Eleventh USA/Europe Air Traffic Management Research and Development Seminar (ATM2015)

Identification of critical scenarios of risk: An operational approach

Karim Mehadhebi
Direction de la Technique et de l'Innovation (DTI)
Direction des Services de la Navigation Aérienne (DSNA)
Toulouse, France
karim.mehadhebi @aviation-civile.gouv.fr

***Abstract*—This paper introduces an innovative approach for identifying critical scenarios of risk, which are scenarios likely to cause an accident. This approach was designed in the course of an ambitious DSNA program called 4-Flight, with a massive operational change (switch to electronic stripping, new Flight Data Processing Server, DataLink, new HMI for air traffic controllers). The purpose of this innovative approach is to guarantee that, although emerging risk could appear when implementing the new system, all critical scenarios of risk have been identified and mitigated. We present the approach and provide applications both in SESAR and in one 4-Flight large scale experimentation.**

Safety, risk modelling, risk mapping, SESAR

I. INTRODUCTION

A. Context

A general trend in the Air Traffic Management (ATM) is the "speeding up" of operational changes due to a new generation of air traffic management systems. When performing the safety studies, Air Navigation Service Providers (ANSP) are faced with new challenges in the safety process, due to the fact that the risk induced by the change may induce innovative scenarios, which may remain undetected until the occurrence of incidents. An analysis of past spacecraft and aircraft accidents [9] reveals that the causes are often to be found in the complexity of the human and software interaction, and to an overconfidence of automation with regards to human. This raises questions on the identification of hazards, which should cover a wider range than the sole technical failures. Within NextGen, an innovative safety approach has been suggested, which a broader view on the propagation of errors, which shouldn't be limited to the propagation of failures, but also consider more complex patterns of component interactions [4].

B. The SESAR safety process

Similarly, within SESAR, the Air Traffic Management (ATM) is challenged by Operational Improvements (OI) based upon an enhanced distribution of information between the different actors. Behind the multiplicity of "possible improvements", we see the same scenario, repeated over and over: industrials design enhanced technologies, more reliant upon ground and airborne information, and ANSPs integrate these new technologies so as to optimize their operational benefit. This process is somehow different from the classical engineering system V-Model [16], since in the V-Model, we would expect the ANSP to firstly express its need, the industrial to design a technical solution meeting this need, and the ANSP to finally validate that the technical solution meets its need. Here, the technical solution is often already (at least partly) existing, so that it is up to the ANSP to "adapt" its operational need in order to make the best benefit of this new technology. In practice, this work is made by a joint ANSP and industrial collaboration, starting from an initial operational concept, which is validated through a trial and simulation process.

In order to address this new process, a new safety methodology has been designed within SESAR ([4]) in order to span the safety process all over the engineering system process. In other words, safety requirements are designed at the very beginning of the process (even before the start of the technical solution), in order to express what we want the system to do "nominally". This is a clear difference from the usual scope of safety, which, in the past, tended to focus only on the failures of the system. Within SESAR, these preliminary safety requirements are denoted as ***success requirements***, in order to differentiate them from the usual safety requirements addressing the system failures. The approach adopted for designing these preliminary success requirements is to consider where where the risk lies in the current environment, and to "guess" which scenarios of existing risk could be mitigated by the new system, when performing nominally. These mitigations are expressed by requirements of the form "*the new system should nominally, perform in such and such way...*". This approach relies upon a mapping of the existing risk ([6],[8]), which was designed before the SESAR program as the Integrated Risk Picture (IRP), and is now denoted within SESAR as the Accident Incident Model (AIM) [11].

The SESAR safety methodology is very appealing, from an ANSP viewpoint, since the global safety argument relies upon an ***actual*** reduction of the accidents and incidents, and not an expected one. This is because the success approach considers a mapping of the actual scenarios of risk, and aims at introducing new mitigations.

C. The EUROCAE approach

It is worth noting that, in the past, a less ambitious safety methodology [9] has been designed by the EURopean Organisation for Civil Aviation Equipment (EUROCAE), whose purpose is precisely to convert an Operational Services and Environment Description (OSED) into Safety and Performance Requirements (SPR). This methodology focuses on air traffic services supported by data communications, and aims at establishing performance requirements for the communication segment. SPR documents have been produced by EUROCAE for (among others) ADS-B and DataLink. SPR documents, however, are not sufficient for building a complete safety argument to demonstrate that tolerable safety levels are achieved, so the EUROCAE safety methodology has not been considered as an accepted mean of compliance with European Safety regulations [12].

In summary, the EUROCAE and the SESAR safety approach illustrate the difficulty to combine, in a global framework, both the operational and the industrial view on the safety. The SESAR approach is rather "operational oriented" and bases its safety argument upon operational benefits, with the difficulty to produce documents which would have the industrial maturity of the EUROCAE SPR. On the other hand, the EUROCAE approach is more generic, but it needs to be further refined by considering the operational use of the communication device.

D. Local ANSP approaches adressing critical scenarios of risk

Besides the EUROCAE and SESAR safety approach, some ANSPs have locally adopted safety practices in order to bridge the gap between operational and industrial requirements. These practices are often based upon an identification of the most critical parts of the system, in order to design mitigations which would reduce their criticality. This general principle, as we shall see, can be followed all along the design of the new system, and serves as a "compass" which indicates where the safety should focus in order to guarantee, in the end, operational benefits.

The idea that safety could support the engineering system in order to reduce the parts of "highest criticality" has inspired several safety approaches that we present in the first part of this paper. Then in the second part, we introduce an innovative approach for identifying critical scenarios of risk, both in the design of the new system and when testing the live system. This innovative approach has been developed by French *Direction des Services de la Navigation Aérienne* (DSNA), within an ambitious program called 4-Flight. This safety approach has been used both in 4-Flight and within SESAR, and we present two examples of its application, one in the design phase and one drawn from an experimentation.

II. SURVEY OF SAFETY APPROACHES ADDRESSING THE CRITICAL PARTS OF A SYSTEM

A. First approach: by Bayesian Networks

Intuitively speaking, an internal component is critical if its "probabilistic distance" from an accident (or an incident) is small. In other words, given that the component has failed, the system is "close to" an accident. The idea is to apply this concept all along the design of a new system, that is, to establish an ongoing estimation of the probability of accident/incident given the failures of internal components. This approach is followed by the German *Deutsche FlugSicherung* (DFS), which has developed a safety methodology based on the use of Bayesian Networks [14].

Bayesian Networks are used in order to express at a global level, the probabilistic relations between the occurrence of causes, hazards and effects. Rather than expressing separately the causes and effects of each individual hazard, with the classical bow-tie representation, all hazards are merged into a "global picture", schematically represented in Figure 1.This allows to model mechanism of "error propagation" transversal to several bow-ties (one cause being able to contribute to several hazards). During the hazard identification phase, the ***hazards layer*** (second layer in Figure 1) is filled, and for each hazard, the probability for this hazard to lead to an accident or an incident is empirically determined. Then, during the hazard mitigation phase, the ***causes layer*** is filled, and "probabilistic edges" are added into the Bayesian Network whenever a cause is likely to result in a hazard, with an associated probability.

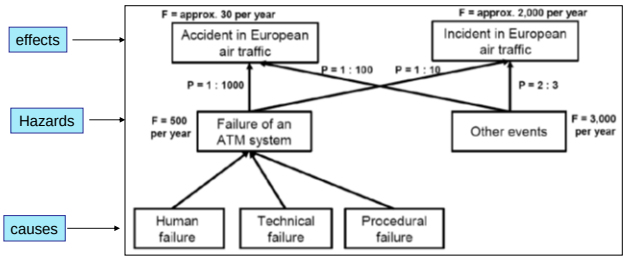

Figure 1.Simplified Example of a Bayesian Network from [14]

This Bayesian Network is updated all along the design of the system, by modifying edges whenever a new barrier is introduced. For each technical component, the conditional probabilities of accident and incident given a failure of this component, $\Pr(\text{accident} \mid \text{failure of the component})$, can be assessed thanks the Bayesian Network, and the purpose is to systematically address all components whose probability becomes too strong, and to introduce adequate mitigation. These mitigations can be either technical (redundancy with another equipment, alarm displayed, etc.), human or procedural.

B. Second approach:by dynamic stochastic tools

The Dutch *Nationaal Lucht- en Ruimtevaartlaboratorium* (NLR) has developed a safety methodology, based upon a toolset denoted as TOPAZ (Traffic Organization and Perturbation AnalyZer). TOPAZ provides another approach for estimating criticalities internal to a system, but within TOPAZ the probabilities are analytically determined, and not empirically estimated as in the previous Bayesian Networks case. The TOPAZ methodology relies upon an exhaustive modelling of all parts within the system, including the possible misunderstandings arising from the human exchanges (see [3]

for a modelling of the evolution of the Situational Awareness error). In principle, the TOPAZ method performs quantified risk assessment, but it is possible to assess the individual effect of each actor within the system by modifying its failure rate, and by assessing the impact on the overall risk.

An interesting illustration of how TOPAZ identifies critical parts within a system is given in [2], where TOPAZ has been used in the course of a safety assessment conducted at Schiphol Airport by the Dutch *LuchtVerkeersleiding NederLand* (LVNL). The details given below come from a direct conversation with Dr Blom, one of the authors of [2]. The safety study had to compare three possible operational development options involving different choices for runway and taxiway crossings, together with the efficiency of a runway incursion alert system called RIAS. The application of TOPAZ methodology showed that the RIAS alerting system tended to perform after the pilot had visually detected the intruder and taken appropriate action. For such cases, the ATCO still may perceive him/ herself to have played a key role in resolving the conflict well, so a safety assessment based only upon brainstorming with ATCOs would have given an incorrect vision of "how to mitigate this hazards". Actually, this hazard had been deemed acceptable by a classical HAZID method, whereas the TOPAZ analysis led to an opposite conclusion: this hazard was not acceptable because pilot intervention was strongly dependent upon visibility, which also depended upon weather. Due to poor weather conditions at Schiphol airport, it was then decided that the early pilot intervention could not be considered as an efficient barrier.

III. PRESENTATION OF AN OPERATIONAL APPROACH FOR ASSESSING CRITICAL SCENARIOS OF RISK

A. *History of this approach*

We now present an innovative approach for identifying critical scenarios of risk, for a new system. This approach has been developed within the DSNA 4-Flight program, and it has also been applied within SESAR. Through the 4-Flight program, DSNA modifies keys components of its technical infrastructure:

- A new flight data processor (COFLIGHT):
  - Compliant with the interoperability standards of SESAR**;**
  - Based on a volumic logic, with a distribution of flight plans according to predefined reasons (Responsibility, Vicinity, etc.)
  - Implementing trajectory prediction
- A new HMI (JHMI), with several ATC tools:
  - A server of alarms for a wide range of "undesirable events" (including non compliance of a flight from its profile, and tactical conflict),
  - A comprehensive set of rules for the static filtering allowing ATCOs to visualize only the traffic flows that they need to see;
  - Electronic negociation
- Electronic stripping

The magnitude of the operational changes within 4-Flight was such that the program had to adopt a process similar to SESAR, with iterative prototypes validated through experimentations. As a consequence, the innovative tools developed in 4-Flight were specified all along the sequence of consecutive validations, and the safety process had to adapt to this, by adopting an approach similar to the SESAR safety approach: express safety requirements at an operational level firstly, and refine these safety requirements at the pace of the system design.

In other words, the main challenge for safety was to express safety requirements for a system which was partly unknown, and for which the operational expertise was very scarce at the beginning. Furthermore (and similarly to the SESAR safety methodology), we wanted to base the overall safety argument on a reduction of the number of observed incidents, so we decided to develop an operational risk mapping similar to the one developed within SESAR, but more focused on the operational side, as we now explain.

B. *Description of our mapping of operational risk*

We now present our mapping for operational risk. Similarly to SESAR, this mapping relies upon a thorough analysis of past incidents, which has lead us to identify human mechanisms of human errors, together with operational scenarios for these mechanisms. The mechanisms of human error together with the corresponding operational scenarios of risk are described for each barrier of the Swiss Cheese model ([17]) of accident causation, also used by Eurocontrol IRP [6], that we reproduce below (in Figure 2).

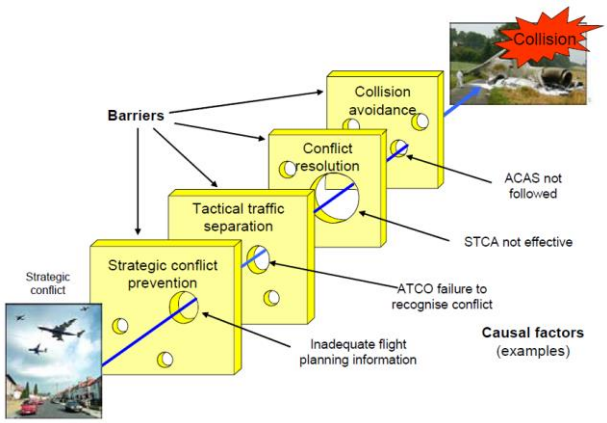

Figure 2. The Swiss cheese diagram of Mid-Air collisions from [6]

We have limited ourselves to the two first barriers in Figure 2 (strategic conflict prevention and tactical traffic separation), and we define ***critical scenarios*** as ***scenarios which infringe simultaneously the two first barriers***. We now describe, for these two barriers, how we have represented the human mechanisms of human error and the operational scenarios of risk.

1) *Description of operational risk for the strategic conflict prevention barrier*

This barrier represents the activity of the planner ATCO, which integrates incoming flights, identifies the conflicts, and

informs his executive ATCO of them. Our approach was elaborated through trials and failures, so we take advantage of this first case for explaining in detail, for this barrier, how we eventually converged toward a formalism that we applied for the other barrier. We were in search of a formalism which would be both exhaustive and "mutually exclusive". By brainstorming, we retained two generic mechanisms of human error:

-PLANNER_01: The planner ATCO has no awareness of a conflict with an incoming aircraft;

-PLANNER_02: The planner ATCO has identified a conflict with an incoming aircraft, but (for any reason) this conflict is still pending to be resolved by the next ATM barriers, without the controller being aware of it.

These two mechanisms are mutually exclusive, and each human error seen at the level of this barrier falls within any of these two mechanisms of human error: if PLANNER_1 does not hold, then the planner ATCO has correctly identified the conflict, and if PLANNER_2 does not hold, then the ATCO team has awareness that the conflict is pending (or the conflict has already been solved by the planner ATCO). We also notice that these two mechanisms of human error are generic and independent of the tools used by the controllers, which means that, although these mechanisms of human error have been observed in the current DSNA paper strip environment, they will still be valid in the future electronic stripping environment.

Each mechanism of human error is then further refined by a description of all scenarios of operational risk, where this human error is likely to occur. We now explain the formalism used for describing these scenarios, and for that we recall our final objective: assess the operational impact of the innovative tools on the system. In the light of this objective, we had the idea to assess this operational impact through a mapping between (on the one side) the scenarios of operational risk and (on the other side) the innovative tools. Schematically speaking, this mapping would look like the matrix illustrated on Figure 3, with the scenarios of operational risk in vertical and the innovative tools in horizontal.

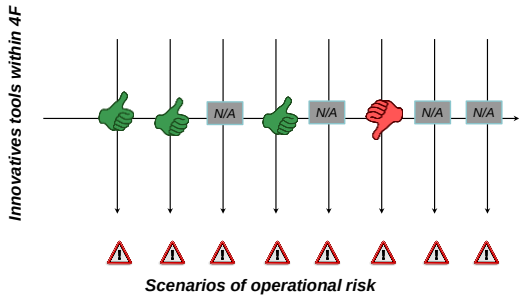

Figure 3. Schematic mapping between the innovative tools and the scenarios of operational risk

The logic of this mapping is to assess, for a given tool and a given scenario of operational risk:

1) Whether the tool is expected to reduce the occurrence of the scenario (by adding an additional mitigation);

2) Whether the tool is feared to increase the occurrence of the scenario (due to reasons to be explained);

3) Whether the tool is expected to have no impact on the scenario

These three modalities are respectively represented, on the diagram of Figure 3, by a green hand, a red hand, and a N/A. In order to do such a mapping, we had to express the operational scenarios of risk at a level of detail allowing to describe the operational context where each tool was used. So, we decided to express the scenarios of operational risk at the level of the operational situations that the air traffic controller had to manage (integration of a flight, negotiation with a neighboring sector, tactical solving of a conflict, etc.). As a consequence, the failures would correspond to human failures occurring during these operational situations.

In summary, we ended up with the following format for our scenarios of operational risk, represented in Figure 4. Similarly to the SESAR AIM, scenarios of operational risk are described with a fault tree representation. The difference from SESAR is that our description of failures encapsulates both ***operational situations*** (in yellow) and ***inadequate human actions*** (in grey), in the context of this operational situation.

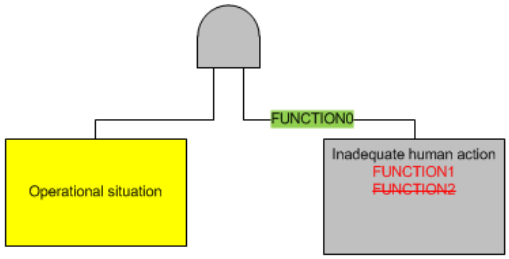

Figure 4. Final representation retained for our mapping

Then, for each inadequate action, we still express the impact of the innovative tools as "mitigating the risk" (FUNCTION0, in green) or "feared to increase the risk" (FUNCTION1, in red). We have added a third category, in red barred, which is "feared to increase the risk when improperly used". This corresponds to situations where the ATCO uses the new tool in an improper manner, different from the expected use. Figure 5 illustrates the complete set of operational scenarios, for the mechanism of human error PLANNER_1. We recall that this mechanism corresponds to a planner ATCO which does not detect a conflict involving an incoming flight. We denote by S the volume sector associated to the planner ATCO, and by S-1 a neighboring sector which sends to a flight to sector S.

For this mechanism, three different operational situations need to be distinguished. The first one corresponds to the situation where the two flights involved in the conflict come from the same S-1 sector. In that case, the human error is due to a misunderstanding of who has to solve the conflict, the

ATCOs of S-1 believing that it was agreed that the next sector S would solve the conflict, whereas the planner ATCO of sector R believing that the S-1 sector would solve the conflict. In that case, the human error is linked to the negotiation of the incoming flight between sectors S-1 and S. In the second operational situation, the two conflicting flights come from two different sectors, and here the human error is mostly due to failure of the planner ATCO to detect a conflict. Finally, in the third operational situation the conflict occurs between one incoming flight and one flight already into sector S , so that the human error has to account for misunderstanding between the planner and the executive ATCOs of sector S, for instance the planner issuing a strategy which is made inefficient by the fact that the executive has modified the profile of the incoming flight, without informing his planner.

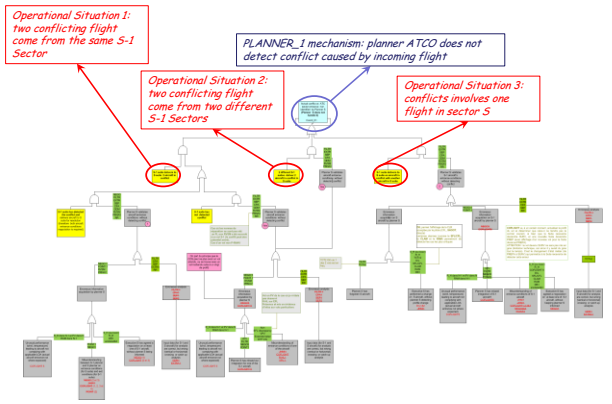

Figure 5. Fault tree of operational scenarios for the mechanism PLANNER_1

In summary, we see that our modelling of operational risk is not quantified, but more in the line of the two-dimensional mapping illustrated in Figure 3 (innovative tools on one axis, scenarios of operational risk on the other side). We also insist on the fact that this mapping was developed all along the design phase of 4-Flight. More precisely, the "red barred" functions were added within the fault tree during the prototyping sessions, when the operational experts were designing the future tools for the ATCOs. It is during these sessions that we questioned ourselves about "how improperly" these tools could be used, and we have taken advantage of the fault tree representation for keeping a memory of all these improper uses. By doing this work, we have provided a structure to the safe design of training and working methods: ATCOs had to be trained so as to be clearly informed of the improper uses of every functions, and working methods had to be designed accordingly.

In essence, our approach is similar to the DFS approach presented in paragraph II.A, in the sense that both approach rely on an "ongoing" mapping of risk, which is refined all along the design of the new system. The difference lies in the nature of the tool, the DFS favoring a probabilistic tool (based upon Bayesian Network), whereas we favor an operational and non-quantified tool. For information, we also point out the difference between our approach and the SESAR approach. Within SESAR, the analysis of past incidents is processed in order to produce a ***quantified*** fault tree, with different probabilistic values computed at each node [7]: frequency of occurrence of the node (blue square), efficiency of the barrier (red square), relative frequency (yellow square). Our approach also relies upon a fault tree representation, but we have discarded the quantification of the risk, for a more refined representation of the scenarios, including the operational situations.

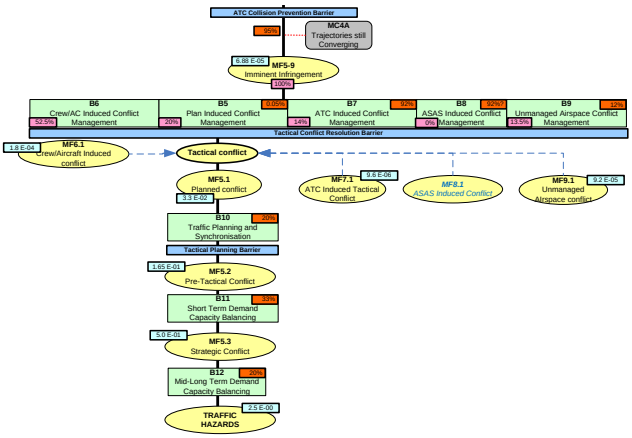

Figure 6: the en-route AIM model from [7]

We now succinctly present the mapping of operational risk for the next ATM barrier, without entering into the same level of detail.

2) Description of operational risk for the tactical traffic separation barrier

We address here situations of risk where the failure is specific to that barrier. The scenarios of risk described in that barrier implicitly assume that the previous strategic barrier has correctly operated, so as to satisfy our "mutually exclusive" representation of risk. We also distinguish, here, two categories of conflict: actual conflicts, which correspond to set of flights in the course of passing below separation, and potential conflicts, which is a set of aircraft in the course of passing close, but not necessarily below separation. Schematically, ATCOs have to solve actual conflicts (by issuing adequate clearances), and to "keep an eye" on potential conflicts. For that ATM barrier, we have identified two mechanisms of human error:

-TACTICAL_1: the executive ATCO is not aware that two flights are in actual conflict.

-TACTICAL_2: a potential conflict is transformed into an actual conflict, without the two ATCOs to notice it.

Here also, the two mechanisms are mutually exclusive and exhaustive. We now introduce a general "trick" that we have used repeatedly in order to find out the different kinds of human error. We recall that our description of a human error is at the level of an operational situation, where the ATCO is expected to execute a specific action (integrate a flight, negotiate with a neighboring ATCO, solve a conflict, etc.). In order to find out reasons which could cause an

inadequate action, we have always searched in two directions:

1) We have identified, for that action, what information the ATCO used in order to perform the action, and we have considered whether the controller could have an improper knowledge of these information.

2) We have considered errors when executing the action.

For all ATCO actions, whenever we searched for "possible inadequate actions", we found that the subdivision between subcases 1) and 2) was a practical way of guiding our thoughts in the good direction. For instance, if the action is "solving a conflict", the information required for that action are both in vertical (actual, cleared and exit flight levels) and horizontal (flight plan route, potentially modified in case of direct). Examples of Errors falling in bucket 1) would include wrong knowledge of one of these information, possibly caused by a misunderstanding between the two ATCOs, or by an improper use of one of the innovative tools. Example of errors falling in bucket 2) would typically be phraseology or callsign error, or error on the diagnosis of conflict (due to a non expert ATCO, for instance).

For the mechanism TACTICAL_1, we have identified errors both at the flight integration (the executive ATCO making his own integration of incoming flights) and at the conflict solving, and for these two subtasks we have considered the two previous subcases 1) and 2). Typically, for the integration, subcase 1) corresponds to situations where the executive ATCO has an improper representation of the profile of the flight, either due to a misunderstanding with his planner, or due to atypical circumstances (flight with an exceptionally low or high climbing rate, for instance). For TACTICAL_2, we have identified two possible operational scenarios:

1) If the two flights are already assumed, the planner ATCO fails to inform its executive of the potential conflict, and the executive ATCO modifies the profile of one of the two flights without detecting that this modification creates an actual conflict.

2) For a flight already assumed and an incoming flight still assumed by the previous sector, the planner ATCO negotiates with the previous sector the parameters of the entering flight, whereas the executive ATCO modifies the profile of the flight already assumed. These two actions "contradict each other" in such a way that an induced conflict is created.

Here also, these two scenarios are further refined by considering ***errors on the information*** and ***errors at the execution***. Errors on the information allow, in practice, to model a large number of mechanisms for error propagation (misunderstanding between the two ATCOs, improper use of a tool, undetected corruption, etc.).

C. Application of our appraoch to SESAR

As illustrated in Figure 3, our mapping of operational risk encapsulates both the scenarios of risk, and the impact of the innovative tools on these scenarios (green for positive impact, red for negative impact). From that mapping, it becomes possible to identify ***critical failures*** as ***failures which impact both the strategic and the tactical barrier***. This approach has been applied both in the safety study of the 4Flight program, and within SESAR. We present in the next subsection how this approach has been applied within SESAR.

1) Presentation of SESAR OFA 03.01.01

DSNA is involved into the safety activities of SESAR Operational Focus Area (OFA) 03.01.01, denoted as "Trajectory Management Framework and System Interoperability with air and ground data sharing". This OFA includes all Work Packages and activities dealing with the exchange of air and ground data, for the purpose of trajectory management. Within this OFA, the Flight Object (FO) paradigm plays an important part for implementing in practice the trajectory management of flights, and we introduce it succinctly.

The concept of FO stems from EUROCAE ED133 [12], this document defines the interface between different instances of civilian ATC Flight Data Processing Systems (FDPS), in support of En-route and Terminal ATC Operations. This interface has been defined to ensure a consistent view of the flight data across all FDPSs. The 'Flight Object' (FO) is a concept to support the sharing of consistent flight data between all stakeholders. The key objective of the FO is to ensure a consistent view of the flight data across all systems, and at the heart of that flight data is the description of the expected flight path of the flight, commonly referred to as the flight's trajectory.

Within ED133 the level of detail of the technical architecture is shown in Figure 7.The logic of exchange between Air Traffic Services (ATS) is defined in terms of volumes, each ATS being in charge of an Area of Responsibility (AOR). Each Flight Data Processing Server (FDPS) contains a Flight Object Server (FOS), where "copies" of the FO are stored. A FO can be sent in advance to the FOS of several ATS, for instance if the flight is expected to visit the corresponding AORs in the future, or if the flight is (or will be) in vicinity of these AORs. ED133 defines several reasons for distributing a FO, and several roles for modifying the FO, several FDPS being able to ask (at the same time) for modifications on the same FO. All these modifications are processed within the FDPS which has the responsibility of the flight (which is the sector where the flight is assumed). In summary, the FO concept is very flexible, and allows a wide range of use, such as the "smoothing" of the planning workload (a planner ATCO being able to ask modification on an incoming flight long before the arrival of the flight).

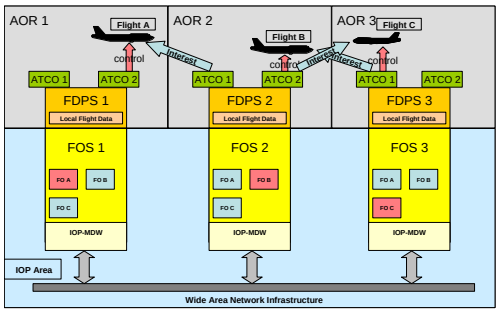

Figure 7. Technical architecture of ATC to ATC interoperability, from [9]

ED133 defines ***roles*** (publisher, contributor, user) associated to the different FDPS, together with ***features***, which are the actions defined for each role.

2) Safety analysis of OFA03.01.01

In addition, ED133 comprises a safety analysis, where hazards have been defined at the level of the Flight Object features, and a severity has been allocated for all hazards. The safety study done within SESAR OFA 03.01.01 was faced with the following challenge: verify whether the severities defined within ED133 were stringent enough for allowing all operational needs defined within SESAR, or if some operational needs would reveal "more severe" hazards.

We now illustrate, on one example, how our approach was carried out. Operational needs within SESAR were mostly defined in terms of Use Cases, one example of them being:

Revised Coordination Flight Level: *ATS unit (upstream) X revises the coordination flight level electronically whilst A/C in airspace X under standard coordination – after the automatic coordination event has occurred. ATS unit (downstream) Y receives update electronically and track label is updated and displayed accordingly.*

From our mapping of operational risk, the identification of critical scenarios was pretty straight forward, it sufficed to see where the flight data processor intervened at a "green function" (see Figure 4), and to look for common mode failures. We quickly identified the following common mode:

1) The planner ATCO bases its diagnosis of conflict upon Entry Flight Level, so he misses a conflict
2) The executive ATCO has applied filtering based on Entering Flight Level, so the flight is not displayed on his screen

If the Entry Flight Level was to be corrupted, operational effects 1) and 2) could occur simultaneously, causing the conflict not to be solved by the ATCO team. For such an undesirable even, the "last minute" conflict resolution ATM barrier of Figure 2 was assumed to be operant (STCA), so the severity was assessed to 3 (according to SESAR convention). When analyzing the causes at the Feature level of ED133, we identified that a failure in the distribution of the FO could cause such an undesirable event, since in that case, the revised FO would not be sent to the downstream ATS Unit, and the Entry Flight Level (EFL) could still be incorrectly displayed in the track label. Pushing the analysis one step forward, we discovered that errors at the level of trajectory prediction could cause errors in the reason of distribution, for instance if the trajectory prediction had an incorrect representation of the future sectors to be visited by the flight. However, within ED133, errors at the level of trajectory prediction had only a severity 4.

In conclusion, we discovered that a severity 4 technical error (trajectory prediction error) could directly cause a scenario of risk of severity 3, so the severity 4 allocation was not stringent enough for the operational use corresponding to the previous Use Case. More generally, by identifying such critical scenarios of risk, we were able to detect where the ED133 safety part had not been stringent enough, for operational needs defined within SESAR.

IV. IDENTIFICATION OF CRITICAL SCENARIOS OF RISK FOR REAL TRAFFIC

The approach presented in the previous section applies to the design phase of a new system, which is not yet implemented. We recall that this approach relies upon an understanding of operational risk based on past incidents, so there is a possibility that the new system reveals genuine scenarios of risk, which were unknown before. In this section, we present an extension of the previous approach, for the identification of critical scenarios of risk based on real traffic data. The purpose, here, is to survey a period of traffic in order to find out scenarios of risk, and to analyze them.

A. Software tools used

The tools that we use for the processing of traffic data from real time simulations are the two toolkits IJAMAN and BISCOT. The IJAMAN toolkit takes as input several data files (aircraft trajectories, flight plans, ATC recorded instructions), its purpose is to extract maneuvers and to interpret them (according to the flight plan and to the ATC recorded instructions). IJAMAN produces, as a main output data file, a file containing the aircraft trajectories, in a "vector state" format. The vector state is ATC oriented, in the sense that it captures the operational representation (at a given time) that a controller would have of the aircraft. This operational representation comprises both the operational constraints associated to the flight (its planned route, its exit flight level, etc.) and the status of the flight with regards to these constraints (whether the flight diverges form its planned route or it recovers it, whether the flight has reached its exit flight level or is in the course of reaching it, or has been leveled off at some intermediate flight level).

BISCOT (human Based rIsk and deciSion taking Complexity integrated tOolkiT) [1] is the main toolkit for analyzing data from real time traffic or simulations. This toolkit analyzes decisions taken by controller in order to infer an operational risk. The analysis also allows to gain insight on the ATCO cognitive workload (how many "virtual conflicts" the ATCO considers, at which time anticipation it starts processing them, and so on).

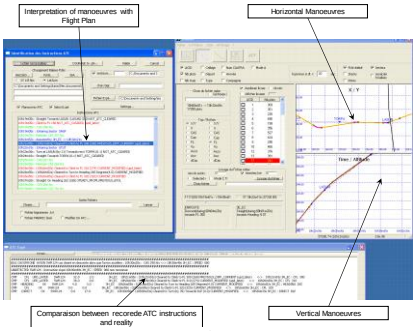

Figure 8. Illustration of the IJAMAN toolkit

The general principle of BISCOT is to extrapolate aircraft trajectories at a given time, for a given logic. Applying this technique, BISCOT extracts encounters, which are pairs of aircraft with an associated scenario of "what if". A possible application is to "erase" an ATC instruction, in order to extrapolate "what could have happened if ATC had not issued that instruction".

Figure 9 illustrates an encounter associated to a heading instruction ("*heading 190*°"). Green and blue trajectories are the real ones, and the red trajectory illustrates the green aircraft trajectory once the heading instruction has been erased (the "what if" scenario). Encounters reveal many operational patterns associated to an ATC instruction, such as:

- The ATC anticipation (how early the controller has issued the instruction)
- The efficiency of the clearance (was the pair actually in the course of passing below separation?)
- The level of complexity of the decision (for the same pair of flight, did the controller issue only one conflict solving instruction, or did it combine several instructions in a general strategy?)

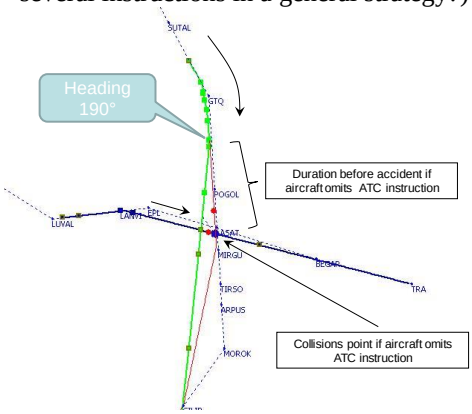

Figure 9. A "what if" scenario for an encounter together with its operational interpretation

In summary, the analysis of encounters allows to explain the global strategies that ATCOs implement when solving conflicts. Detailed examination of these strategies can provide insight on new scenarios of risk, which would not have been understood without the help of BISCOT.

B. Use of BISCOT for identifying scenarios of risk

1) The ACROPOLE experimentation

In March and April 2009 a large-scale experimentation took place in Toulouse in order to evaluate the ability of ATCOs to switch to an electronic environment. At that time (and still currently), ATCOs used paper strips, so the planning of the experimentation consisted of two days of initial training on the electronic environment (EUROCAT) followed by three days of experimentation with two operational scenarios: Orly and Roissy Charles de Gaulle. These two scenarios focused on the transition between en-route and TMA.

2) Risk observed in the ACROPOLE experimentation

During the experimentation, no real safety activity was performed, since the experimentation applied to a completely innovative operational concept, where unexpected events were likely to occur due to both a lack of ATCO training, and an incomplete customization of EUROCAT with regards to the operational environment. Some ATCOs expressed their concern, saying for instance that they had lost their situation awareness. This raised the following question: was their concern motivated by actual failures (for instance in conflict solving), or, despite their negative feeling, did they demonstrate sufficient ability to perform their work? It is in that context that BISCOT was used. An exhaustive survey of all operational errors was done, and this analysis revealed that the most significant errors lied in improper inputs of clearances. More precisely, these errors had the following causes:

1) ATCO forgets to input a clearance
2) ATCO inputs a clearance, but makes up his mind and issues (by voice) a different clearance to the pilot, without correcting the initial clearance
3) ATCO makes an error when inputting a clearance (incorrect value of one parameter, for instance Flight Level, or heading)

The rate of errors for 2) and 3) was pretty low (less than 1%), but the rate of forgetting (for 1)) was up to 10% for horizontal clearances. This first level of analysis revealed that, even if the new system was designed in order to issue alarms for such cases, there was a risk that, at the beginning, ATCOs would "get used" to the alarms and might not pay sufficient attention to them. Finally, one critical scenario of error when inputting an incorrect clearance was identified, namely the ***FL undershoot***. In this scenario, the ATCO would clear (by voice) a climbing aircraft at a given FL (say FL320), but would input (in the system) a smaller value of FL (say FL280). Under this scenario, the system would not detect a conflict between the climbing aircraft and an aircraft steady at FL300, and would not issue any alarm. The system would only "discover" the conflict once the climbing aircraft would overshoot the FL280, which might be too late for efficient ATCO intervention. This scenario pointed out the necessity to base alarms upon the Selected Flight Level (FL selected by the

pilot) rather than the Cleared Flight Level, which is done in 4-Flight.

3) Specific analysis of one critical scenario of risk

The clearance errors did not cause any significant operational incident (such as a loss of separation), they provided insight on "how improperly" the ATCOs were expected to use a new system based on electronic stripping. However, for one experimentation exercise, several losses of separation were observed during the exercise, and the reasons were not immediately apparent.

In that case, BISCOT was used in order to "shed some light" on the underlying reasons, and the subsequent analysis performed with BISCOT revealed a "hidden cause", namely an incorrect tuning of the Arrival MANager (AMAN), that we present in the sequel of this subsection.

Figure 10 shows, for this exercise, the traffic assumed by the executive Controller Working Position (CWP), where the displayed trajectories go from the "assume" to the "transfer". We have also represented the operational constraints for the CWP, namely two letters of agreement at the two exit beacons BALOD and ODRAN. On that exercise, 40 aircraft have been assumed by the CWP, 26 being sent BALOD, 12 to ODRAN, and 2 transverse flights. The analysis of conflicts performed with BISCOT revealed that most conflicting pairs of aircraft were due to a pre-sequencing performed by the EXEcutive controller (EXE). However, this pre-sequencing was often complicated by the transverse flights.

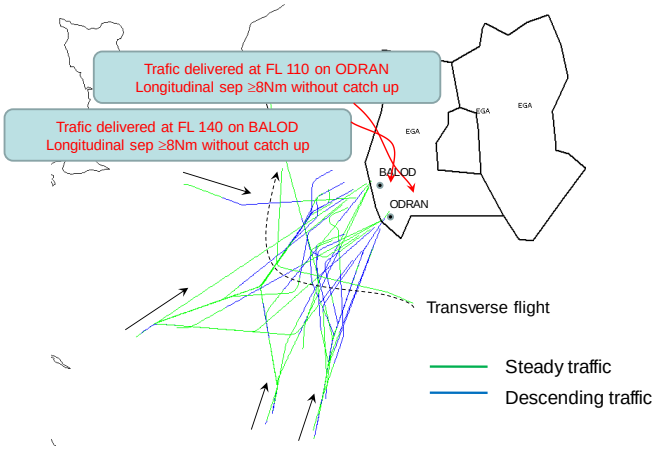

Figure 10. Configuration of the traffic flows for the simulation

When paying closer attention to the EXE strategies, we discovered that these strategies could lack optimality. Optimal strategies corresponded to situations where the EXE had succeeded in solving, in a minimal number of instructions, several problems, by splitting them into simpler sub-problems. Figure 11 provides an illustration of such an optimal strategy. The left diagram on Figure 11 shows the initial situation; Aircraft 1, 2 and 3 are to be delivered at ODRAN, but aircraft 3 has a higher speed than aircraft 1 and 2, an in addition aircraft 3 is in conflict with transverse aircraft 4. The strategy of the controller consists in lengthening the trajectory of a3 so that despite its higher speed it does not catch up a1 and a2, and this lengthening also solves the conflict with a4. The diagram to the right on Figure 11 shows the final situation: a2 was put in direct towards ODRAN once a1 was well ahead, and the lengthening of a3's trajectory solved the conflict.

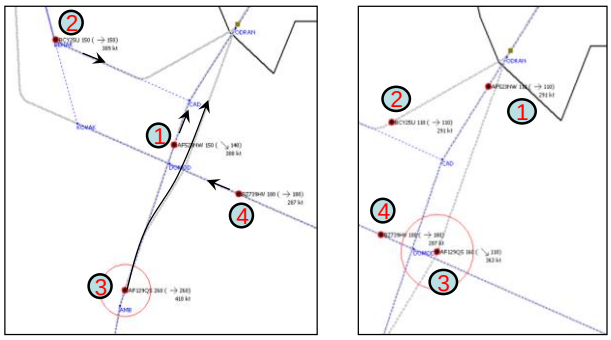

Figure 11.Illustration of an efficient strategy

However, the analysis of strategies also revealed "last minutes" strategies, where the EXE was overwhelmed by several issues that he had to solve in urgency. These strategies appeared to be caused by the fact that the aircraft exhibited different speeds, and the sequencing had been badly prepared by the AMAN.

Such an example is illustrated in Figure 12, for a sequence of seven aircraft being sent to ODRAN, where the three first one have been sequenced, but a4 and a5 are slower than a6 and a7, which causes the air traffic controller to issue a complex trajectory lengthening for a6 and a7, so that they do not catch up a4 and a5.

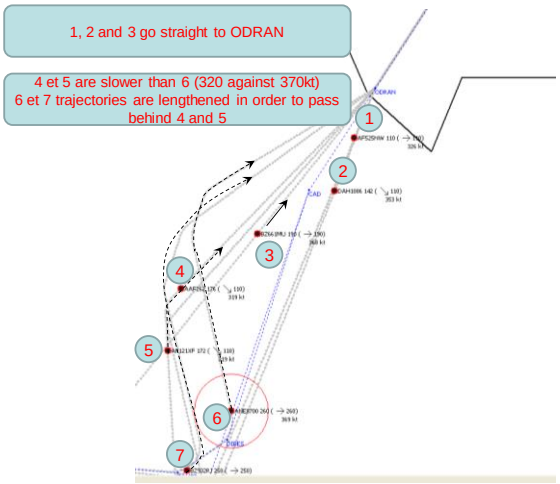

Figure 12. Illustration of a "last minute" (degraded) strategy

Finally, when tackling such "last minutes strategies", the ATCO had to create additional conflicts, as illustrated in Figure 13, where aircraft a7 had to pass before a8 in the sequencing. Such strategies are very costly in terms of cognitive resources, since the ATCO has to manage additional conflicts. Faced with this extra work, the executive ATCO

missed some conflict, and the planner ATCO had no tool for informing him that some conflicts were still pending.

In summary, the analysis made with BISCOT revealed the following propagation of events which eventually led to the infringement of both the strategic and the tactical ATM barriers:

- Traffic was not properly sequenced, and slow aircraft were sequenced with fast aircraft, creating additional sequencing workload.
- As a consequence, the Executive ATCO was often heavily busy on sequencing issues (such as Figure 12)
- Paper strip plays an important part in the common representation of "pending tasks" between executive and planner controllers. Thus the absence of paper strip played a part in the fact that the planner controller did not intervene.

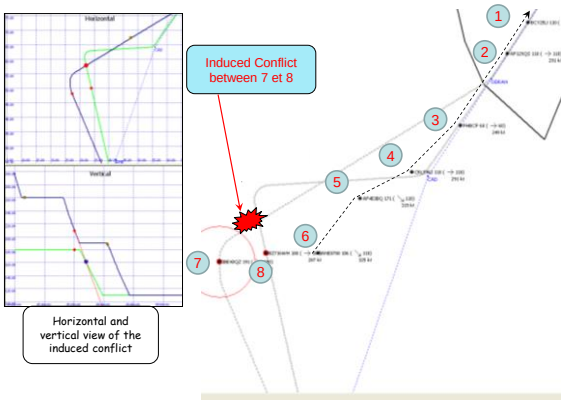

Figure 13. Induced conflict due to last minute strategy

Having determined this propagation of effects, it became possible to suggest safety recommendations or changes, either on the technique (sequencer issue), on the training and working method (for improving ATC collaboration), or on the procedural.

V. CONCLUSION

The analysis of past accidents reveals new patterns of error propagation [9]. Several analytical approaches have been designed in order to model error propagations (Bayesian Networks[14], TOPAZ[2][3]). The approach presented here is more operational, propagation of error being at a cognitive level (error either during analysis or execution of the task).
These approaches requires to model "patterns of propagation", with a risk of omitting (or improperly assessing the frequency of) a given mechanism of propagation. For an innovative system, we found that this approach needed to be completed by a survey on live traffic, the crucial point being the analysis of the global strategies implemented by ATCOs. The analysis of such strategies is very informative, particularly for limited traffic samples. Analysis of experimentations shows that few hours of sample traffic suffice to detect whether the strategies are still adapted to the new environment or not.

AUTHOR BIOGRAPHY

Karim Mehadhebi graduated from Ecole Polytechnique (France). He holds a MSc in Artificial Intelligence from Université Paul Sabatier (Toulouse) and a MSc in Computer Science from Mc Gill University (Montreal).
He has worked within the R&D department of DSNA from 1994 till 2008, in fields involving both mathematical and algorithmic expertise (radar trajectory smoothing, radar bias tuning, risk assessment). He got involved in the ICAO Review of General Concept of Separation Panel (RGCSP) and in its successor the Separation and Airspace Safety Panel (SASP). He is the author of ICAO circular 319 which presents a general framework for designing collision risk models for airspace planning, and has attempted to apply this approach to French continental airspace. In support to this work, he has designed the two toolkits IJAMAN and BISCOT, which allow involving air traffic controller and safety experts in order to analyze real traffic together with real time simulation for safety and human factor purposes. He joined the DSNA DTI (Direction of Technique and Innovation) in 2008, where he is in charge of managing the safety case for the 4-Flight project.

REFERENCES

[1] P. Averty, K. Mehadhebi and J.L. Pirat, "Evaluation of ATC working practice from a safety and human factor perspective", Eighth USA/Europe Seminar on ATM R&D, June 29 - July 2, 2009

[2] H. A.P. Blom, J. J. Scholte, J.C. van den Bos, R. Jansen, "Management of ATM performance in operational concept development and validation: a case study", Eighth USA/Europe Seminar on ATM R&D, June 29 - July 2, 2009

[3] H. A.P. Blom, S. Stroeve and M. van der Park, "Multi-Agent Situation Awareness Error Evolution in Accident Risk Modelling", Fifth USA/Europe Seminar on ATM R&D, June, 2003

[4] C. Fleming, N. Leveson and M. Placke, "Assuring Safety of NextGen Procedures", Tenth USA/Europe Seminar on ATM R&D, June 10-13, 2013

[5] D. Fowler, E. Perrin and R. Pierce, "2020 Foresight A systems-engineering approach to assessing the safety of the SESAR Operational Concept", Eighth USA/Europe Seminar on ATM R&D, June 29 - July 2, 2009

[6] Eurocontrol Experimental Center, "Main Report for the 2005/ 2012 Integrated Risk Picture For Air Traffic Management In Europe", EEC Note No. 05/06, April 2006.

[7] A.Kilner, "Validation / Verification of the SESAR Accident Incident Model (AIM)", SESAR WP 16.1.1, V00.01.00, April 2014

[8] E. Perrin, "A Systemic Model of ATM Safety: The Integrated Risk Picture", Seventh USA/Europe Seminar on ATM R&D, July 02-05, 2007

[9] N. Leveson, "The Role of Software in Recent Aerospace Accidents", Huntsville AL, USA

[10] EUROCAE ED78/A, "Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications", December 2000

[11] Eurocontrol Note, "Safety & Human Performance", available at http://www.eurocontrol.int/sites/default/files/publication/files/safety-human-performance-guide.pdf

[12] EUROCAE ED133, "FLIGHT OBJECT INTEROPERABILITY SPECIFICATION", June 2009

[13] Safety Regulation Commission Document 20, "Assessment of EUROCAE Ed78A as a means of Compliance with ESARR4", December 2002

[14] DFS, "Handbuch der Sicherheitsbewertungen", Version 2.02, November 2008

[15] "Security, Safety, Efficiency and CBA Assessment Env. Baseline 2007", Deliverable 4.4.1 of ERASMUS project

[16] National Computing Centre, Starts purchasers handbook, Procuring software based systems, NCC Publications, Oxford Road, Manchester, second edition, 1989

[17] J. Reason, "Human Error", Cambridge University Press, 1990