A PROGNOSTIC METHOD TO IDENTIFY HAZARDS FOR FUTURE AVIATION CONCEPTS

Brian E. Smith*, Hans H. de Jong, Mariken H.C. Everdij*****
NASA Ames Research Center,
****DFS Deutsche Flugsicherung GmbH***
*****NLR Air Transport Safety Institute***

Keywords: *prognostic hazard identification method, unimaginable hazards, FAST*

Abstract

Safety professionals are constantly in the process of assessing the safety risk of new aviation systems and supporting the identification of mitigating measures, which may be necessary to reach appropriate future safety targets. Diagnostic tools and methods are under development to monitor the overall health of the aviation system as it adapts to both planned and unplanned disruptive technologies and operational models that may be driven by market forces. However, prognostic safety analyses are required to anticipate the safety impacts of changes internal and external to the aviation system that are beyond the near-term planning horizon. Industry and government leaders have both an ethical and engineering responsibility to safely manage changes out in the future. This paper presents an integrated approach to prognostic hazard identification employing structured brainstorming to identify functionally imaginable and unimaginable hazards and systematic identification of hazards due to predicted changes that will impact aviation in the distant future. This method will generate a set of safety hazards that can serve as input to traditional safety analysis. This method has been co-developed by NLR, DFS, and the ECAST/ESSI Future Aviation Safety Team (FAST).

1 Introduction

Traditional approaches to hazard identification generate a set of hazards within the scope of the domain of the particular concept of operation or technology system of interest. These approaches are well developed and yield a robust set of hazards usable for conceived design purposes. However, they typically do not identify hazards associated with human operators of digital, electro-mechanical, and process systems used in new and novel ways, beyond the level of human error. Since this could lead to a gross underestimation of the risk associated with such new operations, there is a need to include hazards that are not easily conceived and imagined using traditional approaches. This paper presents a hybrid method for identifying additional hazards using structured brainstorming by domain experts coupled with a systematic assessment of the contextual factors present either within or external to the future operational setting. This hybrid approach combines the best features of free-form brainstorming by subject-matter experts (SME) and a multi-disciplinary approach to hazard identification across eleven functional domains relevant to aviation.

The organization of this paper is as follows: Section 2 outlines the traditional approaches to hazard identification. Section 3 describes a pure brainstorming approach to hazard identification. Section 4 gives a general introduction to the FAST method, restricted to the hazard identification part. Section 5 explains why and how the FAST method enriches the brainstorming approach to hazard identification by systematic consideration of future developments. Section 6 provides conclusions.

2 Traditional Approaches To Hazard Identification

The first generation of hazard identification is the functional approach, well known from system engineering and for example employed in the Guidelines for approval of the provision and use of air traffic services supported by data

communications [5]. In this approach, first the service characteristics, functions and procedures of air traffic services are determined. Next, hazards are identified considering:

- Loss or unavailability of information;
- Misleading information; and
- Whether or not hazards involving lost, unavailable or misleading information are detected.

Although this establishes a systematic approach to identify hazards from a functional failure point of view, not all hazards are identified in this way:

- There may be hazards associated with systems functioning as designed. Controllers might become overly reliant on a well-functioning alerting system. One could consider these phenomena as causes for failing to separate aircraft, but it is unlikely to imagine such hazards when starting from failures;
  There may be hazards not or only remotely associated with failures of services. Situational awareness differences could in hindsight be represented as such failures but they are so rich in their possible appearances that they are very hard to identify exhaustively in that way; and
- There may be implicit functions relevant for safety only recognized after failure. Analyses performed for runway crossing operations e.g. indicate the importance to protect the runway against "lost" pilots who do not even have the intention to cross, see [1] and [4]. Indeed, a complete functional description may be excessively complex.

Hazards that are not identified by means of the functional approach are referred to as "functionally unimaginable" or, briefly, unimaginable hazards. Fig. 1 contrasts the domain of functional hazards with universe of all possible hazards.

The second generation hazard identification method "HAZOP" (Hazard and Operability study, see for instance [10]) identifies and analyzes hazards with operational experts. HAZOP involves brainstorming along keywords, and an advantage above the functional approach is that it creates space for the identification of functionally unimaginable hazards. In addition to hazard identification, HAZOP sessions are also used to assess safety risks and to identify potential solutions for hazards. Unfortunately, as will be pointed out, assessment and solution activities themselves disturb the identification process, such that some hazards are left unidentified. Another complication is that, potential solutions may introduce new hazards.

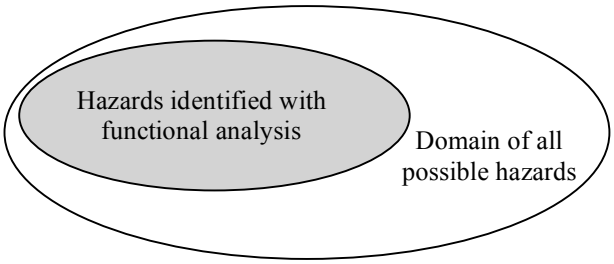

Fig. 1. Subset of Functional Hazards within Set of All Possible Hazards for a Certain Operation

3 A brainstorming method to identify unimaginable hazards

This section elaborates a third generation hazard identification approach involving pure brainstorming with operational experts (air traffic controllers and pilots). Guidelines for this approach have been developed at NLR on the basis of a large number of safety risk analyses of air traffic operations, have been published in [2]-[4], and have been incorporated in [6].

3.1 What is a hazard?

Instead of services, functions and failures, the starting point of the hazard identification is the safety of the operation: a hazard is anything that might negatively influence the operation's safety. In other words, the notion of hazard is defined in relation to safety, which makes it a much more general notion than failures or

"something going wrong", which are rather related to reliability. At this stage in the safety risk analysis, the risk and the underlying severities and frequencies associated with a hazard do not play a role yet.

3.2 Basic rules of hazard identification brainstorming

Identifying as many hazards as possible is a prerequisite for a safety risk analysis: hazards left unidentified are not analyzed and lead to an overly optimistic perspective on the risk of the operation considered. From a more general brainstorming context, the basic brainstorming rule "quantity breeds quality" is known [11]. Therefore, the goal of the hazard identification step is to obtain as many hazards applicable to the operation as possible. A productive brainstorm is not an indication of an unsafe operation: the safety risk of the hazards is still to be analyzed. Moreover, if there are hazards pointing towards flaws in the operation, it is better to know them early than late. The second basic rule of brainstorming is that criticism and analysis are forbidden during the sessions. This rule is also motivated from cognitive science [11]. Criticism easily kills the open atmosphere necessary for productive brainstorming. Identified hazards that seem unimportant to somebody must not be filtered out in the hazard identification; safety risk is to be assessed in a later stage of the analysis cycle. All time should be used for generating hazards. It is known from experience that analysis is time-consuming – analyzing a single hazard may well take much more than a session – and should be performed by safety risk analysts.

3.3 Participants of a hazard identification brainstorm

A suitable group of participants for a hazard identification brainstorming session consists of:

- Operational experts (a controller and a pilot);
- A moderator;
- Somebody taking notes;
- A safety analyst (preferably coinciding with the moderator); and
- If the developed operation is complex, an expert on the operation (preferably coinciding with the person taking notes).

Guidelines for selecting a controller and pilot for the brainstorms are:

- The operational experts have NOT otherwise been involved in the development of the operation;
- The operational experts must be able and willing to play devil's advocates;
- The kind of controller (area, approach, tower or ground control) should match the operational scope of the brainstorm;
- Vary with the kind of pilots (heavy, medium, light; scheduled, charter; foreign, home carrier) if there are more brainstorms; and
- Current expertise is preferable over past experience.

The moderator's task is to make the brainstorming session as productive as possible. This is complex as it involves strictly watching the basic rules of brainstorming, making short notes of the identified hazards on a flip chart or via a beamer, and subtly steering the hazard identification process along the many dimensions of the operation and possible kinds of hazards. Preferably, moderation is done by a safety analyst involved in the analysis. Especially if the brainstorm is a one-time opportunity, experience and background in moderating brainstorm sessions, as well as extensive preparation, is important.

Somebody else than the moderator has to make more detailed notes of the hazards identified, as a starting point of the minutes of the session.

If the operation is complex, it is good to have an expert give a quick operational oversight presentation (at most half an hour) and answer questions about it. It would be good if the expert on the operation takes notes.

It is important that a safety analyst of the project is present at the brainstorming session. (S)he is the most suitable person to make sure

that the brainstorm delivers what the rest of the analysis needs. If possible, the safety analyst and moderator should coincide, as the moderator is highly influential with respect to the outcome of the brainstorm. This will also reduce the amount of preparation the moderator needs. A "blank" moderator will have to learn many safety issues that are basic to a safety analyst involved in the analysis. An alternative way to keep the number of participants minimal would be to have the safety analyst take notes.

Experience has indicated that the aforementioned group of four to six people is more than adequate for brainstorming – it should rather be considered as a maximal than a minimal group! The reason for this is that controllers and pilots are the main sources of hazards and adding more people to the group will rather hamper than help these operational experts.

More generally, it is well-known in cognitive science [11] that the productivity of brainstorming groups generally does not grow proportionally with the number of participants. As a matter of fact, there are only a few special settings in which the productivity of a brainstorming group surpasses or even equals that of situation where the participants would brainstorm alone! For this reason it is advised not to have the project leader participate in the brainstorm: such a session flourishes with a minimal set of persons with necessary expertise (controller and pilot) and skills (moderator). More participants can even severely damage the brainstorm, e.g. in case some of the additional people are very talkative while the operational experts are shy or when people feel they cannot speak openly due to presence of superiors – group composition is of crucial influence.

3.4 Preparing a hazard identification brainstorm

Active controllers and pilots have busy schedules and their time is precious, hence their participation should be arranged long before the session. Recognition of the project's importance by the employing air traffic service provider or airline is important for obtaining operational expert involvement.

As the operational experts (controller and pilot) must not be involved in the development of the operation, they have to be informed about the operation in order to identify its hazards. In view of their busy schedules, the best way to do that is to start the session with a short overview presentation. This should cover all the aspects of the operation listed below, but not in a detailed way:

- The objective of the developed operation;
- Operational context (geometrical description, timeframe and traffic characteristics);
- Human roles and responsibilities (Air Traffic Control (ATC) and pilot point of view);
- Procedures (ATC and pilot point of view); and
- Technical systems (communication, navigation and surveillance).

Pictures with e.g. airspace/airport layout, in- and outbound routes, and schematic diagrams often work better than a lot of text.

The moderator should prepare a presentation (of at most ten minutes) introducing hazard identification brainstorming:

- What is a hazard?
- The goal of brainstorming;
- The basic rules; and
- The way of working.

The moderator should also prepare hazard categorizations according to:

- Operational aspects;
- Potential conflict types conceivable in the operation at hand (such as conflicts between two departures, between a taxiing aircraft and a vehicle, et cetera); and
- Flight phases and combinations of flight phases in possible conflict situations.

In the preparation, the moderator should populate these categorizations with hazards using:

- Preliminary scoping brainstorms (performed individually, or by moderator and analyst); and
- Hazard and incident/accident databases and relevant literature.

It is not advisable to restrict preliminary scoping brainstorms to functional hazards only: such restrictions almost inevitably induce similar restrictions in the output of the main brainstorm.

3.5 Performing a hazard identification brainstorm

Tasks of the moderator during hazard identification brainstorming are:

- Take strict care that the basic rules of brainstorming are respected (as many hazards as possible and no analysis/criticism);
- Make short notes of the mentioned hazards on the flip over using the format "hazard id (number) and short description" and watch that hazards have a correct and common interpretation;
- Take subtly care that "all" aspects of the operation and possible hazard categories are covered by pointing to such aspects (rather than specific hazards), especially if the identification process gets stuck in specific subsets of the space of all hazards; and
- Apply short breaks before productivity drops significantly, such that the participants can free their memory.

3.6 Comparing functional and brainstorming approach

Fig. 2 gives an impression how hazards identified with the functional and the pure brainstorming approach relate [2], [1] and [4].

The figure indicates that the functional approach explores a limited part (the grey oval at the left side of the large white oval) of the set of all hazards in a rather dense way, and that the pure brainstorming approach covers more

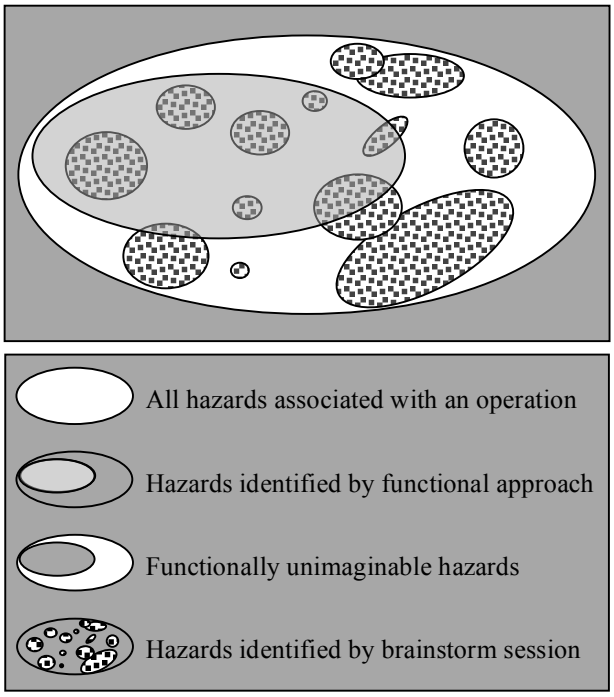

Fig. 2. Subset of functional and pure brainstorming hazards

various parts (the smaller dotted ovals). Hence it is useful to perform both the pure brainstorming and the functional approach to hazard identification, the correct order being: first the brainstorming and then the functional approach, especially when the same operational experts are involved. However, even by applying both approaches one may not expect to be exhaustive.

3.7 After the brainstorm session

The note taker works out and distributes the hazard list among the participants asking to check and correct or complement if necessary – hazards conceived after the brainstorm are welcome, too. The moderator and safety analyst check how effective the brainstorm has been:

- Have all prepared operational aspects, conflict types and hazard categories been covered?
- Have hazards necessitating new conflict types and hazard categories been identified? If not, the moderator has either prepared extremely well, or, more probably, restricted the brainstorm too much to his prepared material;

- Have most hazards identified in the preparation been re-identified during the brainstorm? and
- Is a significant percentage of hazards unimaginable to the moderator and safety analyst?

Based on this evaluation, it may be necessary to have additional brainstorms.

4 Prognostic Hazard Identification by the Future Aviation Safety Team (FAST)

The European Strategic Safety Initiative (ESSI) operating under the aegis of the European Aviation Safety Agency (EASA) chartered the FAST to identify "future hazards and at reducing risks arising from future system changes either within or outside the aviation domain" [8].

Many prognostic hazard discovery processes exist today. For instance, during the design of a new airplane, a manufacturer will spend a substantial amount of engineering effort to identify previously unknown hazards that may be unique to that new design. Building on past experience, using expert understanding of the proposed design, as well as expert conjecture regarding associated hazards, the manufacturer will identify hazards, and then work to eliminate, avoid or mitigate those hazards in the final design.

4.1 The FAST Process, Concentrating on the Concept of Areas of Change

FAST augments existing hazard identification techniques by taking into account an inventory of future changes within and external to the aviation system. Future changes may take the form of unintended evolutionary or revolutionary developments. They may also be deliberately planned with the intent of achieving specific results. Changes affecting the aviation system will usually take the form of technology infusions, organizational or business model changes and/or regulatory modifications and updates. Such "Areas of Change" are the future backdrop, context or milieu in which proposed new concepts, technologies and procedures will be immersed. FAST utilizes these Areas of Change to systematically assess the accumulation of interactions that can create new failures or increase the severity or likelihood of existing ones. Fig. 3 illustrates the process.

4.2 Development of the List of Areas of Change

Members of FAST, in concert with regulation authorities, expert advice, and input from interested parties, first developed a list of Areas of Change during a series of workshops hosted by EUROCONTROL in 1999.

The FAST has cataloged approximately 220 change phenomena that will affect the future aviation system in one way or the other. These phenomena are categorized using the domains listed below:

- Aircraft;
- Maintenance, Repairs, and Overhaul Operations;
- Crew;
- Passenger;
- Organization;
- Authority;
- Air Navigation Services;
- Airport;
- Environment; and
- Space Operations.

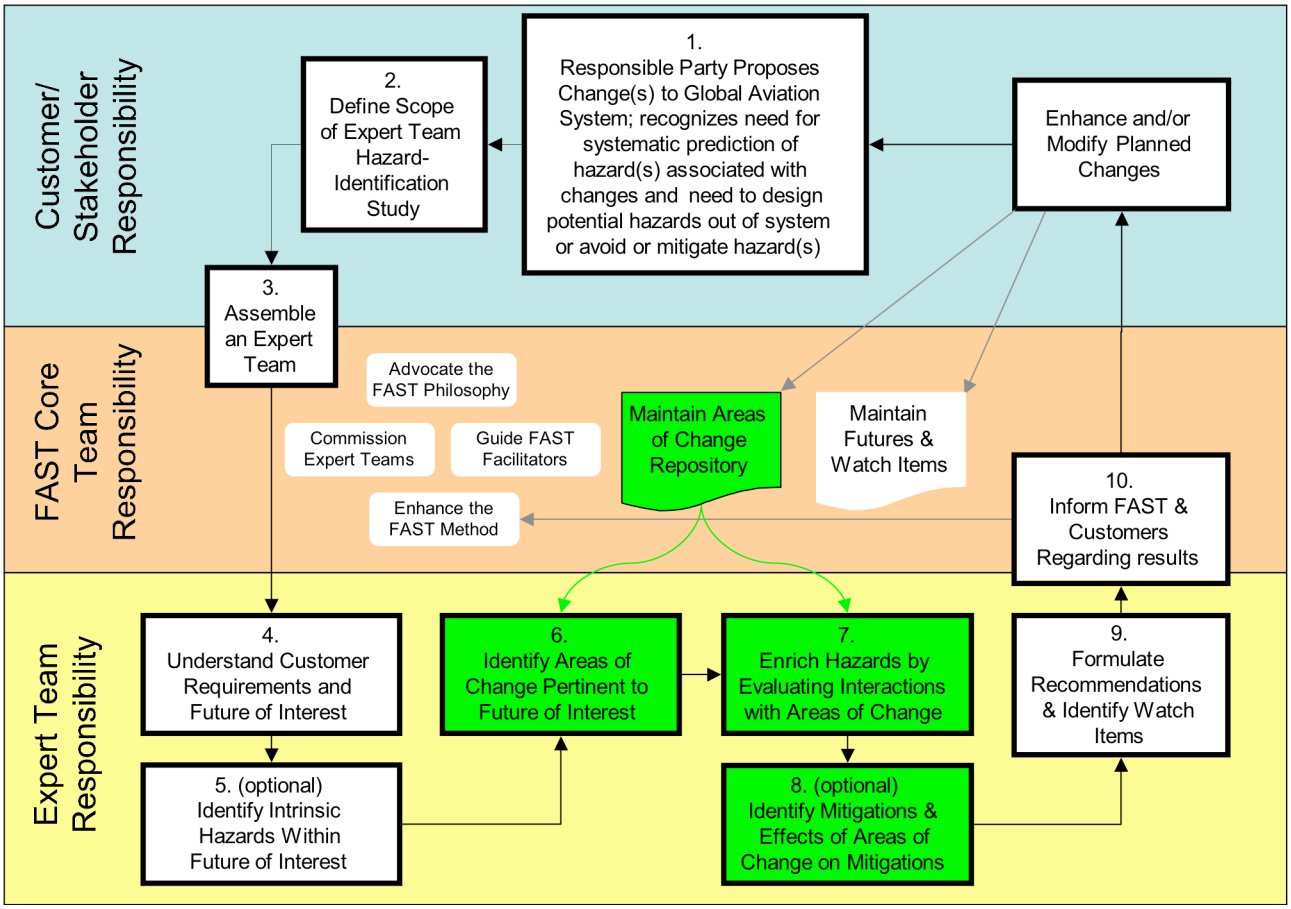

Fig. 3. The FAST Process

The FAST continuously solicits submission of new, candidate Areas of Change affecting the future aviation system. Submission of new AoC's should be made to Rudi den Hertog, Chief Engineer, Fokker Services, FAST Co-chair, rudi.denhertog@stork.com.

Plans are in place to combine FAST AoC's with other sources of future safety concerns, for instance with those emerging from the Issue Analysis Team within the Joint Implementation Measurement Data Analysis Team (JIMDAT). The JIMDAT reports directly to the U.S-based Commercial Aviation Safety Team (CAST).

4.3 Evolution and Interaction of the Areas of Change

An important feature of the FAST method is that it considers that several possible futures may interact with the future under study, producing unanticipated hazards.

Figure 4 illustrates the concept of how Areas of Change ebb and flow with time and how different futures are composed of different sets of Areas of Change. Areas of Change are the future backdrop, context or milieu in which proposed new concepts, technologies and procedures will be immersed. For instance, the future will likely feature the gradual phase out of early-generation jet transports (AoC "a") coupled with the advent of fleets of micro-jet personal aircraft (AoC "l").

Figure 5 illustrates the eleven categories of domains that potentially influence the safety of future concepts of operation. It also illustrates how AoC's in each of these categories interact within and among the categories.

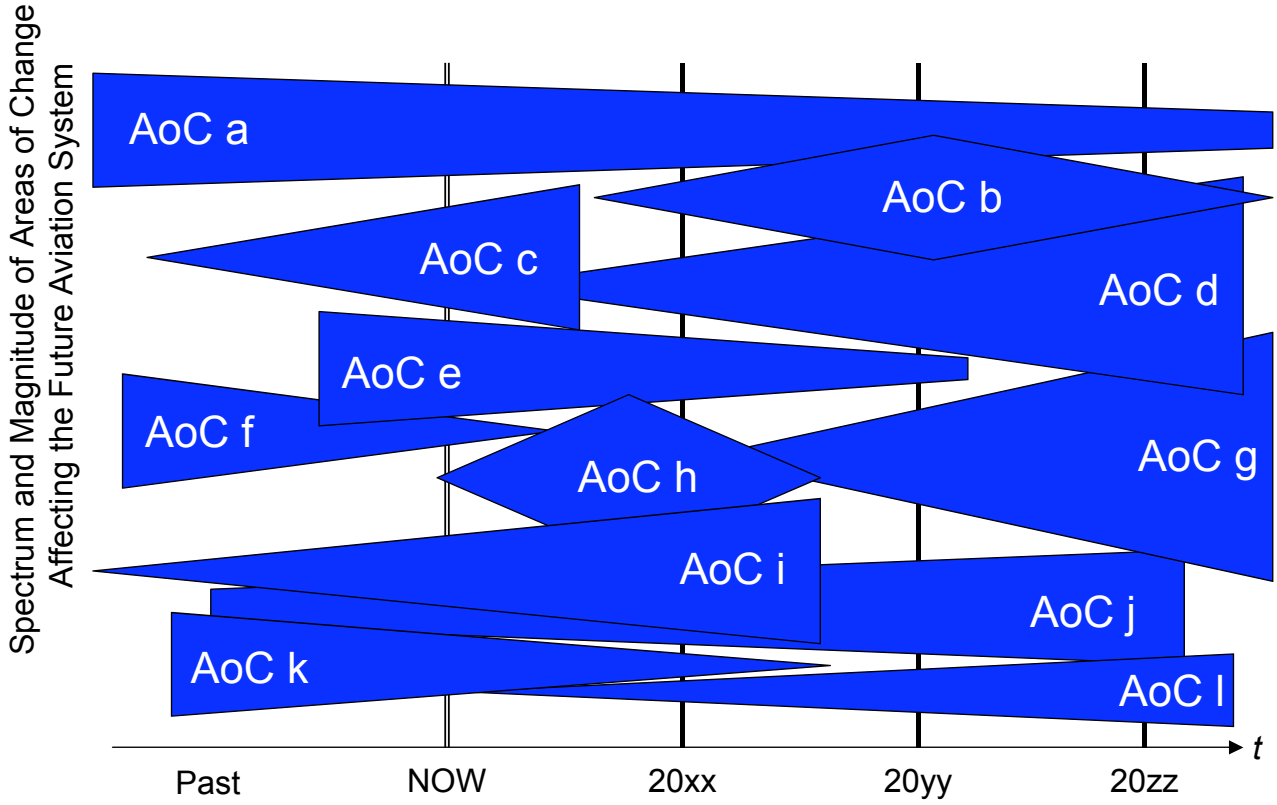

Figure 4 – Temporal Ebb and Flow of Areas of Change

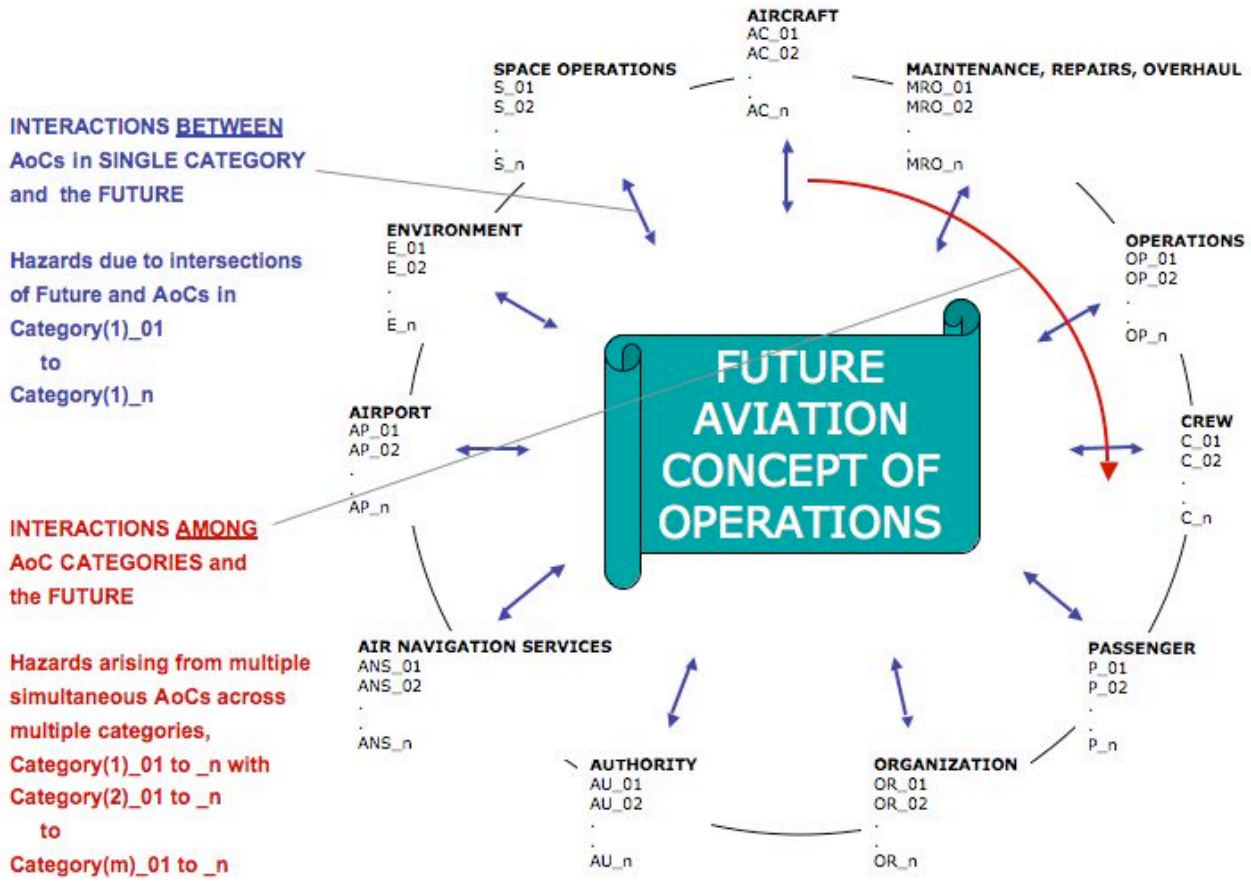

Fig. 5. Interaction Within and Among Areas of Change

4.4 Using the Areas of Change in Hazard Identification

At the stage of the hazard identification process, the AoC's are used as systematic prompts by the analysis team. Their job is to determine how the AoC's may affect the safety and genesis of hazards of the future system under consideration. Using the AoC's, the FAST method recommends that the hazard-analysis team ask the following key questions with respect to the system of interest:

- Does this AoC increase the likelihood of well-understood current hazards that will exist in the Future?
- Does this AoC create new hazards synergistically with other AoC's or with the Future that would not have come into being without the presence of the AoC?
- Does this AoC increase the subjective likelihood of Future hazards to an unacceptable level?
- Does this AoC create increased potential for human error, procedural non-compliance or equipment failure?
- Does this AoC decrease the resilience of the projected safety system?
- Does this AoC render the projected safety systems more brittle to off-nominal conditions?
- Does this AoC decrease safety levels during non-normal or emergency operations within the projected Future?
- What current and projected safety assurance measures within the Future may be lost or rendered ineffective as a result of this AoC?
- Does this AoC require creation of new control measures for critical aspects of the Future? Definition: A control measure is an action or procedure that will reduce, prevent or eliminate a potential hazard.
- Does this AoC adversely affect control measures, critical control points or critical limits? Definitions: A critical control point is a step at which a control measure is applied. A control limit is a maximum and/or minimum value for controlling a physical parameter.
- Will this AoC create new conditions that are currently not part of the design assumptions for the Future systems and procedures?
- Will this AoC result in decreased skill levels and judgment among operators of Future systems?

5. How FAST enriches hazard identification by systematic consideration of future developments

The first fundamental notion of this paper is that while a traditional, i.e. functional, approach to hazard identification yields a subset of all hazards associated with an operation, it leaves some important hazards unidentified. The pure brainstorm technique developed by NLR will identify hazards outside the range of the functional approach (and will duplicate some as well).

To address the second fundamental notion of this paper, let us assume that any possible hazard affecting aviation can be associated to one of the eleven aviation system domains categorized by the FAST and shown in Fig. 5. This then results in the pie-shaped domains in the oval depicted in Fig. 6 below.

Systematic consideration of the 220+ FAST AoC's via the eleven categories shown above will extend the scope of the hazard identification to include these changes and this will direct explicit attention to threats caused by these areas of changes that have not been considered systematically with the functional approach or the structured brainstorming approach.

The combined approach works as follows:

1. Structured brainstorming "discovers" certain "unimaginable" hazards not readily identified using the functional approach. These hazards are of necessity limited in scope due to the range of expertise of the domain experts participating in the exercise.

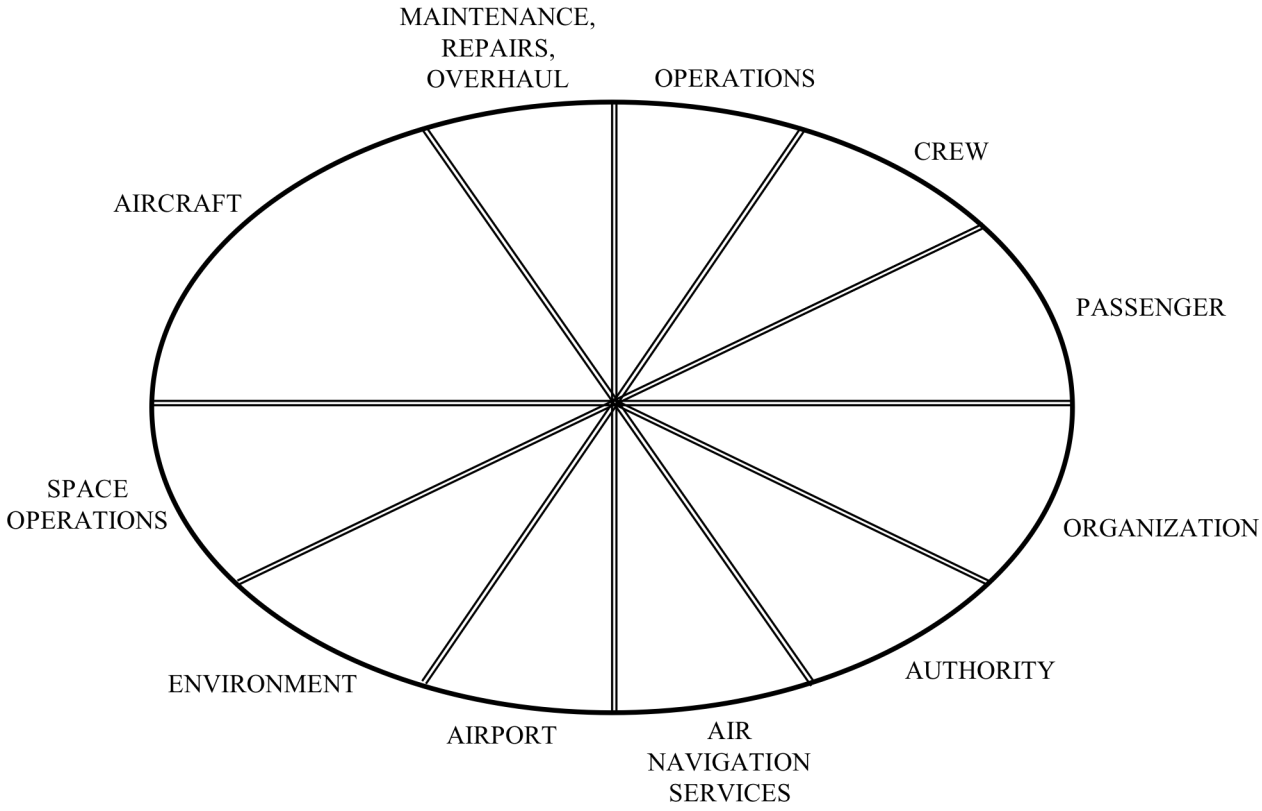

Fig. 6. Eleven Categories of the Universe of All-Possible Hazards

2. Hazard identification is then augmented by systematic consideration of the contextual factors within each of the eleven categories of all-possible hazards. Consideration is also given to interaction of hazards within specific categories as well as among and across the various categories.

The expected end result is that application of a functional approach plus NLR brainstorm plus the FAST method (based on AoC's) will identify a more complete set of hazards and cross-domain interactions than any one method will on its own:

- The functional approach will densely cover hazards directly associated with functional failures of the operation considered.
- The brainstorming approach will add hazards of the considered operation less or not associated with functional failures.
- The FAST approach to hazard identification will in addition yield hazards associated with "perturbations" of the considered operation along the AoC's.

The additional hazards identified using the FAST AoC's in each of these categories as prompts will add significant value to traditional hazard-identification techniques. An impression of the additional hazards identified is given in Fig. 7. There will be some inevitable overlap between hazards identified by the respective methods.

6. Conclusion

This paper describes a hazard identification methodology that will help reveal hazards not typically uncovered by traditional "functional" approaches to hazard identification. Its key elements are structured brainstorming by aviation subject-matter experts coupled with an systematic identification of additional hazards of a proposed aviation "future" in light of the contextual factors – so-called Areas of Change – that will be present at the time of development and deployment. Application of the method outlined in this paper to future concepts of

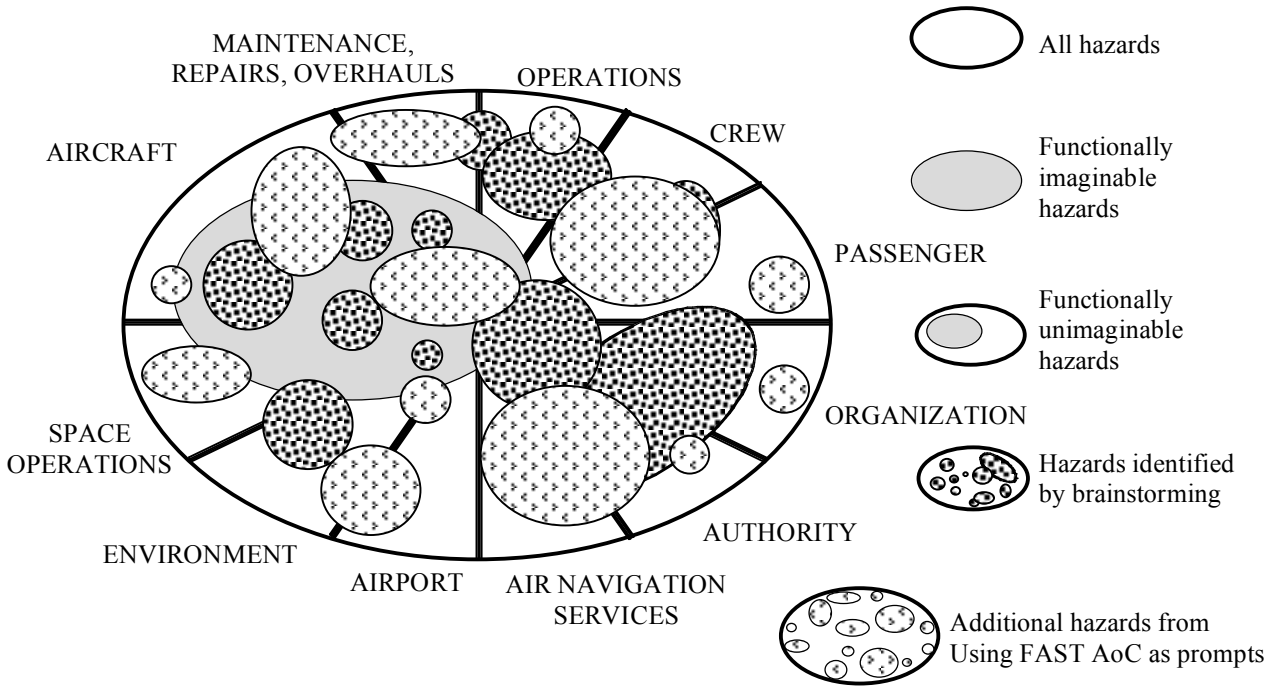

Fig 7. Augmentation of Functionally Imaginable and Unimaginable Hazards by Consideration of FAST Categories

operation will identify emergent hazards. Foreknowledge of these hazards will ensure that aviation safety research is responsive and relevant to emerging safety risks. The aviation community must not focus solely on safety problems of the past or the risks of near-term system deployments. It must anticipate and prepare for the hazards of the emergent future.

New vehicles, operational paradigms, and business models will introduce novel safety risks into the airspace system. Potentially, the most important issue for air transportation in the future is how to safely integrate the air-, ground- and space-based aviation support systems with the human operators/monitors of the technology. For Part 121 operations this will include the safety considerations of evolving flight crew and ATM integration. Not all hazards associated with such operations will necessarily be revealed by traditional "functional" approaches. Hence, the proposed hybrid approach incorporates the best features of multi-disciplinary brainstorm teams with systematic consideration of Areas of Change affecting the future aviation system.

Not all past safety concerns may necessarily be relevant in future operational environments. There is a very real danger in apparent certainties in assessment of the significance of traditionally important causal factors of aviation accidents revealed by pure functional hazard assessment. Many historic safety concerns are now statistically insignificant in certain geographic areas. We must not relax our vigilance especially in those emergent domains where human performance will remain an essential ingredient for system safety. This vigilance demands that all available hazard identification methods be brought to bear on the novel operational concepts of the future.

References

[1] Blom, H.A.P., Stroeve, S.H. & De Jong, H.H. 2006. Safety Risk Assessment by Monte Carlo Simulation of Complex Safety Critical Operations. In Redmill F & Anderson F (eds.), Proc. of the 14th Safety critical Systems Symposium, Bristol, UK, February 2006, Springer.

[2] De Jong H.H. 2004. Guidelines for the identification of hazards; How to make unimaginable hazards imaginable? NLR Contract report 2004-094 for EUROCONTROL, March 2004, included in [6]: FHA, Ch. 3, GM B.2.

[3] De Jong, H.H., Stroeve, S.H. and Blom, H.A.P., The roles of air traffic controllers and pilots in safety risk

analyses, Proc. ESREL 2006, 22-26 September 2006, Estoril, Portugal.

[4] De Jong, H.H., Blom, H.A.P. and Stroeve, S.H., Unimaginable hazards and emergent behavior in air traffic operations. Risk, Reliability and Societal Safety – Aven & Vinnem (eds), Proc. ESREL 2007, Stavanger, Norway

[5] EUROCAE/RTCA 2000. Guidelines for approval of the provision and use of ATS supported by data communications, EUROCAE WG-53/RTCA SC-189, EUROCAE document code ED-078A, Save date 24 July 2001.

[6] EUROCONTROL 2006. Safety Assessment Methodology, Version 2.1, November 2006, Mana P (contact person), http://www.eurocontrol.int/safety/gallery/content/public/library/SAM/SAM_Electronic_Self_Assessment.zip.

[7] Everdij, M.H.C. and Blom, H.A.P. (editors). Database containing over 700 safety assessment methods and techniques from various industries, Maintained by NLR, Available at http://www.nlr.nl/documents/flyers/SATdb.pdf.

[8] Future Aviation Safety Team Handbook, September 2006

[9] Future Aviation Safety Team, Terms of Reference, 14 December 2006.

[10] Kletz, T. 1999, Hazop and Hazan; identifying and assessing process industry hazards, The Institution of Chemical Engineers, 4th ed.

[11] Nijstad B.A. 2000. How the group affects the mind, PhD thesis University of Utrecht, Interuniversity Center for Social Science Theory and Methodology, 29 September 2000.

[12] Smith, Brian E., Prognostic Aviation Safety in the 21st Century – The Future Aviation Safety Team, NASA Ames Research Center; Moffett Field, CA, International System Safety Society Conference, August 2006

[13] Smith, Brian E. System Safety & Reliability of Current Modern Large Jet Aircraft, NASA Ames Research Center; Moffett Field, CA, International System Safety Society Conference, August 2006

Copyright Statement