Manuscript Details

Manuscript number	SAFETY_2017_1067
Title	SAFETY RISK ASSESSMENT IN FUTURE HIGHLY AUTOMATED AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS
Article type	Research Paper

Abstract

This paper presents a methodology for safety risk assessment in future air traffic management (ATM) system developed and applied in AUTOPACE project. AUTOPACE project (funded by the SESAR Joint Undertaking within the framework S2020 Exploratory Research Programme) looks at future ATM system beyond 2050. Based on SESAR's vision, future ATM system will significantly change – larger sectors, Flight Centric ATM, free route airspace, 4D trajectories, dynamic sectorization, etc. Significant increase in automation is expected in order to cope with growing air transport demand in the future. The automation will take more active role during the provision of the air traffic control (ATC) services, while future air traffic controller (ATCo) will be rather a supervisor of actions performed by automated ATC systems. ATCo will need to be trained to safely adapt to new (less active) role, with special emphasis to be prepared for active participation in the case of automated system failure. The aim of the safety risk assessment is to provide the safety feedback to ATCo training designers. List of critical hazards is provided and risk mitigation measures that rely primarily on adequate training strategy of the future ATCo are proposed.

Keywords	Safety risk assessment; Hazard identification; Air traffic management; Air traffic control; Automation; Air traffic controller training
Taxonomy	Air Traffic Control, Aviation Safety, Hazard Analysis
Manuscript region of origin	Europe

Corresponding Author	Fedja Netjasov
Corresponding Author's Institution	University of Belgrade, Faculty of Transport and Traffic Engineering
Order of Authors	Fedja Netjasov, Bojana Mirkovic, Tatjana Krstic Simic, Obrad Babic

Submission Files Included in this PDF

File Name [File Type]

Cover letter.doc [Cover Letter]

Abstract.doc [Abstract]

Title page.doc [Title Page (with Author Details)]

Manuscript.docx [Manuscript (without Author Details)]

To view all the submission files, including those not included in the PDF, click on the manuscript title on your EVISE Homepage, then click 'Download zip file'.

Safety Science
Editor-in-Chief

Dear Sir,

I am submitting a paper for publication in Safety Science.

The Title of the paper is:

SAFETY RISK ASSESSMENT IN FUTURE HIGHLY AUTOMATED AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS

Fedja Netjasov, Bojana Mirkovic, Tatjana Krstic Simic, Obrad Babic

University of Belgrade – Faculty of Transport and Traffic Engineering
Vojvode Stepe 305, 11000 Belgrade, Serbia
f.netjasov@sf.bg.ac.rs, b.mirkovic@sf.bg.ac.rs, t.krstic@sf.bg.ac.rs, o.babic@sf.bg.ac.rs

I hereby inform you that this paper was not previously presented at any conference and is not under consideration by any other Journal neither is published elsewhere.

Sincerely yours,

Fedja Netjasov

ABSTRACT

This paper presents a methodology for safety risk assessment in future air traffic management (ATM) system developed and applied in AUTOPACE project. AUTOPACE project (funded by the SESAR Joint Undertaking within the framework S2020 Exploratory Research Programme) looks at future ATM system beyond 2050. Based on SESAR's vision, future ATM system will significantly change – larger sectors, Flight Centric ATM, free route airspace, 4D trajectories, dynamic sectorization, etc. Significant increase in automation is expected in order to cope with growing air transport demand in the future. The automation will take more active role during the provision of the air traffic control (ATC) services, while future air traffic controller (ATCo) will be rather a supervisor of actions performed by automated ATC systems. ATCo will need to be trained to safely adapt to new (less active) role, with special emphasis to be prepared for active participation in the case of automated system failure. The aim of the safety risk assessment is to provide the safety feedback to ATCo training designers. List of critical hazards is provided and risk mitigation measures that rely primarily on adequate training strategy of the future ATCo are proposed.

Keywords: Safety risk assessment, Hazard identification, Air traffic management, Air traffic control, Automation, Air traffic controller training strategy

SAFETY RISK ASSESSMENT IN FUTURE HIGHLY AUTOMATED AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS

Fedja Netjasov*, Bojana Mirkovic, Tatjana Krstic Simic, Obrad Babic

University of Belgrade – Faculty of Transport and Traffic Engineering
Vojvode Stepe 305, 11000 Belgrade, Serbia
f.netjasov@sf.bg.ac.rs, b.mirkovic@sf.bg.ac.rs, t.krstic@sf.bg.ac.rs, o.babic@sf.bg.ac.rs
* Corresponding author

SAFETY RISK ASSESSMENT IN FUTURE HIGHLY AUTOMATED AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS

ABSTRACT
This paper presents a methodology for safety risk assessment in future air traffic management (ATM) system developed and applied in AUTOPACE project. AUTOPACE project (funded by the SESAR Joint Undertaking within the framework S2020 Exploratory Research Programme) looks at future ATM system beyond 2050. Based on SESAR's vision, future ATM system will significantly change – larger sectors, Flight Centric ATM, free route airspace, 4D trajectories, dynamic sectorization, etc. Significant increase in automation is expected in order to cope with growing air transport demand in the future. The automation will take more active role during the provision of the air traffic control (ATC) services, while future air traffic controller (ATCo) will be rather a supervisor of actions performed by automated ATC systems. ATCo will need to be trained to safely adapt to new (less active) role, with special emphasis to be prepared for active participation in the case of automated system failure. The aim of the safety risk assessment is to provide the safety feedback to ATCo training designers. List of critical hazards is provided and risk mitigation measures that rely primarily on adequate training strategy of the future ATCo are proposed.

Keywords: Safety risk assessment; Hazard identification; Air traffic management; Air traffic control; Automation; Air traffic controller training

1. INTRODUCTION

The air transport system belongs to a class of complex, human-centered and safety-critical industries. Constant growth in air transport demand has many positive effects on the global economy, but providing additional capacity to accommodate such demand, can have a negative impact, primarily related to safety of operations. Namely, safety and capacity of one system are mutually conflicting goals, and tendency to further increase capacity could put system safety at danger. Increasing capacity without decreasing system safety requires the development of new technologies, operational procedures and corresponding regulations (Netjasov, 2015).

This capacity-safety relationship also applies for the Air Traffic Management (ATM) system. Further growth in air transport demand requires changes in ATM. These changes lead to further system evolution, i.e. to synchronized changes in procedures, pilot and Air Traffic Controller (ATCo) operating methods, airborne and ground-based systems, legislative and regulatory frameworks, and aeronautical data sources. All those changes have to be introduced carefully because it could jeopardize system safety (Netjasov, 2015).

Two ongoing programs dealing with the definition of the future of air transport systems are Single European Sky Air Traffic Management Research (SESAR) in Europe, and U.S. Next Generation Air Transport System (NextGEN). The main goal of both programs is to increase system capacity cost-effectively, while ensuring safety. The common vision is to integrate and implement new technologies to improve ATM performance. Both combine increased automation with new procedures, in order to achieve safety, economy, capacity, environmental and security benefits.

In future ATM a significant increase in automation is expected, in order to cope with growing air transport demand. The automation will take more active role during the provision of the Air Traffic Control (ATC) services, while future ATCo will monitor and/or approve actions performed by automated ATC systems. ATCo will need to be trained to safely adapt to new role, with special emphasis to be prepared for active participation in the case of automated system failure (non-nominal situations).

The main objective of the AUTOPACE project (funded by the SESAR Joint Undertaking within the framework S2020 Exploratory Research Programme) is to assess how novel automation features would impact on ATCo performances, tasks, skills, competences and training strategies. As a final result, 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: a) a safety feedback to ATCo training designers in a form of list of critical hazards for the pre-defined system design, and b) risk mitigation measures primarily associated to refining ATCo training strategies.

Paper is organized as follows. Section 2 defines eight steps of the safety risk assessment process proposed and applied in AUTOPACE project. Section 3 describes future Concept of Operations (ConOps), system boundaries and scenarios analyzed. Section 4 presents hazard identification approach used in AUTOPACE and the summary of the results - identified hazards and their categorization. Section 5 describes hazard characterization used to assess risks and introduces risk criteria to identify critical hazards. Safety feed-back based on critical hazards and risk mitigation measures are discussed in Section 6, followed by Conclusions provided in Section 7.

2. SAFETY RISK ASSESSMENT METHODOLOGY

In order to identify potential safety effects of the high automation in ATM, the methodology for safety risk assessment of future ATM ConOps is proposed. The methodology is based on the fundamental risk management principles. Namely, the International Civil Aviation Organization (ICAO) 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” (ICAO, 2006). Risk management serves to focus safety efforts on those hazards posing the greatest risks. The methodology applied in AUTOPACE project consists of the following steps:

1. Future ATM ConOps definition;
2. System boundaries and its components definition;

3. Selection and definition of scenarios to be analyzed;
4. Hazard identification: identification and analysis (qualitatively) of safety hazards;
5. Hazard categorization: choice of the appropriate criteria (one or several);
6. Hazard characterisation (risk assessment): assignment of severity and likelihood (in order to assess the risk of each hazard);
7. Risk acceptance: definition of risk criteria and listing of critical hazards;
8. Provision of safety recommendations for critical risks and proposal of risk mitigation measures.

After introduction of certain mitigation measures in ATCo training strategy, Steps 4 to 8 should be repeated, in order to evaluate to what extent safety of the system can be improved through adequately designed training.

3. AUTOPACE CONCEPT OF OPERATIONS, SYSTEM AND SCENARIOS

2050 AUTOPACE ConOps (AUTOPACE, 2016) has been defined on the basis of the state-of-the-art on future automation perspective in ATM in 2035 (SESAR, 2014) and the possible directions for its further evolution (2050 and beyond). Future ATM will be rather different than current ATM system. The sectors will evolve to significantly larger geographical areas, within which 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 ATCo role. Free routing will apply. Airlines will file their desired trajectories that will pass through de-confliction process on the planning level and will negotiate 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.

The system defined and analyzed in AUTOPACE project consists of the core part, environment and their interactions. The core elements of the system are ATC System and ATCo. The environment consists of all external elements such as: Local Traffic Manager (LTM) involved in traffic de-complexion process, other ATC System/ATCo (depending on the scenario), Aircraft/Pilot that receives instructions and data/information exchange (System Wide Information Management - SWIM).

Two Future Automation Scenarios are identified in AUTOPACE project (AUTOPACE, 2016): High Automation Scenario (S1) and Medium Automation Scenario (S2), presenting two independent visions for ATM system in 2050. In S1 extreme case is assumed - ATC System takes over all major ATC responsibilities, while ATCo acts only as a supervisor of the ATC system. In S2,

somewhat more active role of the ATCo is assumed - ATC System mostly proposes alternatives of the actions to be performed, while ATCo decides which action to approve or apply from the set of proposals given by the ATC system.

All ATC tasks performed 30 minutes prior to assuming (taking over) the flight until its transfer to another ATC System/ATCo are observed (28 tasks are identified in (AUTOPACE, 2016)).

Three levels of responsibility share between ATC System and ATCo are defined:

- Apply/Monitor: ATC System assumes the major ATC actions, the ATCo monitors system behaviour to prevent deviations;
- Propose/Approve: The ATC System proposes to the ATCo a set of actions to implement, and ATCo must approve it before being implemented;
- Support/Apply: Major ATC actions are performed by ATCo. ATC System only supports the ATCo decisions by providing him/her necessary information.

The responsibility share by tasks is summarized in Table 1 and also depicted in Figure 1.

TABLE 1 Share of responsibilities for the task execution between ATC System and ATCo in S1 and S2

Responsibility	**Tasks**	**S1**	**S2**
Plan conflict free paths	7, 8	Apply/Monitor	Apply/Monitor
Determine the needs for pre-tactical complexity solution measures	20	Propose/Approve	Support/Apply
Identify Conflict Risk	1	Apply/Monitor	ATC System
Early Conflict Detection and Resolution	6	Apply/Monitor	Propose/Approve
Coordination and Transfer	15, 16, 17*, 28	Apply/Monitor	Support/Apply (*Propose/Approve)
Monitoring	23-27	Apply/Monitor	Support/Apply
Separation provision	9, 10	Apply/Monitor	Support/Apply
Implement solutions	11, 12, 13, 18	Apply/Monitor	Popose/Approve
Input changes into Flight Data Processing System	14, 19	Apply/Monitor	Support/Apply
Communication - provide information and alerting service	2, 3, 4, 5, 21*	Apply/Monitor	Apply/Monitor (*Support/Apply)
Special instructions e.g. Holding	22	Propose/Approve	Support/Apply

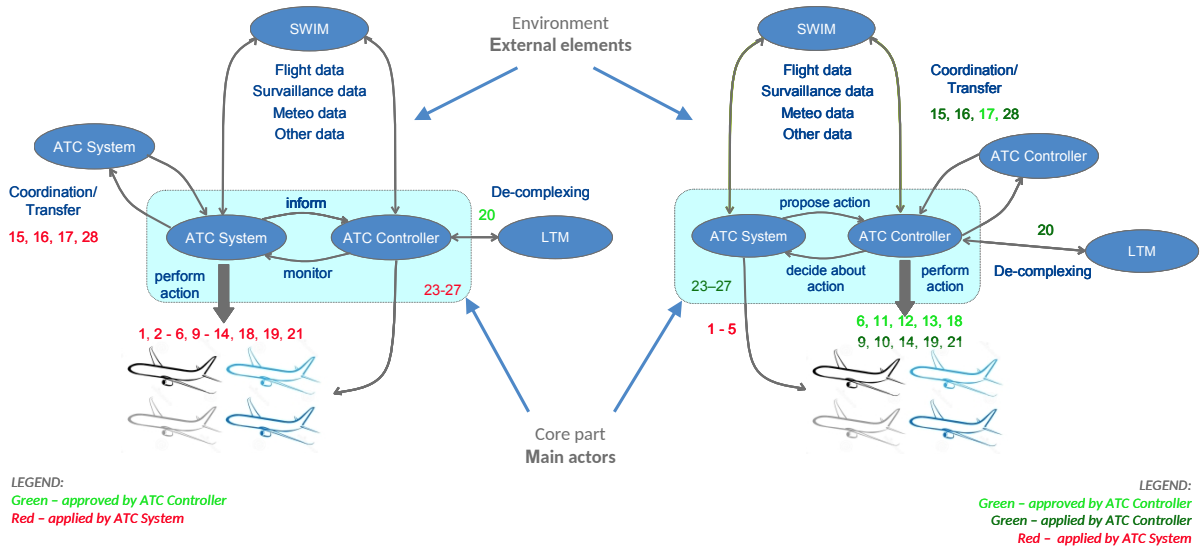

FIGURE 1 Responsibility share between ATC System and ATCo (left S1, right S2).

A failure or a malfunction in the service provision of one or several ATC tools is considered as non-nominal situations. Three non-nominal situations are addressed in AUTOPACE project (AUTOPACE, 2016):

1. The Conflict Detection and Resolution tools failure;
2. The Complexity Management Tools failure;
3. The System Supported Coordination Tools failure.

In all three non-nominal situations the ATCo will need to change his/her mode of operation i.e. to take over certain set of tasks performed by the ATC System in regular (nominal) conditions. Responsibility share between ATC System and ATCo changes. Such situations present the main challenge in designing training for the future ATCo.

The occurrence of each of those failures in S1 and S2 results in eight scenarios in total (two nominal and six non-nominal situations) addressed in AUTOPACE project.

Apart from non-nominal situation itself, transition from nominal to non-nominal situation was considered highly important for safety risk assessment, since it holds the potential for the most critical safety hazards. During the transition period ATCo should follow certain contingency procedure (AUTOPACE, 2017), i.e. to perform set of actions that enable taking over responsibilities for given set of tasks from ATC System, see Figure 2.

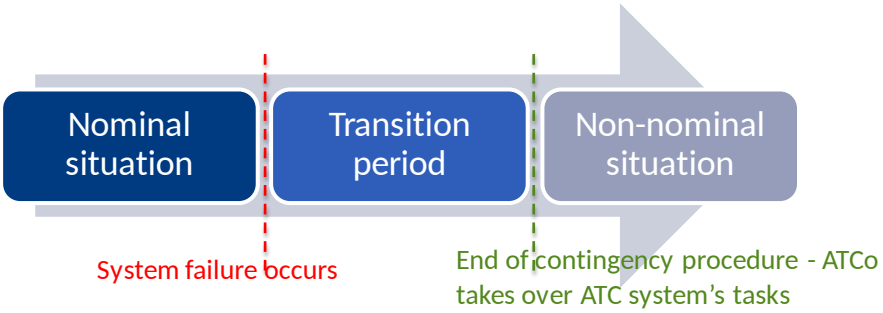

FIGURE 2 Transition from nominal to non-nominal situation

4. HAZARD IDENTIFICATION

Hazard identification (HAZID) is the most critical stage in safety risk 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. AUTOPACE project is specific because it looks in a far future – 2050 and beyond, so qualitative process was a single option. This fact together with fact that details for future automation are uncertain makes hazard identification process very challenging. In order to assess safety hazards, an approach based on hazard identification brainstorming sessions with operational experts was proposed, combining advantages of four well known and complementary methods used in aviation. Those are:

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

Due to lots of uncertainties related to future ATM system analyzed in AUTOPACE project, 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).

4.1 Hazard brainstorming sessions

Two HAZID brainstorming sessions were performed based on future tasks, responsibilities and description of nominal and non-nominal situations identified at the beginning of AUTOPACE project. The first one with academic experts (AUTOPACE representatives, experts in safety and ATM fields, four of them in total) resulted with initial set of hazards. The second one with operational experts (experienced ATCos from different Air Navigation Service Providers (ANSP), three of them from two ANSPs) together with four academic experts (AUTOPACE representatives) provided a validation of the initial set of hazards and enriched it with some additional, complementary hazards. During HAZIDs, special attention was paid to the list of tasks (28 of them, presented through 11 groups in Table 1) and how they are distributed among actors (ATCo and ATC System).

Having in mind the main characteristics of future automated ATM (ATC System takes active role, ATC Controller remains less active) two main sources of hazards are identified:

- A hazard can be the result of a system or component failure (failure and hazard are frequently linked, but it is not always the case), and
- A hazard can exist without anything failing – e.g. the human errors and mistakes can often lead to hazards.

In AUTOPACE project it is assumed that ATC System performs its tasks correctly i.e. its failures are limited strictly to three non-nominal situations. Possible corruptions or temporary failures of some support functions (such as data-link, human-machine interface (HMI), ATC support tools) were also considered.

The main focus of this project was on ATCo and tasks he/she performs. Human errors are the consequence of intentional or unintentional human behavior. Depending on the degree of intentionality preceding them they can be divided into the following categories (ICAO, 2002; Netjasov, 2015):

- Slips – unintentional actions resulting from a lack of appropriate attention caused by distractions, miss-ordered sequences or miss-timed actions;

- Lapses – unintentional actions caused by a memory failure arising from forgetting one's intention, losing one's place or omitting planned items;
- Mistakes – intentional actions resulting from errors in planning without any deliberate decision to contravene established rules or procedures.

Slips and lapses are "conditioned or automatic responses, with little, if any, conscious decision making", while mistakes "involve deliberate decision-making and evaluation, based on knowledge, experience and mental models that have worked well in the past". Also related to mistakes are violations, which are not errors. Violations involve intentional planning failures, often based on knowledge and the mental models acquired through daily experience, but also involve a deliberate decision to contravene established rules or procedures (ICAO, 2002; Netjasov, 2015).

Moreover, having observed far future ATM system defined on very general level, sources of hazards (besides ATCo skills/competences) can also be related to procedures and system design. In this case, if some aspects are not defined or not defined to enough depth, it is desirable to have them listed as potential hazards, thus drawing the attention to system designers to address properly those issues during the system design and prior to system implementation.

The main difficulty of hazard identification is to decide when a hazard identification exercise is complete because there are many things to consider, especially in terms of interactions between system elements. The main challenge involves shifting the boundary between imaginable and unimaginable hazards. That means hazard identification is a never-ending process which should be continuously carried out. The main output of hazard identification is a defined set of hazards which number in a certain system is generally infinite (FAA/EUROCONTROL, 2007; Netjasov, 2015).

4.2 Summary of identified hazards

During HAZIDs, it was noticed that some hazards (or group of hazards) are relevant for the particular scenario/situation in general – operations specific (general) hazards; while other hazards are specific for a particular task (one of 28) – task specific hazards. Among operations specific (general) hazards special attention is given to transitional hazards that occur only in non-nominal situations. After both HAZID brainstorming sessions a final set of hazards is defined. Total number of hazards per scenario/situation is given in Table 2.

TABLE 2 Number of hazards (different types) per scenario/situation

Situation	High Automation Scenario (S1)			Medium Automation Scenario (S2)		
	Task specific hazards	**General hazards**	**Transitional hazards**	**Task specific hazards**	**General hazards**	**Transitional hazards**
Nominal situation	101	9	not applicable	150	12	not applicable
Non-nominal situation 1	158	16	10	173	13	10
Non-nominal situation 2	88	11	10	133	12	10
Non-nominal situation 3	116	13	10	151	13	10

It should be noted that the same hazards (or group of hazards) can be associated to various tasks (or group of tasks) in the same scenario /situation and/or repeated in different scenarios. If one hazards repeats in 10 tasks in six non-nominal situations that appears as 60 hazards, but it is only one (with certain varieties) when it comes to risk mitigation measures.

Greater number of hazards is identified in the case of S2 which resulted from the more active role of ATCo in this scenario. Lesser number of hazards appears in more automated environment (S1) due to assumption that ATC System performs its tasks correctly.

4.3 Hazard categorization

In order to be consistent and comprehensive in HAZIDs and, later, with hazard characterization (assignment of severity and likelihood to each hazard), hazards are 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 hazard (Internal/External).

According to responsibility share types, three combinations of ATC System/ATCo responsibilities were recognized in the future ATM system (Figure 3, left) – Hazard category I (only task specific hazards can be categorized in such a way). The responsibility share was very important for hazard identification, triggered with performing a specific task, and later also for severity and likelihood evaluation. Nature of hazard can be various (Hazard category II). Eight groups are recognized (Figure 3, center). Further, with respect to their origin (Hazard category III, Figure 3, right) hazards are split to those related to the core part of the system (ATC System and ATCo) and external components (belonging to environment).

Rules to assign severity and likelihood for hazards are connected to hazard categorization. Nature of hazards is the most relevant categorization for assessing the safety risks.

FIGURE 3 Hazard categories with respect to responsibility share (green), nature of hazard (orange) and origin of hazard (blue).

4.4 Operations specific (general) hazards

Operations specific (general) hazards are hazards that are typical for the scenario/situation as a whole. Transitional hazards are a sub-group of general hazards that are related to transition period between nominal and non-nominal scenarios/situation, during which ATCo needs to complete contingency procedure, thus they appear only in non-nominal situation (actually ATCo changes his/her mode of operation, i.e. takes control over certain set of tasks regularly performed by ATC System in nominal situation). Total of 30 different general hazards are identified, out of which 12 are transitional. General hazards are not categorized with respect to responsibility share.

Majority of general hazards appear in both S1 and S2, like:

- *ATCo performance/Reduced Situation Awareness (SA)* (III-2/II-5): Reduced SA due to boredom (out-of-the-loop effect, i.e. overconfidence), overload (fear of automation effect) or fatigue; Omission of ATCo to carry out prescribed procedures; ATCo confusion about responsibility over specific flights, etc.
- *ATC System/Tool corruption* (III-1/II-6): Corruption/temporary failure of data-link, HMI or any other support function.

Some of operations specific hazards are typical only for S1, like:

- *ATCo performance/Reduced SA* (III-2/II-5): Skill degradation - wrong evaluation, reaction time too long, procedure mistakes, etc;
- *ATC System/Tool corruption* (III-1/II-6): Impossibility to take over control from the ATC System.

Examples of transitional hazards are:

- *ATCo performance/Reduced SA* (III-2/II-5): the same hazards as listed above for S1/S2, but they are characterized differently (higher severity),
- *ATCo performance/Other* (III-2/II-8): Transition process too slow;
- *Other/Undefined responsibility* (III-5/II-4): Lack of contingency procedure; Unclear responsibility share between ATCo and ATC System.

4.5 Task specific hazards

Great number of task specific hazards is identified. Some hazards (or group of hazards) are repeated for certain tasks (or group of tasks) in the same or even different scenarios.

Hazards related to *Communication/Incorrect input* (III-3/II-1) coming from the system data-base (SWIM) are considered as highly important in S1 when ATC system performs all the tasks. Although the ATC System works correctly the decisions based on the wrong data can be the cause of safety critical situations.

One of the most important group of hazards belongs to the *Coordination/Undefined responsibility* (III-4/II-4) group and assumes lack of „master system“ or „master“ ATCo, when solution requires communication between different ATC Systems/ATCos (e.g. separation violation between two flights under the responsibility of two different ATCos in the same airspace, Collaborative Decision Making with Local Traffic Manager, etc.).

Hazards related to *ATC System/Tool corruption* (III-1/II-6) assume data-link corruption (associated with the tasks that involve implementation of the solution and provision of some additional information to pilots) or temporary failures of other support functions (relevant for the tasks involving particular support).

The most relevant hazards for AUTOPACE project are those that belong to *ATCo performance/Reduced SA* (III-2/II-5). Hazards from this category identified for great number of tasks are:

- ATCo SA reduced due to high taskload/time required to perform the task, etc; ATCo has wrong awareness about the intent of the aircraft,
- Conflict risk not identified between aircraft; ATCo not aware of separation violation between certain pair of aircraft; ATCos confused about responsibilities over flights in conflict, etc. – hazards identified for the specific tasks in non-nominal situations when conflict detection and resolution tools fails.

In all the tasks that involve issuing certain instructions by ATCo, hazards related to human errors - slip/lapse/mistake/violation are identified. Slip, mistake and violation are categorized as

Incorrect action (category II-2) and lapse as *Reduced SA* (II-5). Slip is related to *Communication* (III-3), lapse and mistake to *ATCo performance* (III-1) and violation to *Other* (III-5).

Slip and lapse are associated to the tasks related to information provision or giving the instruction, when ATC system/ATCo responsibility share is *Support/Apply* (I-3) or *Propose/Approve* (I-2), i.e. when ATCo performs the action (applies or approves solutions/instructions, inputs the data, etc.).

Mistake and violation can occur in the tasks related to coordination and finding the solution for separation provision, re-routing, sequencing etc., only when ATC system/ATCo responsibility share is *Support/Apply* (I-3). Mistake and violation are not possible in *Propose/Approve* (I-2) responsibility share, because solutions are proposed by the system, and the assumption is that the system works correctly.

Such hazards exist today in any system that involves human actions and will continue existing in the future. They are something that should be adequately incorporated in the training, aiming not to eliminate them (which is impossible), but to decrease their likelihood as much as possible.

Some hazards related to pre-tactical decisions that can evolve in an undesired way due to various circumstances are also identified (e.g. Transfer given too early). They are mostly categorized as *Other/Uncertain traffic evolution* (III-4/II-7). Also, few hazards related to actions that cannot be performed (category *Other/Non-performable action*, III-4/II-3) are recognized in some of the tasks (e.g. Sector boundaries cannot be adapted to traffic routes).

5. HAZARD CHARACTERIZATION AND RISK ACCEPTANCE CRITERIA

Upon identification of hazards, each hazard needs to be characterized with severity and likelihood (probability of occurrence), in order to assess risk. Based on the chosen criteria, risks can be generally classified as acceptable, tolerable (undesirable) and unacceptable.

5.1 Hazard characterization

Hazard characterization is a process in which for each hazard a severity and likelihood are assigned based on expert judgments. Based on ICAO recommendations (ICAO, 2005; 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 3.

When assigning the severity and likelihood to each hazard (task specific or general) some general rules are used concerning relations between values assigned to each hazard in different

scenarios (nominal and non-nominal situations).

In nominal situations severity is assumed to be same or lower in High Automation (S1) than in Medium Automation (S2), since in the former the majority of the tasks (almost all) are performed by the ATC System. The opposite applies only for one category – *Incorrect input*. For *Non-performable action* and *Undefined responsibility* the severity is the same regardless of the scenario. For non-nominal situation 1 substantial change in responsibilities is expected. Severity is assumed to be serious (high) and should take the same values in both S1.1 and S2.1. In non-nominal situations 2 and 3 (in both scenarios) the severity will remain the same as in nominal situation in (majority) of tasks that do not require any change in responsibilities.

TABLE 3 Severity/Likelihood scale applied in AUTOPACE project

Severity scale		**Description – possible effects on operations and air traffic service**
5	**Accident**	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.
Likelihood scale		**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.

Likelihood is independent of the scenario, except for those that involve ATCo - *Incorrect action* and *Reduced SA*. For example, boredom/fear of automation are more likely to occur in S1, while fatigue - in S2. Likelihood for *Incorrect action* is higher when the ATCo is required to perform tasks he/she do not perform on regular basis, as everyday routine.

Since decimals cannot be used in hazard characterization (neither for severity or likelihood) higher value is assigned whenever there was a doubt between two integer values. Such more conservative approach is considered appropriate for the far future system observed in this case.

5.2 Risk 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 4 (description of risk levels is also provided). Each hazard is, according to assigned severity and likelihood, allocated in the appropriate field within the risk matrix.

Green fields represent acceptable risk, considered to be manageable by routine procedures. Two levels of tolerable risk are defined for AUTOPACE project. Yellow represents minor risk and requires development of appropriate risk mitigation procedure. 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.

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

Risk level	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 4 Risk matrix applied in AUTOPACE project with description of risk levels

6. SAFETY FEED-BACK FOR CRITICAL HAZARDS

6.1 Critical Hazards

In order to provide proper safety feed-back to ATCo training designers, it is important to identify critical hazards (hazards with significant safety issues), but also to distinguish between various types of hazards with respect to measures needed to decrease the level of risk - risk mitigation measures (those measures could be related to reduction of severity, likelihood or both). Critical hazards are those with the High and Unacceptable risk levels (red and orange in risk matrix).

Some hazards are related to system functioning and data accuracy, and it is not possible to mitigate safety problems caused by those hazards, with ATCo training only (e.g.: Incorrect/ incomplete input data, Incorrect weather forecast, Data-link corrupted, etc.).

Also, hazards related to some non-regular situations, indicate safety issues that can simply

appear in the system, but there are no special measures to prevent their appearance (e.g. Existence of unknown flights, Lack of procedure and/or undefined responsibility for interception of aircraft, Message sent by pilot is not in standard format, Insufficient capacity of an ATC centre, etc.). The likelihood of such hazards cannot be affected, but if ATCo is trained for these situations it can decrease severity of the hazards when they occur.

One of the most important group of hazards identified - Undefined responsibility, assumes lack of ”master system“ or ”master“ ATCo when solution requires communication between various ATC Systems/ATCos. Those hazards represent serious safety issues. But, if the scenario implementation (S1 or S2) assumes that clear responsibility between ATCo(s) and/or ATC System is pre-defined and ATCos are properly trained to recognize the “hierarchy” in all situations, those hazards will not be relevant any more, i.e. will not be the characteristic of the system that endangers safety.

And last, but the most relevant for the AUTOPACE project, are the hazards which could be mitigated through future ATCo training. Those are hazards related to ATCo performance, reduced SA due to boredom/fatigue/overload/too much information shown/tunneling, human errors - slips/lapses/mistakes/violations, etc.

Number of critical hazards (task specific + general + transitional) for High Automation and Medium Automation scenarios and corresponding non-nominal situations are summarized in Table 4.

TABLE 4 Number of critical hazards (different types) per scenario/situation

Situation	High Automation Scenario (S1)			Medium Automation Scenario (S2)		
	Task specific hazards	General hazards	Transitional hazards	Task specific hazards	General hazards	Transitional hazards
Nominal situation	7	2	not applicable	22	3	not applicable
Non-nominal situation 1	38	11	10	45	8	8
Non-nominal situation 2	5	4	3	18	5	3
Non-nominal situation 3	14	4	6	26	6	6

6.2 Safety Recommendations

Initial list of critical hazards (resulted from the first cycle of risk assessment) was used as an input for another brainstorming session with experts involved with ATCo training (experienced ATCos, instructors and training designers, four of them from four institutions) and AUTOPACE representatives (nine experts).

The goal was to identify possible measures to mitigate critical hazards through newly

designed training for the future ATCos.

Recommendations resulted from this brainstorming session were the following:

- Training should not be based only on technical aspect, but it should also contain psychological aspect (cognitive and non-cognitive). Future ATCo should practice his/her cognitive skills.
- Training for the (emergency) procedures, should be combined with human factor training (fatigue and stress management).
- Train ATCo to recognize symptoms for stress and fatigue (heart beating, sweating, etc.). "Self evaluation" would be more "accurate" than training third person (e.g. supervisor) to recognize those symptoms, because reactions to the same situation can be different among ATCos.
- Design simulation and theoretical training to prepare ATCo for transition procedure under various situations. Simulate failures to train ATCos for detecting the alert.
- Competence training should be combined with evidence training. Competence training should be based on numerous real-life examples (traffic demand and ATCo/ATC System relationship).
- Train ATCo for the team decision making (needed in Flight Centric ATC) and to recognize leader and follower in the team.
- Due to less active role in operations, higher number of training hours in simulation environment is needed (refreshing trainings). Interaction with the system (random checks, fake alerts, etc.) should be introduced to check attention and situation awareness. Maintaining SA is the key for hazardous situations related to ATCo performance, if not to avoid them, then to keep likelihood of their appearance as low as possible.

7. CONCLUSION

AUTOPACE project looks in a far future – 2050 and beyond, when significant changes in ATM system operations are expected, including higher involvement of automation in performing ATC services. Future ATCo will need to be trained to safely adapt to new (less active) role, with special emphasis to be prepared for active participation in the case of automated system failure (non-nominal situations). Developing appropriate training should rely on assessed safety hazards in future ATM.

Although high level guidelines are known for future ConOps, there are many uncertainties about ATM System design, procedures, etc. what makes hazard identification process very challenging. That is why an approach based on hazard identification brainstorming sessions with academic and operational experts is used, combined with principles from four well known and complementary safety assessment methods. Two expert brainstorming sessions were performed based on concept of operations, assumptions related to system definition and description of nominal

and non-nominal situations, defined and analyzed in AUTOPACE project. Final output from both sessions is the list of operations specific and task specific hazards identified. They were categorized with respect to several criteria: responsibility share, nature and origin of hazard.

Followed by hazard characterization, risk is assessed for each hazard and based on risk criteria, critical hazards are extracted. These are hazards with high and unacceptable risk levels. Another brainstorming session with operational experts is performed aiming to propose recommendation for mitigating (some of the) critical hazards through appropriately designed training for the future ATCo. The recommendations emphasizes the need to combine basic (technical) training with cognitive training and frequent refreshing training to keep ATCos attention and situation awareness at the acceptable level to deal with non-nominal situation if and whenever they occur.

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

AUTOPACE. *Deliverable D2.1 - Future Automation Scenarios*, version 00.02.00. AUTOPACE Consortium, H2020-SESAR-2015-1, 2016.

AUTOPACE. *Deliverable D3.1 - ATCo Psychological Model with Automation*, version 00.01.01. AUTOPACE Consortium, H2020-SESAR-2015-1, 2017.

Blom H., S. Stroeve and H. de Jong. Safety risk assessment by Monte Carlo simulation of complex safety critical operations. 14th Safety-critical Systems Symposium, Bristol, UK, 2006.

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

European Commercial Aviation Safety Team (ECAST). *Guidance on Hazards Identification*. European Strategic Safety Initiative (ESSI), ECAST, 2009.

European Organization for the Safety of Air Navigation (EUROCONTROL). *SAM - Safety Assessment Methodology*, version 2.1. EUROCONTROL, 2006.

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

International Civil Aviation Organization (ICAO). *Doc. 9806 - Human Factors Guidelines for Safety Audits Manual*, 1st edition. ICAO, Montreal, Canada, 2002.

International Civil Aviation Organization (ICAO). *ICAO Accident Prevention Programme*. ICAO, Montreal, Canada, 2005.

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

Netjasov F. *Air Transport Safety: An Introduction*. Nova Science Publishers, Inc., New York, U.S., 2015.

SESAR Joint Undertaking. *SESAR Concept Of Operations Step 2*, B04.02, Del ID D105, edition 01.01.00. SESAR JU, 2014.

U.S. Federal Aviation Administration & European Organisation for the Safety of Air Navigation (FAA/EUROCONTROL). *ATM Safety Techniques and Toolbox*, Safety Action Plan-15, version 2.0. FAA/EUROCONTROL, 2007.

U.S. Department of Transportation (DOT). *Risk Management Handbook*. U.S. DOT, 2009.