the description given in Table 1 for severity and in Table 2 for likelihood.

When assigning the severity and likelihood to each hazard (task specific or general) some high level guidelines should be used concerning relations between values assigned to each hazard in different scenarios (nominal and non-nominal situations). As mentioned before, they should be connected to specific hazard category.

Table 1: Severity classes

Severity class		Description – possible effects on operations and air traffic service
5	**Accident**	Examples: Total loss of flight control. Mid-air collision.
4	**Serious (major) incident**	Large reduction in safety margins or a total loss of air traffic control for a significant time.
3	**Moderate incident**	Significant reduction in safety margins or significant reduction in air traffic control capability.
2	**Minor incident**	Slight reduction in safety margins or slight reduction in air traffic control capability.
1	**No safety effect**	No immediate direct or indirect impact on the operations. Slight increase in air traffic controller workload.

Table 2: Likelihood classes

Likelihood class		Description
5	**(Almost) certain**	May occur once or several times during the day.
4	**Probable**	May occur once or several times during one week, but not each day.
3	**Possible**	Unlikely to occur every day, but may occur once or several times during one month.
2	**Unlikely**	May occur once or several times during the year.
1	**Rare**	Should virtually never occur.

7. RISK ACCEPTANCE CRITERIA

The criteria adopted for AUTOPACE project to classify risks to be acceptable, tolerable (medium and high) or unacceptable are presented in the risk matrix – Figure 2 (description of risk levels is also provided). Each hazard is, according to assigned severity and likelihood, allocated in the appropriate field.

Green fields represent acceptable risk, considered to be manageable by routine procedures. Two levels of tolerable risk zone are defined for AUTOPACE. Yellow represents minor risk and requires development of appropriate procedure for the risk mitigation. Orange requires special, strategic mitigation measures to be developed and implemented. Unacceptable zone is shown in red, meaning that review of the system functioning (including both ATC System and ATCo, their functioning and inter-relations) is required in this area.

In order to provide proper safety feed-back, it is important to identify critical hazards and distinct between various types of hazards with respect to measures needed to decrease the level of risk – mitigation measures. Critical hazards are those with the High and Unacceptable risk level.

Risk matrix		Severity				
		1	**2**	**3**	**4**	**5**
Likelihood	**5**					
	4					
	3					
	2					
	1					

Level of risk	Description
Unacceptable	Review the functioning of the system.
High Risk	Strategical measures required. Develop and implement appropriate measures.
Medium Risk	Develop appropriate procedures in order to mitigate risk.
Acceptable	Manage by routine procedures.

Figure 2: Risk matrix applied in AUTOPACE project with description of risk levels

8. SAFETY RECOMENDATIONS

Critical hazards are divided in two groups. The first one is ATCo skills/competences related hazards, and the second one is System and procedures related hazards.

System and procedures related hazards should be taken into account during the system re-design and implementation.

The focus of AUTOPACE project is on the first group of hazards since their risk level can be decreased (through severity and likelihood) with appropriately designed training. Those are hazards related to ATCo

performances, reduced situation awareness due to boredom/fatigue/overload/too much information shown/ tunnelling, human errors - slips/lapses/mistakes/violations, etc. To find appropriate mitigation measures, training designers should pay attention to each hazard and its characteristics.

In this stage, another brainstorming session with experts involved with ATCo training (experienced ATCos, instructors, training designers, etc.) should be performed to identify possible measures to mitigate critical hazards through newly designed training for the future ATCos.

Second cycle of the safety analysis can be performed with modified training strategy in order to show how appropriate training improves safety of the system.

9. CONCLUSION

High level of automation in future ATM will significantly change concept of operations, and consequently human role in the future environment that is expected to engage automation to much more extent than nowadays.

Related to the main objective of the AUTOPACE project (to assess how novel automation features would impact on ATCo performances, tasks and training strategies), one of the goals was to identify potential safety effects of the high automation implementation, in order to provide list of critical issues that should be addressed by refining ATCo training strategies and/or the automation design.

In order to assess safety hazards, a methodology for safety risk assessment of future air traffic management concepts of operation is proposed and described in this paper. The eight step methodology is proposed. This paper describes each step and presents a foundation for execution of safety hazard assessment. Hazard identification, as the most important step, is performed through brainstorming sessions with operational experts, combining four well known and complementary methods used in aviation. The advantages of brainstorming sessions are also used in the final step to provide as more useful as possible recommendations to training designers.

Acknowledgement

This paper is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 699238 (AUTOPACE - Facilitating the Automation Pace, http://autopace.eu/) under European Union's Horizon 2020 research and innovation programme. The opinions expressed herein reflect the author's view only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.

REFERENCES

[1] AUTOPACE Consortium (2016). Deliverable D2.1. - Future Automation Scenarios (v00.02.00), H2020-SESAR-2015-1.

[2] de Jong H. (2004). Guidelines for the identification of hazards: How to make unimaginable hazards imaginable? (NLR-CR-2004-094), NLR, Amsterdam.

[3] ECAST (2009). Guidance on Hazards Identification. European Commercial Aviation Safety Team. European Strategic Safety Initiative (ESSI).

[4] FAA/EUROCONTROL (2007). ATM Safety Techniques and Toolbox, Safety Action Plan-15 (Version 2.0). US Federal Aviation Administration & European Organisation for the Safety of Air Navigation.

[5] FAST (2006). The FAST Approach to Discovering Aviation Futures and Associated Hazards, Methodology Handbook. Future Aviation Safety Team.

[6] ICAO (2005). ICAO Accident Prevention Programme. International Civil Aviation Organization, Montreal, Canada.

[7] ICAO (2006). Doc. 9859 - Safety Management Manual (SMM), 1st edition, International Civil Aviation Organization, Montreal, Canada.

[8] Netjasov F. (2015). Air Transport Safety: An Introduction (ISBN 978-16-3321-927-4), Nova Science Publishers, Inc., NY, USA.

[9] SAM (2006). Safety Assessment Methodology (Version 2.1). European Organisation for the Safety of Air Navigation.

[10] SESAR Joint Undertaking (2014). SESAR Concept Of Operations Step 2, B04.02, Del ID D105, Edition 01.01.00, 2014.