

Evaluation of air traffic management procedures—safety assessment in an experimental environment

Alberto Pasquini^a, Simone Pozzi^{a,b,*}

^a*Deep Blue s.r.l., Via Basento 52/D 00198 Rome, Italy*

^b*Department of Communication Science, University of Siena, Via dei Termini 6, 53100 Siena, Italy*

Available online 25 September 2004

Abstract

This paper presents and discusses the application of safety assessment methodologies to a pre-operational project in the Air Traffic Control field. In the case analysed in the present paper a peculiar aspect was the necessity to effectively assess new operational procedures and tools. In particular we exploited an integrated methodology to evaluate computer-based applications and their interactions with the operational environment. Current ATC safety practices, methodologies, guidelines and standards were critically revised, in order to identify how they could be applied to the project under consideration. Thus specific problematic areas for the safety assessment in a pre-operational experimental project are highlighted and, on the basis of theoretical principles, some possible solutions taken into consideration. The latter are described highlighting the rationale of most relevant decisions, in order to provide guidance for generalisation or re-use.

© 2004 Elsevier Ltd. All rights reserved.

Keywords: Safety assessment; Air traffic management; Human–computer interaction

1. Introduction

Air Traffic Control is an interesting example of the successful use of safety practices and methodologies. A considerable safety record has been achieved, since European Air Traffic Control currently contributes as a major cause in approximately 2% of aircraft accidents, with only two air collisions between civil aircraft over the last 50 years. However if the accident rate remains unchanged but the traffic volume increases, the total number of negative events will probably become unacceptable. Combining a static accident rate and increasing traffic ICAO¹ estimated an accident per week (see also EUROCONTROL [1, p. 16]). Hence considerable efforts are constantly put in

designing and experimenting with technological or process innovation. The object is two-fold: increase safety in current conditions, and assure appropriate safety levels in future operational environments.

The present paper describes the safety assessment of an experimental project in the Air Traffic Management (ATM) domain. Safety activities were thus conducted to explore future concepts and procedures for Air Traffic Management. This paper is divided in two main parts:

- the first part presents basic information about the ATM domain characteristics (Section 2), the safety assessment methodologies adopted therein (Section 3), the role of computer systems (Section 4), and the experimental project where the safety assessment activity took place (Section 5). This part is intended to provide the reader with a basic understanding of the main factors and problems that should be managed in safety assessment activities in an ATM experimental project;
- the second part describes the practical solutions adopted in our safety assessment activity to solve some of the above problems. In particular compliance to safety

* Corresponding author. Address: Department of Communication Science, University of Siena, Via dei Termini 6, 53100 Siena, Italy.

E-mail addresses: alberto@dblue.it (A. Pasquini), simone@dblue.it (S. Pozzi).

¹International Civil Aviation Organisation: ICAO was established in 1947 to develop principles and techniques of international air navigation and to support planning and development of international flight transportation.

standards is addressed in Sections 6.1–6.3. Accommodation to the peculiarities of an experimental project are considered in Sections 6.2 and 6.4. The assessment of the specific integration between computer systems and human actors is dealt in Sections 6.3 and 6.4.

2. The air traffic management system

The whole set of ATM services can be seen as a single system: there is a large number of elements (human and organizational actors, but also hardware components) and multiple interactions are taking place between them, with feedback loops and complex causal dependencies. What we deem relevant in this definition is the parallel with natural systems (as opposed to mechanical ones). A natural system is largely unpredictable (non-deterministic) and self-producing the causes of its own development. Each part has to be described on its own (because of its own peculiar behaviour), but it is also necessary to refer to the interactions with other system's elements. This causes the system behaviour to be to a certain extent unpredictable and far from perfectly known. Unexpected interactions may occur and, in addition, the system behaviour can be affected by external factors. In case of a local malfunction, failures are likely to spread very quickly to other parts of the system.

In respect to other safety critical domains, the ATM system is characterized by the key role played by human actors. As a matter of fact safety relevant decisions are taken mostly by humans, whereas computer systems are supporting tools for monitoring and data presentations. Hence controllers has a key-role in facing system complexity, because their main objective is to actively manage unpredictable situations affected by multiple elements.² It is important to highlight that complexity does not barely regard the environment. Indeed no clear cut separation has to be traced between the environment and the ATM system. The environment perception and the feasible actions are strongly affected by how controllers' working tools present information. In other words while defining the ATM system as a complex system, we need to consider that controllers' tools are entirely part of that system. Indeed radio communications, phone communications, radar displays and computers are system elements, that add to its complexity. The largely discussed transition from *paper flight strips to stripless systems* can provide a good example. In this case while designing new ATM systems that could digitally elaborate data formerly written on paper strips, designers were faced with the overwhelming number and

complexity of cognitive tasks supported by the paper flight strips. Paper flight strips could not be simply replaced by a digital system, and further studies addressing the whole set of controllers' tools and practices were required to avoid unexpected consequences (paper flight strips role in controllers' work and consequent implications for the design of new systems are described in Bentley [2]; Hughes [3]).

Another characteristic of the ATM work (at least of the en-route ATM work, that is the focus of the case presented in this paper) is that controllers usually perform few recurring tasks. Anyway, even if these tasks are well-known, their order remains largely unpredictable because of two main reasons. The former is that tasks are mainly event-driven and situation specific, thus spoiling most of the efforts to identify and predict task sequences. The latter is that the tasks' order is strongly affected by the complex strategic planning carried out by air traffic controllers. They do not simply react to local conditions, on the contrary they are constantly trying to predict traffic development in order to arrange safe traffic configurations.

These characteristics well justify the claim that ATM shall be analysed as a complex system, and that any technological innovation shall be assessed by taking into account how the system accommodates to its introduction.

3. Safety assessment in ATM

Safety issues have always played a primary role in ATM and continuous efforts and resources are being put in making the system safer. The travelling public acceptance of risks is relatively low compared to other transportation systems, thus safety represents a primary concern within the ATM community. Different general approaches were adopted in the ATM history, in order to cope with the main safety problems present at that stage of development. During the pioneering years, when the aircraft technology was still being developed, a fly-and-fix model was applied. Analyses were conducted after major incidents, in order to prevent their re-occurrence. The main efforts were thus concentrated on reacting to negative events. Clearly this model was bound to change, as soon as the increasing rate of technological innovations and of aircraft usage made unrealistic and uneconomical to follow the accident-investigate-fix model [4, p. 87].

Development of 'proactive models' marked the maturity of civil aviation, and the ATM domain readily adopted them. Proactive models are based on the early identification, assessment and mitigation of any credible hazards, thus assuring an inherently safe design, rather than reacting to negative events. The official date of adoption of this philosophy in ATM may be the 1979 ICAO Accident Prevention and Investigation Divisional Meeting. On that occasion the accident prevention was defined as involving

² This definition reflects a shift of emphasis from traffic control to traffic management occurred in the last 10 years. Consequently it is underlined the active role of flow management and traffic structuring, rather than 'simple' conflicts avoidance. The term Air Traffic Management has accordingly replaced the Air Traffic Control one.

an active search for hazards to be eliminated or avoided. As a guidance for proactive safety, ICAO delivered the Accident Prevention Manual (ICAO [5]). Although the manual was intended for pilots, the underlying approach was valid also for ATM and the rest of the civil aviation community.

Current safety practices are still based on proactive approaches, with some significant changes as far as the human role in the system is concerned. While the initial focus was on hardware elements, the fundamental role of humans in the system is now recognised. Theoretical contributions are adopted, that take into account human operators as part of the system design, not as following add-ons [6]. Focus is no longer on single isolated elements, but on the interactions between them, and on how they are rearranged to adapt to new events. Moreover during the last 15 years, the massive introduction of new digital technologies brought into light the necessity to adopt an user-centred point of view in the design and evaluation of the systems. The revolutionary opportunities offered by innovative technologies need to be driven by research on human cognitive skills, in order not to overwhelm the operator with meaningless information and functions. However integration between successful traditional hardware safety assessment techniques and human reliability methods is still an open problematic issue.

In the ATM domain, a state-of-the-art synthesis of Safety Management is provided by the Eurocontrol Safety Regulatory Requirements.³ These documents are issued as guidance for the Service Providers and they identify the requirements to comply with for adequate and effective safety management. In particular the ESARR4 (EUROCONTROL [7]) defines the requirements for risk assessment and mitigation when introducing changes in ATM systems. This requirement covers the human, procedural and equipment (hardware, software) elements of the ATM system, as well as its environment and operations. The objective of the ESARR4 is to ensure that the *risks associated with hazards in the ATM System are systematically and formally identified, assessed, and managed within safety levels, which as a minimum, meet those approved by the designated authority* (EUROCONTROL [7, p. 9]). The risk assessment process may be divided in the following phases:

- identify all ATM-related credible hazards and failure conditions, together with their combined effects;
- assess the effects that may have on the safety of aircraft, as well as assess the severity of those effects, using the ‘ESARR4 severity scheme’ (see Table 1).

³ Eurocontrol is the European organisation for the safety of air navigation. It currently numbers 31 Member States. Eurocontrol has as its primary objective the development of a seamless, pan-European air traffic management (ATM) system.

Table 1
ESARR4 severity scheme

Severity class	Effect on operations	Examples of effects on operations Include
1. [Most severe]	Accidents	-one or more catastrophic accidents; -one or more mid-air collisions; -one or more collisions on the ground between two aircraft; -one or more Controlled Flight Into Terrain; -total loss of flight control. No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).
2.	Serious incidents	-large reduction in separation (e.g. a separation of less than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation; -one or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).
3.	Major incidents	-large reduction (e.g. a separation of less than half the separation minima) in separation with crew or ATC controlling the situation and able to recover from the situation; -minor reduction (e.g. a separation of more than half the separation minima) in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).
4.	Significant incidents	-increasing workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional capability of the enabling Communication Navigation Surveillance system; -minor reduction (e.g. a separation of more than half the separation minima) in separation with crew or ATC controlling the situation and fully able to recover from the situation.
5. No safety effect [least severe]	No immediate effect on safety	No hazardous condition i.e. no immediate direct or indirect impact on the operations.

Depending on their potential effects, hazards are classified along a scale of five categories, from *accidents to no safety effects*;

- determine their tolerability, in terms of the hazard’s maximum probability of occurrence. As it will be

Table 2
Severity classification scheme

		FREQUENCY				
		Extremely Rare	Rare	Occasional	Frequent	Very Frequent
SEVERITY	Accidents					
	Serious Incidents					
	Major Incidents					
	Significant Incidents					
	No Immediate Effects on Safety					

The risk tolerability areas depicted below are hypothetical as they should be defined on a national basis.

better described below, these frequency thresholds are currently qualitative (apart from the worst case one);

- derive an appropriate risk mitigation strategy, which specifies the defences to be implemented, includes the development of safety requirements and presents an assurance of its feasibility and effectiveness.⁴

Hence safety objectives are based on risks, that are established in terms of the hazards maximum tolerable probability of occurrence and the severity of the effects. ESARR4 provides an European Safety minimum for the most severe class, set at 1.55×10^{-6} for accidents (with direct contribution from ATM) per Flight Hour. Frequencies for the other severity levels are not specified in ESARR4, and are to be determined at a national level based on past evidence on numbers of ATM related incidents, as soon as a reliable safety reporting and assessment system is established. In the meanwhile a qualitative definition is provided for five frequency categories (EUROCONTROL [8, p. 11]), that can be used to determine maximum tolerable probability of occurrence:

- *extremely rare*: has never occurred yet throughout the total lifetime of the system.
- *rare*: only very few similar incidents on record when considering a large traffic volume or no records on a small traffic volume.
- *occasional*: several similar occurrences on record. Has occurred more than once at the same location.
- *frequent*: a significant number of similar occurrences already on record. Has occurred a significant number of times at the same location.
- *very frequent*: a very high number of similar occurrences already on record. Has occurred a very high number of times at the same location.

⁴ What is described in a standard obviously differs deeply from what is feasible in the real world. In this case, usually time and resources availability seriously constrains the possibility to identify all relevant hazards. Furthermore it is highly unlikely that there are enough resources to mitigate all of them. Anyway the ESARR4 risk assessment process should also be intended as the description of a state-of-the-art process in ideal conditions.

It should be emphasised that frequency thresholds refer to an overall safety performance of ATM at European and national level and are not directly applicable to the classification of individual hazards. A method of apportionment of the overall probability to the constituent parts of the ATM system is still to be developed.

In order to deduce the effect of a hazard and to determine its severity, the systematic assessment shall include the effects of hazards on the various elements of the ATM system, such as: air crew, Air Traffic controllers, aircraft functional capabilities, functional capabilities of the ground part of the ATM system, ability to provide safe ATM services.

The combination of severity classes in Table 1 and of the above qualitative frequency categories results in a severity classification scheme as depicted in Table 2 (for other examples of severity classification schemes see EUROCONTROL [8, p. 10 and 15]; EUROCAE [9, p. 29]). Depending on the position on that scheme, a hazard is classified as:

- unacceptable and requiring mitigation actions (if it falls in the dark grey area),
- unacceptable if it is a single point failure (i.e. it is caused by only one failure, and not by a combination of more failures at the same moment), while it can be tolerable if multiple failures are implied (light grey area),
- acceptable as residual risks (white area).

The definition of the area of *risk acceptability* (or that of *mitigation actions needed*) is accomplished on a national basis, and it may vary depending on national legislation, traffic levels, technological infrastructure, etc. For instance the ALARP (As Low As Reasonably Possible) principle adopted in the UK or the Germany MEM (Minimum Endogenous Mortality) cannot be recognised as a valid principle by the Italian and Spanish law, that apply the Latin principle *neminem laedere* (no risk is acceptable). Figs. 1 and 2 show examples that highlight the differences between the Latin principle and the ALARP principle in an hypothetical case. The large unacceptable area in the *neminem laedere* principle highlights that the only acceptable severity level is the less severe one. For this

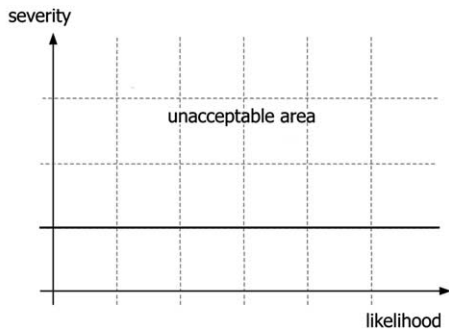


Fig. 1. *neminem laedere* principle.

reason in defining the acceptable probability of occurrence of any severity class it is impossible to refer directly to any of the above stated principles, but it should be adopted a definition of unacceptable risk that is compatible with all the national laws.

Besides identifying state-of-the-art risk assessment principles, the ESARR4 addresses another major goal of Eurocontrol: providing a common standard for the European ATM Service Providers. The general requirement for that may be identified in the deregulation and privatisation of the airline industry. In fact a general tendency to separate the provision of Air Navigation Services and national governments is apparent in Europe, thus exposing Air Traffic Service Providers to commercial pressures. This may seriously hamper safety and the coordination between organisations based all over Europe. On the contrary ATM need to assure comparable levels of safety all over Europe. Standardisation (and coherence with national legislations) has thus become a major issue, even more crucial after the inclusion in the European airspace of countries from the former Soviet Union block.

A major open issue is the extent to which specific project objectives may constrain adherence to standards. In the case discussed in the present paper the international guidelines and standards ([7,9–11]) had to be taken into account considering the specific needs and characteristics of the project. This inevitably lead to some significant differences. On the other hand a too strict standard hampers customisation to specific projects, making the standard useless.

Reliance on everyday operational experience is another key matter in the ATM risk assessment. It is widely

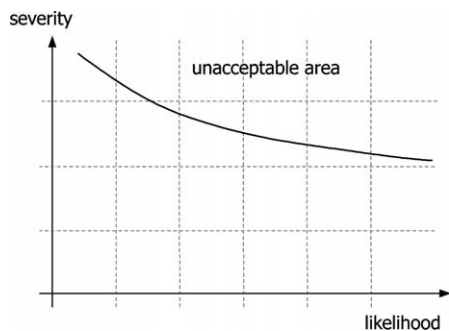


Fig. 2. ALARP principle.

recognised that human actors involved in the system daily functioning can provide fundamental feedback to system designers and safety experts. The argument is two-fold. First of all not all the occurrences can be foreseen and dealt with during the design phase. Secondly a system is likely to change significantly during its life cycle, due to environmental pressures or local adjustments. As a result reliance on reporting from pilots and controllers is the major information source for an effective monitoring during the operational phase (see ESARR4 [7], Section 8.2.3).

4. Role of computer systems

The concepts and principles steering ATM have evolved slowly, despite the traffic growth and the technological evolution. The result is a gap between technological possibilities and their exploitation by ATM. The increasing integration of computerised support systems have thus generated several debates and studies to clarify technologies' impact on ATM practices and procedures [12]. Nevertheless nowadays the ATM system certainly presents high density of computer systems. Computer support systems are used for a variety of functions, that we may roughly summarise in three categories, outlined in what follows.

As a monitor of human actions: given the high relevance of human decisions, computer systems are sometimes used to monitor the situation and alert the controller whenever a dangerous situation is detected. Computer tools in this category are known as 'safety nets', and for instance they may alert the controllers when two aircraft will be conflicting in 1 min Short Term Conflict Alert (STCA). Clearly the STCA is not a managing tool, rather it is meant to bring to the controller's attention undetected dangerous situations.

As planning advisors: this category represents the focus of many current researches. The computer system is used to help controllers in managing the traffic. This may be done for instance by algorithms that predicts aircraft trajectories, or by proposing ranked solutions from existing databases. All these systems leave the final decision to the human controller, but attempt to support his/her work by exploiting advanced computations.

Anyway the most pervasive category of computer usage is a very basic one: that is when computer systems are utilised in the essential working tasks. This category encompasses the vast majority of current computer systems. In this case computer systems form the infrastructure of the ATM domain, enabling the most basic activities. The most striking example is probably the controller console itself. Any information, apart from audio communications, passes through it, and it is transformed by appropriate data filtering or by customised representations that facilitate information gathering and decisions. The vast majorities of data used by controllers in their daily work is pre-computed. Controllers

continuously interacts with their consoles functionalities, and many controllers' actions possess a meaning only in relation to the computations performed by them. Furthermore cognitive psychology findings has demonstrated that the representation of a problem provided to users can strongly affect their performances [13], hence any pre-computation, data filtering or customised representation cannot be regarded as a neutral design choice.

The result is a tight integration between humans and computer systems, that possesses significant consequences on the safety assessment methodology. Any method that studies separately the controllers and their tools is probably running the risk to build non-existent boundaries between them, thus failing to grasp a correct understanding of controllers' activity. A systemic approach is required, in order to consider the various parts of the system without isolating single elements. As already pointed out above (see Section 3), in case of hazards assessment the analysis shall include the effects of hazards on the various elements of the ATM system, such as: air crew, Air Traffic controllers, aircraft functional capabilities, functional capabilities of the ground part of the ATM system, ability to provide safe ATM services. Thus only a comprehensive methodology can be adequate for an effective safety assessment, addressing the various system elements in interaction.

The above conclusion may be well illustrated by a specific case, where the integration between operator and tool leads to specify different procedures according to system characteristics. While managing the airspace between Italy and Greece, controllers have to work with radar displays with a scale that is larger than usual, due to the geographical extension of the area. This kind of visualisation makes it very difficult to work with usual separation minima that appear extremely small compared to the whole area. Prescribed separation minima are thus doubled. Therefore a specific hardware configuration is recognised as requiring different procedures. The underlying rationale is that the system (made of humans, tools and procedures) has to be taken into account as a whole.

In particular it should be highlighted that, in the daily working environment, practices and procedures always appear integrated with either a tool or a human actor. It is clearly possible to isolate and write down a procedure or a practice, but it should not be overlooked that its manifestation in the working activity is always bound to a physical support (human or tool). The integration between procedure-tool (or procedure-human) has relevant practical consequences on the safety assessment process and methodology (see Section 6.4).

5. The Mediterranean Free Flight project

As mentioned in the previous paragraph the ATM domain has long been characterised by a gap between

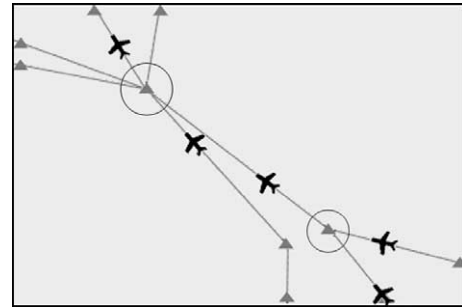


Fig. 3. Fixed routes airspace. Circles highlight congested waypoints.

technological possibilities and their exploitation. Currently ATM is based on ground-controlled traffic, airspace structured in fixed airways, ground controller responsibility for maintaining separation minima between aircraft, aircraft dependence on controllers' instructions and ground-based sources of information. To achieve the required targets in terms of safety, efficiency and cost-effectiveness, radical changes in the organization and methods of ATM are needed. The ideas of Free Routes and Free Flight are possible answers to these problems.

Compared to the actual fixed routes situation (i.e. aircraft move along pre-defined and fixed trajectories), the Free Routes airspace is based on the idea of user preferred routes (see Figs. 3 and 4). On entering an airspace sector, aircraft should be able to select whichever trajectory they prefer, in order to shorten the travelled distance.

The Free Flight concept refers to the capability of aircraft to self-separate. Suitably equipped aircraft will have the freedom to choose route and speed in real-time. Responsibility for separation assurance will rest with the aircraft in almost all circumstances. Mixed airspace are foreseen, where controllers will delegate separation assurance to some aircraft, while providing traditional air traffic service to other ones.

The Mediterranean Free Flight (MFF) project aims to investigate, simulate and assess these new ATM concepts and functions in a live ATM environment. For this purpose evaluation exercises are executed in Free Routes and Free Flight environments.

The MFF process starts with the definition of high level ideas of new ATM methods, then specifies procedures and requirements for their applications. The evaluation⁵ and refinement of procedures is carried out through evaluation exercises conducted in different environments, namely Fast Time (or Model Based) Simulations, Real Time Simulations (RTSs) and Flight Trials (FTs). The MFF project is based on several iterative cycles. Evaluation exercises will be repeated different times, to ensure appropriate feedback

⁵ In the present paper the term evaluation will be used as a synonymous of the term validation, that usually appears in ATM technical documents. The term validation refers to the process through which it is ensured that an ATM concept addresses the ATM problem for which it was designed and that it achieves its stated aims [14].

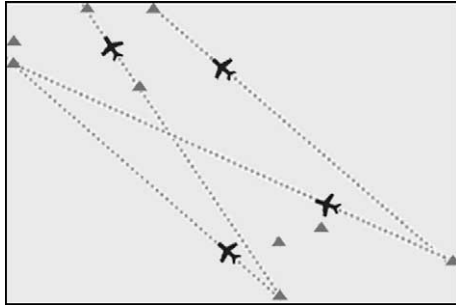


Fig. 4. Free routes airspace, with user-preferred routes. Aircraft can select whichever trajectory they prefer.

loops. Findings from the evaluation exercises will be utilised to refine ideas, procedures and requirements, that will be evaluated again in the following iterative step.

The most interesting findings for the safety assessment process are definitely obtained through Real Time Simulations and Flight Trials. The Real Time Simulation setting is a very interesting mixture of reality and simulation: basically controllers and pilots are humans, whereas the aircraft traffic is simulated on a computer platform. Controllers interact with their usual working console and speak via an audio-LAN with other controllers and with pilots. The latter are named pseudo-pilot, because they control the simulated aircraft through a computer console. Observers are also present in the simulation room, in order to gather data on controllers' behaviour and interactions, and to evaluate human-machine interface, procedures and working methods. This environment makes it possible to set up interesting traffic patterns (also very high density ones), observing controllers' reactions in real time. Traffic patterns can be managed in two ways. First of all they can be shaped directly changing the software parameters of the computer platform running the simulated traffic. But it is also possible to involve controllers and pseudo-pilots, in order to have them performing necessary actions (see Section 6.4, Table 5 for examples of accomplice pilots actions). Since Real Time Simulations can exploit an airspace of more than one sector, in the latter case observers can focus on just one or two sectors and arrange with remaining controllers to set up the configurations under analysis. The involvement of accomplice controllers or pseudo-pilots will be a key-characteristic for the definition of an integrated methodology for the MFF safety assessment (see Section 6.4).

In the same environment the airborne part can also be simulated, reproducing a cockpit and the interactions that pilots are supposed to experience with the new procedures and tools. Anyway as far as the airborne part is concerned, a more realistic environment is assured during the Flight Trials, where a suitably equipped aircraft is employed. Therefore procedures and tools are evaluated in the real operational environment, and only surrounding aircraft are simulated.

The main goal of the whole evaluation process is to analyse the advantages of identified procedures in terms of

cost effectiveness, safety, efficiency and capacity. Given the relevance of safety objectives, during the evaluation process a safety assessment is also completed. The safety assessment ensures that each proposed concept is evaluated in terms of its safety impact on the activity. The overall safety objective, explicitly stated in the MFF Safety Policy [15, p. 21], is to improve or, at least, to maintain the safety level of current procedures. In particular a safety case will gather safety data in order to ensure that the procedures developed within the MFF project are compliant with the ATM 2000+ strategy, which is: *To improve safety levels by ensuring that the number of ATM induced accidents and serious or risk bearing incidents do not increase and, where possible, decrease* (EUROCONTROL [1, p. 28]). No operational benefits can justify a decrease in terms of safety.

The MFF safety assessment process was designed to make the most of ATM safety assessment best practices. Thus it is compliant with international standards and safety principles, and with the guidelines therein (see MFF Safety Plan [16] and MFF Safety Policy [15]). Anyway, as already stated before, a thoughtless standard application cannot assure efficacy. The general framework had to be adapted to MFF specific objectives and resources. In the present case particular attention was paid to the difference between an operative project and the MFF pre-operative experimental status.

6. Solutions for the MFF safety assessment

In the previous paragraphs we identified and illustrated some major open issues to be taken into account in designing an effective safety case for a ATM project. During the MFF project some solutions that proved to be effective were considered. Thus it was possible to cope with the particular requirements of the ATM field and to the actual needs of the project. In particular safety standards compliance is addressed in Sections 6.1–6.3. The peculiarities of an experimental project are considered in Sections 6.2 and 6.4. The specific role of computer systems is dealt in Sections 6.3 and 6.4.

6.1. Compliance with international standards

The MFF safety case is designed to comply with the process and the requirements of ESARR4 [7]. According to the phases illustrated above (hazards identification, hazards evaluation, mitigation means) it was planned to develop three main steps: Operational Services and Environment Definition (corresponding to hazards identification), Operational Hazard Assessment (hazards evaluation), Allocation of Safety Objectives and Requirements (mitigation).

An Operational Services and Environment Definition (OSED) gathers all the information concerning the operational services provided by MFF. The OSED describes the characteristics of the envisaged environment. It is developed

in order to support the safety assessment process, hence it is supposed to contain all the relevant information for it. In theory no further assumptions or information are needed by safety experts, whose decisions can be grounded on OSED contents.

The next step consists of an Operational Hazard Assessment (OHA), which aims to identify all the credible hazards that could affect system operations. A thorough assessment of their potential effects under worst case conditions is conducted. Afterwards hazards severity is ranked using a qualitative classification scheme (compliant with the one identified in the ESARR4), that is also utilised to specify a maximum acceptable frequency of occurrence. As a result, at the end of the risk identification and assessment process safety objectives are determined for each credible hazard.

The final step is tightly interrelated with OHA, because the hazard assessment results therein are utilised to inform the design decisions about safety objectives. The Allocation of Safety Objectives and Requirements (ASOR) specifies a first allocation of safety, performance and interoperability objectives to specific parts of the system. Risk mitigation strategies for the whole system are designed and evaluated at this stage. A set of safety requirements and the responsibility for their implementation is eventually defined. The overall design should ensure that all the non-acceptable risks are eliminated or at least mitigated, either in frequency or in severity.

This process is meant to guarantee traceability of decisions from operational requirements to hazards. At the same time it is intended to make explicit any underlining assumption about the expected operational environment. The introduction of unmotivated assumptions in the risk assessment process is a widely recognised issue in the scientific literature [17–19]. In fact assumptions are often necessary to provide a frame for the evaluation process, but it should not be underestimated the powerful effect of the chosen frame on the conclusions. That means that the framing of a problem and of the possible solutions is very likely to give shape to the decisions taken. In a pre-operational project like MFF some reasonable assumptions may turn out to be inappropriate at a later stage of development. As a consequence the frame of reference for safety relevant decisions may happen to change. For that reason a clear traceability between safety decisions, hazards and operational context is mandatory. However this requirement would be of little use if proper feedback loops aren't included in the process. Hence, the second solution adopted in the MFF deals with feedback loops.

6.2. Providing safety feedback

A three-steps safety case is planned, for effective feedback between the safety case and the project life cycle. Each safety case step is developed in different phases of the MFF project. As already mentioned the MFF project is based on several

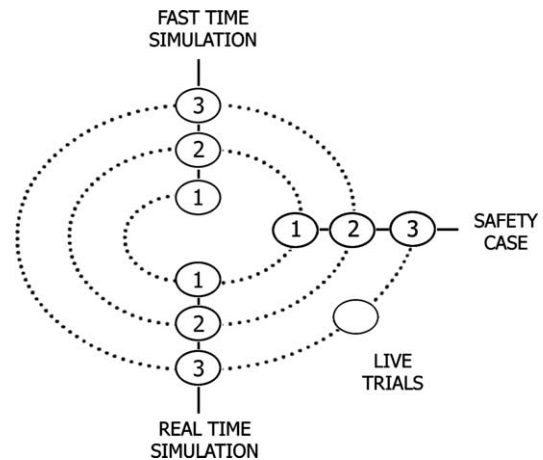


Fig. 5. Feedback loops between the steps of the safety case and the evaluation exercises.

iterative cycles (see Fig. 5), that allow the gathering of feedback from simulations and live trials. From one cycle to the next one, requirements and procedures are revised and specified accordingly, thus constantly modifying and detailing the project characteristics.

The three safety case steps (Preliminary, intermediate and final) have been designed following the same time frame. Thus their level of detail will depend on the data available at the moment, according to the simulations and live trials already performed and to the level of development of requirements and procedures. In this way each step reviews, details and assesses the validity of the previous step(s), at the light of the new data gathered, both in the simulation environments and from operational experts' feedback.

The Preliminary and the Intermediate steps also address the communication and coordination between MFF safety experts and people involved in the different MFF activities, whereas the third and final safety case step has to be effective in providing the appropriate information to future projects moving from the pre-operational status of a project like MFF to operational status (in the same way the MFF project considered safety activities of related projects).

With reference to the design of the process, feedback inputs to the other MFF activities were explicitly planned. According to the MFF plan, formal safety inputs will be provided three times (by the above mentioned Safety Cases), at different moments. As a consequence the ability to affect the development of the project is maximised, since safety insights can be assured for the whole duration of the project. Hence simulations and live trials can be designed according to safety analyses to be performed, providing new data on hazards, or testing mitigation means. A single step safety case would have run the risk of identifying interesting issues too late, and it would have also faced a too large amount of information.

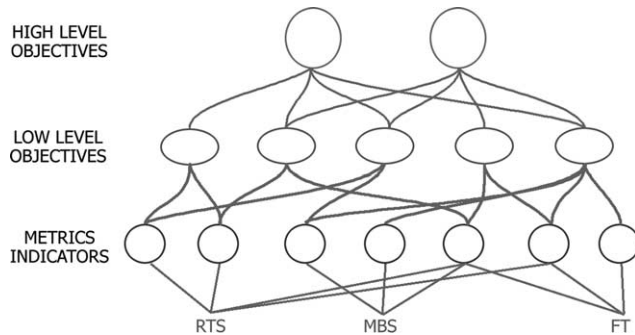


Fig. 6. Hierarchy of safety objectives and metrics.

6.3. Coordination and integration of different evaluation exercises

The overall safety objectives of the MFF project are defined in abstract terms, that cannot be related to specific measurable (or observable) issues. To assure an effective safety assessment these objectives had to be associated to more detailed and low level objectives. Actually a low level objective identifies the specific aspects of the activity to be analysed, in order to assess the high level objective. The relation between these two levels is many-to-many, that is a low level objective can be related to more than one high level objective, while a high level objective is assessed through more than one low level objective (see Fig. 6).

The third level depicted in the figure is represented by metrics and indicators. This level is meant to identify what can be observed or measured in the system, in order to analyse and assess low level objectives. The link between the second and the third level is not a straightforward one. Low level objectives are usually expressed in rather specific terms, but they typically refer to the overall system behaviour. On the contrary the metrics should be related to individual actions or interactions. Drawing from complex systems theory [20] we may say that metrics constitute local elements interacting, whereas the low level objectives may be identified with emerging properties, that can only be observed at a systemic level. No need to further highlight that an emerging property cannot be related by definition to the local level. The extent to which the link between these levels may be apparent and clearly connected to an appropriate system model varies depending on the matter analysed.⁶

A detailed example may help clarify the issue. A general safety objective of the MFF project is *to assure that the system is at least as safe as current operating conditions* (see MFF Safety Policy [15, p. 21]). Some of the corresponding low level objectives may be: *determine*

whether the overall level of workload is changed by the introduction of new support system, determine whether the overall level of workload is changed by the introduction of new procedures, determine whether military activities impact differently in the new operational environment, etc.

Corresponding metrics and indicators: number and duration of radio communications, number of altitude, heading and speed changes, number and duration of phone communications with adjacent sectors or military controllers, etc.

The process of identification of all the metrics needs to take into account the experience of many stakeholders: safety experts, human factors, and most of all people involved in the organisation of the evaluation exercise, whose knowledge of the evaluation environment should not be overlooked.

The number and variety of metrics to be studied required the preparation and coordination of different evaluation exercises, because during each exercise data could be collected only on some specific qualitative or quantitative metrics. The main reason is that each exercise was carried out in a peculiar environment (i.e. Real Time Simulations, Flight Trials or Model Based Simulations), where only some methodologies were appropriate. The coordination and integration of different evaluation exercises allowed to make the most of each one's strong points.

Coordination of many metrics is required to evaluate any low level objective, since it is highly unusual that a low-level objective can be evaluated using only one metric. In the same way each metric may be related to more than one low level objective. The integration and coordination of several metrics allow the consideration of the whole system, without isolating a single aspect and overestimating the relevance thereof.

Last but not the least, almost independent data sources (in this case different environments and exercises) assure a methodologically sound cross-checking of results, highlighting potential discrepancies (or consistencies).

6.4. Assessing the tool–procedure integration

The MFF project relied extensively on Real Time Simulations and Flight Trials as sources of data. By definition an experimental project has to gather and produce new data, since no previous experience is available. The validity of similar project findings or of generic databases is usually questionable. Indeed it has to be verified the extent to which results may be transferred from one context to a different one, even in those cases where findings and methods of analysis can be comparable. For instance probabilistic research on human reliability has too often turned out to be highly context sensitive, thus losing nearly all of its predictive power [23, p. 231].

To overcome these limitations it was planned to make extensive use of data collected during Real Time Simulations and Flight Trials. These experimental environments

⁶ An approach based on similar principles and logic has been proposed by Boehm [21] for a software validation process, and by Leveson [22] for the definition of software requirements at different abstraction levels. In any case, the different objectives of a software requirements specification and of an evaluation process should not be overlooked.

present many advantages, that largely compensate resources devoted to their planning and management. First of all Real Time Simulations and Flight Trials allow to evaluate the system as a whole. As previously mentioned (see Section 4) the tight integration of human and computer systems in the real work settings makes unrealistic any assessment that considers each element in isolation. On the contrary during Real Time Simulation and Flight Trial human–computer interactions are placed in a realistic context, thus enabling a systemic analysis of safety issues.

In more detail, the evaluation of new tools and new procedures was an essential part of the MFF exercises, that is to study how controllers' usual working practices and tools could accommodate to the introduction of new tools and procedures. As mentioned before (see Section 4), ATM procedures and practices always appear as integrated with either humans or tools. The safety assessment should therefore study the properties of the integration, and not merely address the 'disembodied aspect' of procedures. For this reason new procedures and tools should be studied in the operative context, where the integration can be apparent. A de-contextualised comparison of a procedure with the one it is supposed to replace is likely to keep out of the assessment essential elements. For instance it cannot evaluate adequately the interactions between the tools normally associated with the replaced procedure and the new one. On the contrary it can be easily figured out that the new tool–procedure integration may interfere with the old ones, maybe disrupting efficient and semi-automated sequence of interactions.

The major strong point of the Real Time Simulations and Flight Trials settings is that they enable to employ integrated methodologies, that combine careful analyses of each element with the study of their interactions. In these environments it is possible to gather data on each single element from a systemic point of view, that is to assess a new procedure by how a system accommodates to its introduction. One of the main means employed by MFF for this purpose was to implement some relevant scenarios in the simulation. A scenario describes an operational situation by identifying the actors involved, the operations going on, the tools and procedures being utilised [24]. In a Real Time Simulation setting this means describing (and implementing) some specific conditions, in order to observe how controllers react to and manage the situation recreated. A scenario evolution can hardly be predicted, since it is deeply affected by human variability. For this very reason scenarios are very powerful means to collect information from a systemic point of view, since they bring into light controllers' role in the ATM system. Furthermore the structure provided by a scenario enables the observer to gain a deeper understanding of controllers' activity, by making their specific goals and intentions apparent. Every observed interaction can then be analysed from an appropriate point of view, i.e. one that takes into account controllers' intentions and operational knowledge. Specific scenarios

were developed to assess the introduction of new procedures, and they proved to be appropriate means to discover new unforeseen hazards, not covered by previous hazard lists.

Another major use of scenarios in the MFF project was to enrich the process of hazards analysis, by implementing safety scenarios in the Real Time Simulations. Critical situations were recreated, according to hazards that may induce them. In this way information could be gathered to assess severity of the consequences, to identify co-occurrence of other hazards and their effects on the system. A brief description of the process of OHA construction and refinement may help detailing the way relevant hazards could be simulated.

The first step is to identify credible hazards and failure conditions (as specified by ESARR4 [7]. See also above in Section 3). In MFF this meant gathering a set of hazards from different sources and assessing if they could apply to MFF specific system configuration. Data sources considered were:

- information contained in the OSED;
- generic hazards databases;
- experts interviews;
- brainstorming sessions with controllers.

The first obvious source was the analysis of information contained in the OSED and the task analysis of the MFF procedures. For instance every procedure could be divided in different phases (an example is depicted in Fig. 7), and possible mode of failures identified for each one of them.

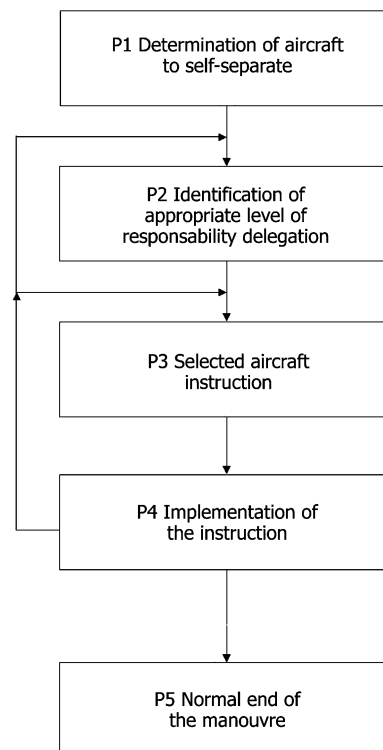


Fig. 7. Phases of the self-separation procedure.

Then the MFF project exploited generic hazards database to identify credible hazards, and to maximise their validity it was performed a cross-checking with domain experts' opinions. The experts were selected among experienced controllers or among controllers involved in the Real Time Simulations. Anyway even after the experts' validation these data needed to be considered taking into account well-known cognitive biases (i.e. novelty can make underestimate a hazard frequency, whilst an infrequent hazard can be highly overestimated if it happens to occur during the Real Time Simulations [18]. The same *caveat* applies to group brainstorming sessions, that were conducted with other domain experts. They were asked to reflect on their operational experience in order to imagine and describe potential hazards in the new environment.

Hazards identified at this stage could be described at a good level of detail, but it proved hard to assess potential consequences and severity whenever new hazards were considered. For instance an operational hazard identified in this phase was: *an aircraft (under controller's responsibility) is interfering with a pair of aircraft that are self-separating between each other* (see Fig. 8).

In the present case it was judged that more information should be obtained, given that the novelty of the procedure (i.e. the two aircraft increased freedom) may have an unpredictable impact on controller's activity. Real Time Simulations represented certainly a proper environment to obtain more data.

Only a limited sample of hazards could be simulated (given cost and time constraints), thus hazards were prioritized on the basis of the safety experts confidence in severity and consequences estimates. In other words, the hazard with the highest priority were those for which the safety experts were less confident in the estimated severity and consequences. At this point, the major difficulty was to reconstruct a realistic situation where the procedure and the related hazard could be analysed from a systemic point of view, preserving all contextual factors that shape controller's behaviour. Safety scenarios were then used to avoid the assessment of hazards in isolation, so that credible situations could be presented to controllers. Broadly speaking, any safety scenario represented a problem offered to

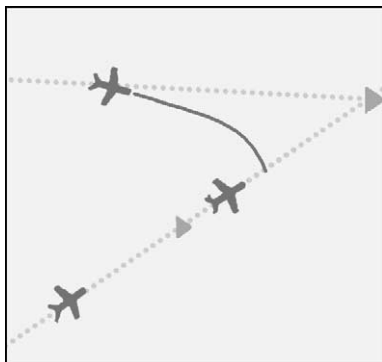


Fig. 8. aircraft interfering with a pair of self-separating aircraft.

Table 3
Information used as input for scenario implementation in Real Time Simulation

Operational hazard identifier	An aircraft (under controller's responsibility) is interfering with a pair of aircraft that are self-separating between each other.
Preliminary scenario description	Two aircraft are involved in self-separation manoeuvres and are flying to the same way-point. They are for instance under a Remain Behind operation. An aircraft is also converging to the same way-point but it abruptly deviates from its cleared trajectory and interferes with pair of aircraft involved in self-separation manoeuvre (see Fig. 8).
Detection means, if any	Short time warnings (STCA) are triggered and involve the three aircraft
Fall-back procedures, if any	Navigation instructions may be provided to one or two aircraft, which could possibly impair on the self-separation instruction. Temporary interruption of the self-separation instruction and possible re-initialisation of the same instruction.
Hazard effects on operations	In a very short term the controller will have to face a conflict and in parallel to manage an on-going self-separation instruction. The worst case is met when the controller will have to issue navigation instructions to one of the self-separating aircraft to solve the conflict, which will be incompatible with the instruction itself. Activity of the involved actors will heavily increase. After the resolution of the conflict, re-initialisation of the instruction is still possible.
Severity according to ESARR4	1 to 3 because of the workload induced to controller and involved aircraft and because of the necessity to perform an immediate avoidance manoeuvre to solve a conflict
Objectives of the simulations	It is expected to test the reaction of the controllers, who will have to face a conflict: How will they manage such a complicated situation? It is unclear whether the controller will give priority to the pair of aircraft: will the controller try to provide avoidance manoeuvre instruction to the interfering aircraft, prior to impact on the aircraft involved in the self-separation manoeuvre? Is it necessary to interrupt the self-separation instruction? In that case, will the controller intend to re-initialise the instruction?

the controller, in order to observe the impact of the hazard on the activity, controller's ease of detection and mitigation strategy.

Next step was then to specify for each hazard to be investigated the objectives of the simulation, what to observe and which data (quantitative or qualitative) should be obtained. Data collected at this point were used as input for scenario revision and implementation in the Real Time Simulation environment (see Table 3). Data were collected also after each simulation session, by conducting post session debriefings with controllers involved, or by gathering reporting sheets filled in by controllers.

Scenario building is a time consuming activity, since it requires the coordination of various expertise. Each scenario needs to present relevant situations for the analyst, it shall be

Table 4
Actors and process of scenario-based hazard analysis

Actors		
Safety experts	Real time simulation experts	Operational experts
Identification and prioritisation of the hazards to be investigated		Identification and prioritisation of the hazards to be investigated
Description of the hazard and of the main aspects to be investigated		
Preparation of preliminary scenarios		Preparation of preliminary scenarios
Revision of scenarios (iterative)	Revision of scenarios (iterative)	Revision of scenarios (iterative)
Identification of measures and information to be collected	Identification of measures and information to be collected	
Scenarios implementation	Scenarios implementation	

defined in a way that can be implemented, and it has to be realistic. Furthermore it may detail hazard that come from sources as different as the ones outlined above (see beginning of this section). Thus several iterations may be necessary between analysts, Real Time Simulation experts, and operational experts (see Table 4).

In this respect scenarios were also an effective means of communication between people directly involved in the simulation preparation and safety experts. The latter could effectively use their work (i.e. OHA drafts), transferring it to a consistent format that did not cause awkward translation of technical concepts. When more than one scenario could be suitable to deepen the understanding of one hazard, scenarios were selected on the basis of three different criteria:

- their relevance for the hazard under analysis;
- frequency and likelihood of occurrence;
- criticality (i.e. worst case situation).

It is almost impossible to predict a scenario development, thus controllers' reactions offer very relevant insights, that could not be gathered in other experimental settings. Moreover it is worth while emphasising that the Real Time Simulation environment allows the simulation and the analysis of worst case situations, that are fundamental for a risk assessment process.

According to the high relevance of control systems in the ATM domain, specific computer malfunctions could also be studied. Failure of the computer systems were first assessed through reliability analyses. Then, the credible control system failures were placed as hazards in realistic scenarios. As specified by ESARR4 [7] (see Section 3), main focus from the operational point of view should be placed on the effects of a technical malfunction on the system, as well as

Table 5
Story board and actions for two different scenarios

Hazard Identification Code: SA2		Airspace Sector: EW
Time		Events
9.48	Accomplice Pilot Action	AZA123 asks to descend to FL290 for technical reasons
9.50	If Accomplice Pilot Action	IBE3674 and AFR432 are cleared to self-separate while crossing
9.50	then Possible Event	AZA123 interfere with IBE3674 and AFR432 (self-separation on-going)
10.14	Accomplice Controller Action (on sector MN)	Set up self separation (remain in trail) btw AZA542 and DLH292.
10.20	If Controller Action	AFR674 and BWT212 are cleared to self-separate while crossing.
10.24	then Accomplice Pilot Action	DLH292 ask to cancel delegation for on-board technical failure

an assessment of the severity of those effects. In the Real Time Simulation environment this meant focusing on the effects on human operators, for instance gathering data on means of detection, ease of detection, fallback procedures availability and ease of recovery... In order to simulate control system breakdowns it was often necessary to recreate a specific situation both by modifying software parameters but also by instructing pilots or even some of the controllers to perform planned actions, whilst effects on other controllers and their reactions were then observed. In other words technical malfunctions were recreated by having some pilots (or controllers) act as if specific computer systems had failed. Table 5 presents two examples of actions to be performed by controllers or pilots to recreate specific scenarios.

This methodology enables to analyse how the system reacts to and accommodates to diminished performance of one of its components. Again it permits a systemic view, since the control system malfunctions could be observed in interaction with all the other involved elements, with no oversimplification or unrealistic isolation, thus satisfying the requirement for an integrated analysis of the tool-procedure integration. It also satisfies the ESARR4 [7] recommendation to study the combined effects of hazards, and not only their immediate consequences. Indeed the MFF procedures can bring major benefits to the system, but they also entail drastic innovations that need to be studied extensively with the proper tools.

7. Conclusions

The present paper intends to present the major open issues we faced in conducting the safety assessment of an experimental project. Some relevant characteristics of the ATM domain were taken into account, reflecting on strong

and weak points of current safety practices. To identify effective solutions, we tried to take advantage of a sound theoretical framework. Some proposals are thus explained at the light of abstract theoretical principles, in order to provide a broader scope to the MFF experience. If ad hoc (practical and local) solutions had been applied without a proper theoretical background behind, they would have probably provided a too narrow focus. As a consequence any generalisation or re-use would have been impossible, or at least highly constrained.

It should also be emphasized that the theories and methodologies proposed in the present paper are far from representing a fixed point for safety assessment activities. Rather they are discussed as currently available solutions that proved to some extent valid in a specific project. Furthermore, a major limitation is that large efforts and resources are required to conduct the integrated analysis described. Then, an increasing standardization pressure and a larger integration of computer systems will deeply affect and modify the characteristics of the ATM domain in the next future.

Acknowledgements

The MFF project is partially funded by the EU under the *TEN-T program*. We would like to thank all the colleagues of the MFF project and especially those of the WA7 and WA4 for the fruitful collaboration on the activity. In particular we would like to mention Petra Scrivani (Deep Blue-University of Siena) for scenarios preparation. Valentina Barsotti (Deep Blue) deserves a special thank for providing the graphical templates used to draw Figs. 3–5 and 8.

References

- [1] EUROCONTROL. ECAC Air traffic management strategy for the years 2000+, Brussels: 2000.
- [2] Bentley R, Hughes JA, Randall D, Rodden T, Sawyer P, Shapiro D, Sommerville I. Ethnographically-informed system design for air traffic control. In: Proceedings of the ACM conference on computer-supported cooperative work, Toronto (Canada); 1992, p. 123–9.
- [3] Hughes JA, Randall D, Shapiro D. Faltering from ethnography to design. In: Proceedings of the ACM conference on Computer-supported cooperative work, Toronto (Canada); 1992, p. 115–22.
- [4] Leveson NG. Safeware. System Safety and Computers. Reading, MA: Addison Wesley; 1995.
- [5] ICAO Accident Prevention Manual. doc 1984 9422 AN/923.
- [6] Edwards E. Man and machine: systems for safety. In: Proceedings of British airlines pilots association technical symposium. London; 1972, p. 21–36.
- [7] EUROCONTROL. Eurocontrol safety regulatory requirements (ESARR) 4. Risk assessment and mitigation in ATM, Brussels; 2001.
- [8] EUROCONTROL. ESARR2 Guidance to ATM safety regulators. severity classification scheme for safety occurrences in ATM, Brussels; 1999.
- [9] EUROCAE ED-78A/RTCA DO-264. Guidelines for approval of the provision and use of air traffic services supported by data communications.
- [10] SAE ARP 4754. Certification consideration for highly integrated or complex aircraft systems.
- [11] SAE ARP 4761. Guidelines and Methods for conducting the safety assessment process on civil airborne systems and equipment.
- [12] Mackay W. Is Paper Safer?. The role of paper flight strips in air traffic control. In: ACM transactions on human–computer interaction 1999; 6 (4): 311–40.
- [13] Norman DA. Things that make us smart. Reading, MA: Addison Wesley; 1993.
- [14] MAEVA. A Master ATM European Validation Plan. Validation guideline handbook; 2003.
- [15] Mediterranean Free Flight Safety Policy. Available on the MFF web site at <http://www.medff.it>.
- [16] Mediterranean Free Flight Safety Plan. Available on the MFF web site at <http://www.medff.it>.
- [17] Clarke L. Acceptable Risk? Making decisions in a toxic environment. Berkeley: University of California Press; 1989.
- [18] Slovic P, Fischhoff B, Lichtenstein S. Response mode, framing, and information-processing effects in risk assessment 1982. In: Bell DE, Raiffa H, Tversky A, editors. Decision making. descriptive, normative, and prescriptive interactions. Cambridge: Cambridge University Press; 1988.
- [19] Tversky A, Kahneman D. Judgment under uncertainty: heuristics and biases. Science 1974;185:1124–31.
- [20] Holland J. Hidden order: how adaptation builds complexity. Reading, MA: Addison Wesley; 1995.
- [21] Boegh J, De Panfilis S, Kitchenham B, Pasquini A. A method for software quality planning, control, and evaluation. IEEE Softw 1999; 16(2):69–77.
- [22] Leveson NG. Intent specifications: an approach to building human-centered specifications. IEEE Trans Softw Eng 2000;1(26):15–35.
- [23] Reason JT. The Human Error. Cambridge: Cambridge University Press; 1990.
- [24] Carroll JM, editor. Scenario-based design: envisioning work and technology in system development. New York: Wiley; 1995.