SAFETY ANALYSIS METHODOLOGY FOR ADS-B BASED SURVEILLANCE APPLICATIONS

Jonathan Hammer, The MITRE Corporation

Gilles Caligaris, EUROCONTROL

Marta Llobet, Sofréavia

Abstract

The introduction of ADS-B as a surveillance source for both air-to-air and air-to-ground operational use presents many new challenges. While it is possible to use ADS-B for a variety of surveillance applications, development of requirements for these applications requires safety assurance. With the potential disparate uses of ADS-B, a common framework for safety analysis is of paramount importance, both for reducing the time needed for acceptance of new applications, and for providing a common basis for key safety requirements.

This paper describes a method of safety analysis of ADS-B applications that has been agreed to internationally by United States' and European standards bodies. The analysis is structured in two parts: an operational hazard identification and assessment (OHA), followed by an allocation of safety objectives and requirements (ASOR). The OHA identifies hazards and classifies their severity while the ASOR allocates safety requirements to both ground and airborne functions. The safety analysis methodology includes an analysis of hazard causes, likelihoods, internal and external mitigation means, and the potential effects of hazards on safety, known as operational effects.

Although the analysis techniques themselves have a firm standing in government and industry, what is novel is the application of the techniques to the unique problems of ADS-B, and the framework surrounding the analysis that allows for continued development of ADS-B applications. An example of the analysis is presented for a specific ADS-B application, known as the "Enhanced Air Traffic Service in Non-Radar Areas using ADS-B surveillance (ADS-B-NRA)." This application is important because of its expected near-term use in multiple countries and because the analysis represents the first internationally agreed safety analysis for ADS-B.

Introduction

The technology of ADS-B and its attendant applications have been under development for over 10 years. Initial standards for requirements for ADS-B were finalized in 1998 [1]. [1] developed preliminary requirements for several possible applications of ADS-B, but no formal safety analysis was included.

Meanwhile, development of concepts for ADS-B applications evolved during the 1990's and the early 2000s [2] – [9]. Air-to-air application concepts varied from using ADS-B to help achieve higher runway throughput in instrument meteorological conditions by pairing aircraft in extremely closely spaced parallel runways [2], [3], to controlling the spacing between aircraft landing on the same runway [4], [5], to using ADS-B to help control sequencing and merging between en route and terminal control areas [6], [7]. Additional concepts included a variety of situational awareness applications both in the air and on the airport surface [8]. Significant operational tests were conducted on these applications, particularly by the US Cargo Airline Association [9].

Background

Despite the conceptual and sometimes detailed technical development of ADS-B applications, a common, internationally agreed framework for development of safety requirements for ADS-B applications has been lacking until quite recently.

The history of internationally sanctioned safety work for air-to-air applications resides primarily on analysis that was done for the Traffic Alert and Collision Avoidance System (TCAS) [10], [11]. The TCAS safety analysis, however, is quite specialized, and is not generally applicable to a diverse set of ADS-B applications. One attempt was made to compare the likely safety of ADS-B-based Conflict Resolution with the safety of TCAS [12], but the

comparative techniques used in this study are limited to conflict detection and resolution, and the proposed ADS-B applications described above are intended to support a broader spectrum of operations.

Safety analyses of other specific applications have also been performed [13], [14], but again, the applicability to a broad set of applications and international agreement to the methodologies were not yet established. An example of internationalizing a common safety methodology is captured in [15] for data link services, but this analysis was limited to data communications.

Within the US standards community, RTCA developed the Aircraft Surveillance Applications (ASA) MASPS [16] that described and analyzed a broad spectrum of applications. Safety analysis was included, and gave consideration to some US-derived methodologies, as in [17], [18], and [19], but the document was not rigorous in its application of other internationally sanctioned safety methodologies, specifically those of [20], and the newer US FAA required methodologies of [21] (which were not available at the time that the work was performed).

In Europe, EUROCONTROL developed a Safety Assessment Methodology [23] and applied the method to a number of projects but the method has not been used until recently for ADS-B based applications.

The RTCA/EUROCAE joint ADS-B task force known as the ADS-B Requirements Focus Group (RFG) has been instrumental in arriving at an internationally agreed operational safety analysis framework for ADS-B applications. The following sections describe the methodology and offer an example of the analysis and results for the application "Enhanced ATS in Non-Radar Area using ADS-B surveillance". The specific work on this application has been officially agreed to and approved by both RTCA and EUROCAE, and has been published jointly by those organizations as [22].

Safety Assessment Methodology

Although ADS-B applications stress the surveillance component of air traffic services, the applications also impact other CNS/ATM system elements. The safety methodology proposed for assessing ADS-B applications is based on the approach from [20] and [23] but, has been customized to include additional system elements because of the complexity of ADS-B applications.

The process adapted to perform the Operational Safety Assessment can be described through the "bow-tie" model (as in the figure below). In line with this model, the following three steps are performed:

- The first step is to identify Operational Hazards (OH) for the application (depicted in the centre of the figure) based on operational expert analysis.
- The OHs are then analyzed based on their operational effects (OE) in the airspace (as depicted in the right-hand side of the figure). The objective of this Operational Hazard Assessment (OHA[1]) is to set the Safety Objectives (SO) for each OH and to establish the Safety Requirements (SR) that ensure that the safety objectives are met.

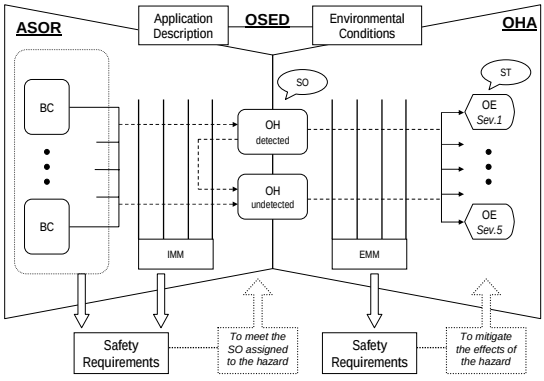

Figure 1. Operational Safety Assessment Process Overview

- The third step is the Allocation of Safety Objectives and Requirements (ASOR), depicted on the left-had side of the figure. The objective of the ASOR is to identify Basic Causes (BC) that can lead to the OH. Fault-trees are used in the identification process and also in the allocation of the safety requirements. Using the fault trees, safety requirements are identified for airborne and ground functions to meet the safety objective for each OH.

[1] also called Functional Hazards Assessment (FHA) in [23].

As annotated in the figure, the overall process is applied based on a detailed description of the application and a description of the environmental conditions where the application is to be used. The application and environment description is described in the Operational Services and Environment Definition (OSED) document.

The above process is usually repeated several times, i.e., an initial assessment is typically followed by revisions to assumptions, descriptions etc.

Operational Hazard Assessment Process

The Operational Hazard Assessment consists of four steps: hazard identification, allocation of severity classes, determination of likelihood, and assignment of safety objectives as illustrated in the figure below.

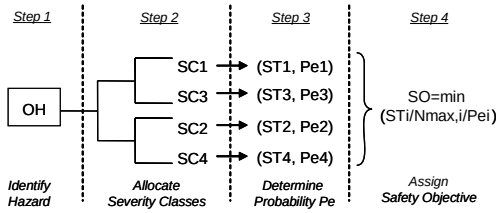

Figure 2. Operational Hazard Assessment Process[2]

During the hazard identification process, the ADS-B application is analyzed in brainstorming sessions with operational experts: air-traffic controllers, pilots, and safety experts. The purpose of these sessions is to identify hazards that could adversely affect the safety of the ATS application.

A hazard may result from an action that is not performed at all or is performed incorrectly. The hazards are analyzed to deduce possible effects on aircraft and air navigation services (e.g. accident, major, minor incidents). Two cases are examined: when the hazard is detected and when it is not.

In the second step of determining severity classes, hazards are classified by the severity of their effects using a common severity classification scheme. Environmental factors and specific external procedures which could mitigate the effects of a hazard are taken into account in determining the effects, and the severity of the effects of each hazard. Severity Classes (SC) are illustrated in the figure; each severity class corresponds with a quantitative safety target.

The severity class is assigned using a modified severity classification matrix from [20] (the hazard classification matrix from [20] was modified by the RFG to correspond to surveillance applications, rather than data link applications). In this matrix severity class 1 corresponds to the most critical effects (e.g. - mid-air collision or controlled flight into terrain) while severity class 5 indicates that there is no effect on safety.

The third step in the OHA is to determine an equivalent probability, termed *Pe*. *Pe* is a conditional probability which expresses the probability that the occurrence of a hazard will result in a specific operational effect, taking into account existing External Mitigation Means (EMM). A value for *Pe* is obtained for each hazard-effect pair and is denoted Pe_{ij} where *i* is the index of each effect and *j* is an index of each hazard. An example is shown in the figure below.

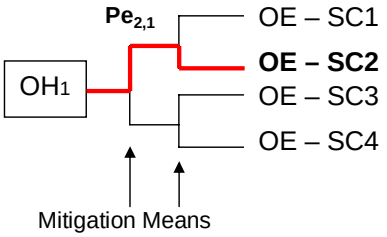

Figure 3. Pe for Hazard-effect Pair[2]

Pe is calculated by quantifying the effectiveness of the Environmental Conditions (EC) and external mitigation means previously identified in the second step. This is accomplished through the following approach: quantify each of the external mitigation means identified for the specific hazard (based on simulation results, statistical analysis, operational expertise - this might be done during the sessions conducted with operational experts described in Step 1). Event trees may be developed to support this process. *Pe* is then calculated based on the probabilities for each effect.

[2] Copyright RTCA, Inc., and EUROCAE used with permission.

Apportionment of the ATM Risk budget for the application: A Safety Target (**ST**) specifies the maximum frequency of occurrence of *all* effects in the ATM system with a specific severity class. For example, safety target 1 specifies the maximum frequency, in the ATM system, of fatal accidents whatever the kind of accident (e.g. mid-air collision, controlled flight into terrain (CFIT), aircraft collision on the ground, collision between an aircraft and a vehicle, etc.).

A Risk Classification Scheme (RCS), based on the severity classification matrix mentioned before, presents the safety targets for each severity class. The risk classification is applicable to the overall ATM system. Values used in the RCS are obtained from several sources[3]. They are presented in the following table:

Safety Target	Risk Per Flight-Hour or Operation
ST1	**1e-08**
ST2	**1e-05**
ST3	**1e-04**
ST4	**1e-02**

Table 1. Risk Classification Scheme

As these requirements encompass the entire ATM system, an apportionment of the budget must be made for each specific ADS-B application hazard. It is assumed that the provision of ATM services includes approximately 100 hazards that can generate effects of severity between classes 1 and 4. An apportionment is performed based on an assumed distribution of these ATM hazards into the different severity classes; we use the quantity $N_{max,i}$ to refer to the number of ATM hazards leading to a specific severity class "*i.*" For example, it is assumed that 20 ATM hazards generate effects of severity class 1 (i.e. $N_{max,1}$=20), and 45 ATM hazards generated effects of severity class 4 (i.e. $N_{max,4}$=45) .

[3] ESARR4 specifies the following ST1 = 1.55 e-8/fh or 2.31 e-8/flight assuming an average flight duration of 1.5 hours. For simplification purposes, an average duration of a flight of 1 hour is used instead of 1.5 and values are rounded off as an integer figure, i.e. ST1 = 1e-8/fh or 1e-8 / flight. Safety Target 2, 3 & 4 values, for ATM are found in ED125, SAM v2, FHA chapter 3, Guidance Material Ev2.1 [24].

The apportionment process is then used to calculate the Safety Objective for each ADS-B application hazard.

Units: The expression of Safety Targets per flight hour (or per flight using an average flight duration), is consistent with standard avionics certification practice. However, in the case of ground ADS-B applications (e.g. the NRA application), since hazards are related to specific services provided by Air Traffic Services, the safety targets have also been expressed in *Air-Traffic Service Unit Hours*, abbreviated as ATSUh. The conversion from flight-hours to ATSUh is calculated based on airspace assumptions, in particular, the number of aircraft expected to be handled in a typical sector over a given period of time. In the specific case of the ADS-B-NRA application, a distinction has been made between en-route and Terminal Maneuvering Area (TMA) airspaces, obtaining the following safety targets:

Safety Target	Air Traffic Service Unit Hours (ATSUh)	
	En route	**TMA**
ST1	**1e-07**	**1e-08**
ST2	**1e-04**	**1e-05**
ST3	**1e-03**	**1e-04**
ST4	**1e-01**	**1e-02**

Table 2. Safety Targets in ATS Unit Hours for NRA Application

Assignment of the Safety Objective: The last OHA step is the calculation of the quantitative safety objective for each hazard, i.e. specifying the maximum acceptable frequency of occurrence of the hazard.

The following formula is applied to calculate the Safety Objective (SO) for each hazard:

$$SO_j = \min_i (ST_i / N_{max,i} / Pe_{ij}),$$

where:

SO_j : Safety Objective for a given hazard j

i: index of each scenario for a hazard leading to a severity class *i* Operational Effect

ST_i: corresponds to the ATM Safety Target associated with the severity class *i*

$N_{max,i}$: number of all ATM hazards having a given Severity Class *i*

j: index of the hazard in a given severity class *i*

Pe_{ij}: Pe relating to a hazard-effect pair

The quantitative safety objective that is assigned to each hazard becomes the starting point for the ASOR process as explained in the following section.

Allocation of Safety Objectives and Requirements (ASOR) Process

During the Allocation of Safety Objectives and Requirements (ASOR) process, safety objectives are apportioned to the ground and air domains, and the corresponding safety requirements are identified4.

Three steps are applied during the ASOR process. As illustrated in the following figure, during the ASOR, fault trees are developed, safety objectives are allocated, and finally, safety requirements are derived.

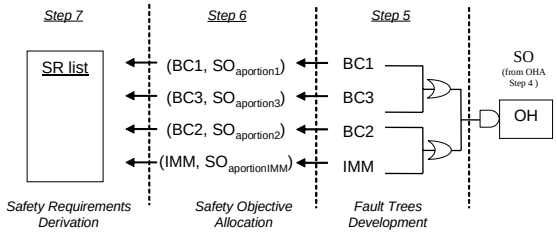

Figure 4. ASOR Steps[5]

Fault Tree Development: For each hazard, a fault tree is developed with the purpose of apportioning the hazard risk among the various system elements. The fault trees detail basic causes and their interactions that can result in each hazard. Each basic cause is analyzed in order to derive appropriate requirements. Internal Mitigation Means (IMM) are procedures and specific means considered to be part of the application under assessment and that reduce the likelihood of occurrence of the hazards. Internal mitigation means and their possible failures are also considered in the fault trees.

The fault tree provides a detailed overview of the contribution of all domains for a given hazard. Fault trees are elaborated by decomposing the hazard, top-down, by examining potential combinations of failures. The hazard is at the top of the fault tree; at the bottom of the fault tree are the basic causes (technical, procedural, human or environmental causes) that can lead to the hazard. The nodes in between the top and the bottom are indicated as "AND" gates (with a straight line at the bottom of the gate) and "OR" gates (with a concave line at the bottom of the gate). For an "AND" gate both conditions must be satisfied for the hazard to propagate; for an "OR" gate either condition may be present for the hazard to propagate.

The following figure provides a graphical view of the structure of a fault tree:

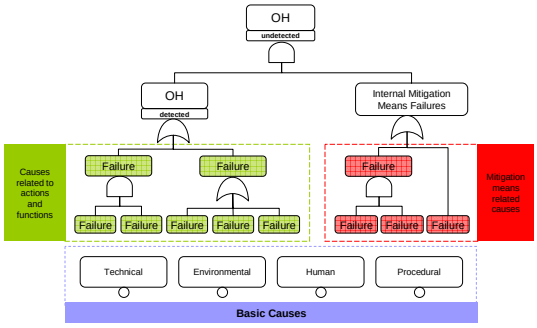

Figure 5. Example of Fault Tree Structure[4]

In order to construct a fault tree, two considerations are accounted for: (1) the various actions[6] that are undertaken to perform the application, and (2) the *Functional Architecture Description* which establishes the level to which the fault trees are to be decomposed (i.e. the basic causes).

As mentioned earlier, each hazard is considered in both a detected and undetected context. By detected we mean that there is a human and/or a system in the process that is made aware of the problem through internal mitigation means. By undetected we mean that the hazard progresses without human and/or system cognizance. The previous figure shows an example of an undetected hazard; the figure illustrates that undetected hazards result when the hazard occurs and internal mitigation means fail.

Safety Objective Allocation: The purpose of the Safety Objective allocation in the ASOR is to establish requirements which, if they are met,

[4] Safety requirements are ultimately combined with other requirement sources (e.g. from performance assessment or collision risk modelling) that not addressed in this paper.

[5] Copyright RTCA, Inc., and EUROCAE, used with permission.

[6] An action is performed by a single actor (or domain). An action may be a human task or a system action, and it may be supported by a technical function.

will eventually enable the system to achieve the safety objectives specified in the hazard assessment and thereby address or mitigate the risk-bearing system hazards. The safety objective corresponding to each hazard is apportioned to the different basic causes in order to derive the safety requirements.

The allocation is carried out in two sub-steps:

- A first allocation based on precedent: existing documents may be used to allocate the likely probabilities or to check their validity;
- A brainstorming session: operational and system experts of each domain participate to validate the results and conclusions. During this session not only is the allocation of safety objectives validated, but the fault trees themselves, and the list of internal mitigation means are also completed and validated.

After the allocation, a sensitivity analysis may be used to determine if some requirements may be relaxed while maintaining the required safety objectives. Sensitivity analysis allows identification of the most important causes affecting the top event probability. Sensitivity analysis can be performed using dedicated software tools (e.g. FaultTree+™, Aralia™ SimTree™, etc).

Judgment is applied to take into consideration existing architectures, requirements, procedures, etc. This consideration can only be obtained by involving all the relevant stakeholders during the ASOR discussions mentioned before, and identifying the suitable shared risk mitigation strategy to be adopted (i.e. how the apportionment of the safety objectives is performed on the different elements of the application: ground and air).

It is important to note that several different allocations of requirements may achieve the desired safety objective (the solution may not be unique).

As a result of the allocation, a required maximum failure rate is assigned to each basic cause. Note that if a basic cause is involved in multiple hazards, the final required failure rate assigned is the most stringent value.

Safety Requirements derivation: Based on the results obtained from the previous step, a study of each basic cause (including internal mitigation means failures) is performed in order to derive appropriate Safety Requirements. The assessment is done based on safety judgment and is validated based on discussion involving operational and system experts.

Several types of safety requirements may be obtained depending on the nature of each basic cause considered:

Functional-system related requirements: Quantitative safety requirements are derived that indicate, for example, the maximal allowable probability or frequency of occurrence for a specific system failure. In the case of systems that are already in operation, feedback from field experience will help to define what is achievable. Qualitative safety requirements may also be identified to specify the system, for example, to establish specific procedures related to the use of some functions or to establish a level of design assurance (e.g. for software).

Human-procedures related requirements: Only qualitative requirements are derived from human related causes. The requirements could be either a new procedure, the modification of an existing procedure, or the need to highlight the safety importance of a procedure (for example the read-back) during training. The requirement that a specific human action must be supported by a specific feature of a tool may be addressed as well.

Case Study: Ground Air-Traffic Control Use of ADS-B in Non-Radar Area (ADS-B-NRA)

The use of ADS-B for non-radar area (ADS-B-NRA) is an important air-to-ground use of ADS-B, and represents a key initial application that is planned for several countries including the United States, Australia, Canada, Sweden, France, Ireland, Spain, Portugal, Italy, Greece, Malta and Cyprus. ADS-B-NRA is the first ADS-B application for which a safety analysis has been performed and accepted internationally by the members of the RFG.

The intent of ADS-B-NRA is to use ADS-B as a surveillance source in airspace that is not covered by existing radar infrastructure, and in so doing, expand the areas of coverage for air-traffic control operations, thus reducing separation minima from procedural to radar-like separation minima. The safety assessment of use of ADS-B for this purpose has been developed

and agreed internationally [22]. It is expected that the proposed approach will be re-used to the maximum extent possible in local implementations of the application, taking into account specific local conditions that may differ from the generic conditions identified in [22].

We present here an example of the safety methodology for the ADS-B-NRA application.

Operational Hazard Assessment results: First, the hazards analysis as described above was conducted through a workshop of operational experts. There were nine hazards identified: (1) a controller loses position information for one aircraft, (2) a controller loses position information for multiple aircraft, (3) incorrect position information for multiple aircraft is displayed to a controller, (4) incorrect position information for one aircraft is displayed to a controller, (5) data quality indicators are unstable, (6) the aircraft Mode A code or special position indicator is lost or incorrect, (7) the aircraft altitude is lost or incorrect, (8) indications to a controller of an aircraft emergency mode are lost or are incorrect, and (9) the aircraft identification is lost or is incorrect. It was noted that hazards 1 – 5 are unique to ADS-B, whereas all the other hazards are identical to the status-quo ATC operation with radar, and so were not further examined.

Operational Hazard (OH)	Severity Class	
	Detected	Undetected
Position loss for 1 AC	4	1 (most severe)
Position loss > 1 AC	3	1
Incorrect position 1 AC	4	1
Incorrect position > 1 AC	4	1

Table 3. Example of ADS-B-NRA Operational Hazard Severity Classes

Per the methodology, each hazard was examined for the cases in which the hazard is detected and in which the hazard is not detected. Based on operational expert judgment, the following severity classes were assigned to the hazards assessing their worst credible effects as described in the table above.

The four hazards listed above in the table are significant because they require the examination of key differences between ADS-B and existing, radar-based surveillance. In particular, the failure modes for information loss and for incorrect information with ADS-B are distinct from the same hazards with radar. The hazards with ADS-B involve a chain of new aircraft avionics and ground systems, including satellite-based navigation systems. Safety targets as described in the previous part of this document have been used for both En-Route and TMA cases. Safety objectives are described further below.

Allocation of Safety Objectives and Requirements Process results: The figure below illustrates the functional architecture for ADS-B. The aircraft systems and subsystems are on the top of the figure, labeled "Transmit Aircraft Domain," while the ground systems are on the bottom of the figure, and are labeled "Receive Ground Domain." The interfaces between subsystems are indicated by vertical lines; the interfaces between the air and ground systems are indicated by the radio bolts. Failures of each of these functional subsystems are considered in the safety analysis, as will be illustrated momentarily.

We will use hazard 4, called "incorrect position for 1 aircraft," as a principal example further illustrating the safety analysis. First, it was recognized that there are two failure modes that can cause of an incorrect position to be displayed to a controller with an ADS-B-based system: (1) an integrity failure of the position source information (e.g. the GNSS source or the aircraft sensors as shown in the functional figure below) or (2) sustained corruption, due to a software or hardware flaw, of the information (through the Surveillance Transmit Function, the ADS-B Transmit Function on the aircraft and the ground-based receive, processing, and display functions as shown in the figure.)

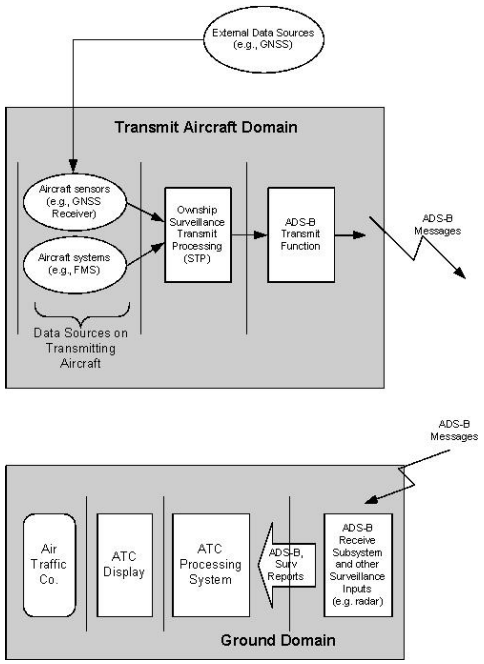

Figure 6. Functional Architecture of ADS-B for Ground-Based Applications

Corruption of information (e.g., due to design flaws) is seen as a distinct issue from position source failures, because corruption is largely controlled by design assurance methods and equipment certification. Corruption can cause an error of nearly any magnitude and little can be said about the probability distribution of the errors. (In contrast, by position source failures we mean the failure of algorithms for integrity monitoring; where probability distributions of the errors for such failures are well understood).

Fault Trees: Once the principal failure modes were enumerated, a set of fault-trees was drawn to analyze the failures and the likely basic causes of the failures.

The fault tree for the undetected, corrupted position discussed above is shown in the figure below for the TMA case. At the bottom of the fault tree are the basic causes (indicated by circles) that can lead to the hazard. At the top of the fault tree is the estimated rate of occurrence of the hazard. Failure rates (indicated with an "r") and/or probabilities (indicated with a "Q") are shown beneath each gate and event. The probabilities are calculated from the failure rates based on an assumed life-time of 1 hour. A description of each gate or event is given inside a rectangular box above the gate, and each gate is numbered for identification.

In this example the basic causes include ground-domain corruption from either the receive subsystem or the display subsystem, or corruption of the information in the aircraft domain. It is notable that we only consider corrupted information that has an error of less than 50 NM for the undetected case, because it is assumed that the controller will flag, as obvious, errors greater than nominally 50 NM. In this case, given that the failure can take on any value, a uniform probability distribution was assumed in calculating the likelihood of an error being less than 50 NM.

The failure rates of the basic events are based on expected subsystem failure rates; these are quantified based on certification and design assurance levels as per [18] and [19]. Part of the objective of the analysis is to determine the appropriate design assurance level for the avionics and ground equipment. In order to arrive at an answer, the failure rates are hypothesized. A determination is then made as to the failure rate adequacy based on the top-level result in the tree.

In this example the failure probability of the avionics component (in the aircraft domain) was postulated to be 1E-5 per flight hour, which corresponds to a "major" failure category, and will result in corresponding design assurance requirements as specified in [18] and [19]. The ground system components were found to require a $5x10^{-6}$ per-hour failure rate, which is roughly halfway between the "major" failure rate and the "severe-major" failure rate ($1x10^{-7}$) normally ascribed to aircraft avionics. Although ground-system components design assurance requirements have not been traditionally specified in this way (especially in the US), with the advent of new systems that integrate air and ground components, such specifications become necessary in order to complete a robust safety case.

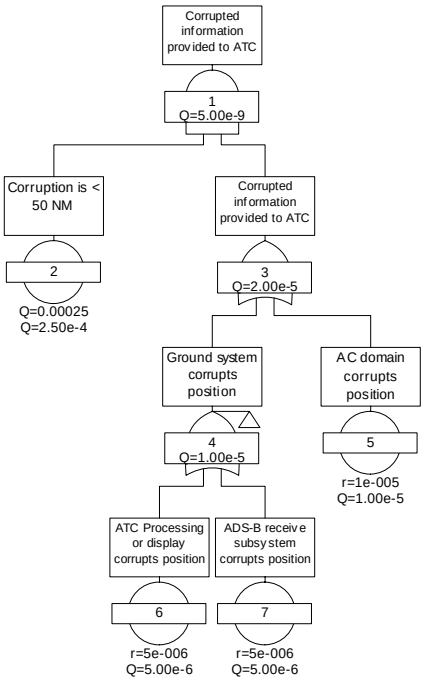

Figure 7. Fault Tree for Corrupted Information

Conversion of Operational Hazards to Consequence Probability: For this example, the top value of the fault tree indicates that with the basic event probabilities indicated in the bottom leaves of the tree, the hazard likelihood is $0.5x10^{-9}$ per air-traffic service unit hour. As discussed above, for hazard class 1 the overall ATM safety target for the TMA area is $1x10^{-8}$ per air-traffic service unit hour. When translated by the assumptions regarding the number of hazards of class 1 in the TMA area, this results in safety objective of $5x10^{-10}$ per air-traffic service unit hour for this specific hazard.

In order to determine that the safety objective is met, the hazard probability needs to be converted to a probability of a consequence. In this case the potential consequence of the hazard, as identified in the hazard analysis, is a mid-air collision. The value that translates between the hazard and the probability of the consequence, as described above, is termed Pe. Pe is a conditional probability that represents the probability of a collision given that the hazard has taken place.

In general, the likelihood of collision is dependent upon the external environment conditions as well as the magnitude of the error. For example, the traffic density, the flight patterns, the distribution of assigned altitude all play a part in the true position being close to another aircraft at the same flight level. For these reasons, additional models were employed to conservatively estimate the Pe, and for this study, Pe was estimated to be less than $1x10^{-3}$.

The result is that the overall safety objectives are met, because the estimated collision probability is $5x10^{-9}$ times $1x10^{-3}$, or $5x10^{-12}$, which is less than the required value of $5x10^{-10}$.

A similar process was repeated for the other hazards described above in order to derive a complete set of requirements to assure safety of the ADS-B-NRA application.

Conclusions

A process for developing safety analysis for diverse ADS-B based applications has been established through a joint RTCA / EUROCAE working group known as the Requirements Focus Group (RFG). The process includes development of an Operational Hazard Assessment and Allocation of Safety Objectives and Requirements. This work represents the first internationally agreed methodology for analyzing ADS-B based applications, and hopefully will provide a way forward for internationally agreed standards for future applications.

A specific example of the analysis was provided for an air-to-ground ADS-B application, the "Enhanced Air Traffic Services in Non Radar Areas using ADS-B surveillance (ADS-B-NRA). It was shown how the analysis results in requirements on equipment and ground systems that will result in safe operations that can be accepted internationally.

Acknowledgments

The authors wish to acknowledge that this work is the result of the contributions of many people that supported both RTCA and EUROCAE through the committee deliberations. While some of the specific people are mentioned here; many more were involved as well. Specifically Patrick Mana (EUROCONTROL) contributed heavily to the ideas surrounding the general methods and probability calculations; Sorin Muresean and Steve O'Flynn (EUROCONTROL) provided the major portion of the operational expertise that supported these efforts; Jorg Steinleitner (EUROCONTROL) and Stu Searight (FAA) provided committee

leadership, and Stan Jones (MITRE) and John Shaw (QINETIQ) provided the analytic underpinnings of much of the effort.

Much of this material represents a summary of RTCA DO-303/EUROCAE ED-126 Appendix C [22] and has been used with permission from RTCA and EUROCAE. The complete document may be purchased from RTCA, Inc., 1828 L. St, NW, Ste 805, Washington, DC 20036, www.rtca.org, or EUROCAE, 102 Rue Etienne Dolet, 92240 Malakoff, France, www.eurocae.org.

References

[1] RTCA, February 1998, DO-242 Minimum Aviation System Performance Standards for Automatic Dependent Surveillance – Broadcast, Washington, DC, RTCA Incorporated, Revision A (June 2002).

[2] Bone, R., Oscar Olmos, Anand Mundra, Jonathan Hammer, H. Peter Stassen, and Matthew Pollack, 2000, *Paired Approach Operational Concept- Version 7*. MITRE Paper 00W0000210, McLean, VA, The MITRE Corporation Center for Advanced Aviation System Development.

[3] Bone, R., Anand Mundra, and Oscar Olmos, 2001, *Paired Approach Operational Concept*, Proceedings of Digital Avionics Systems Conference 2001.

[4] Abbott, Terence S., 1991, *A Compensatory Algorithm for the Slow-Down Effect on Constant-Time-Separation Approaches*, NASA TM 4285, Hampton, VA, NASA Langley Research Center.

[5] Abbott, 2002, *Speed Control Law for Precision Terminal Area In-Trail Self Spacing, NASA Technical Memorandum 2002-211742,* Langley, VA, National Aeronautics and Space Administration.

[6] Hoffman, E., D. Ivanescu, C. Shaw, and K. Zeghal, 2003, *Effect of Automatic Dependent Surveillance Broadcast (ADS-B) transmission quality on the ability of aircraft to maintain spacing in a sequence*, Air Traffic Control Quarterly, Vol. 11(3) 000–000.

[7] Hoffman, et al, October 2002, *Analysis of Spacing Guidance for Sequencing Aircraft on Merging Trajectories*, Irvine, CA, 21st IEEE/AIAA Digital Avionics Systems Conference.

[8] RTCA, September 2000, *DO-259 Application Descriptions for Initial Cockpit Display of Traffic Information (CDTI) Applications*, Washington, DC, RTCA Incorporated.

[9] Olmos, B. O., Randy S. Bone, and David A. Domino, 2001, 1-7 December 2001, *Cargo Airline Association & Safe Flight 21 Operational Evaluation-2 (OpEval-2)*, Sante Fe, NM, Proceedings of the Fourth International Air Traffic Management Research and Development Seminar, Eurocontrol and FAA.

[10] The MITRE Corporation, 1983, *System Safety Study of Minimum TCAS II*, MTR83W241, McLean, VA, The MITRE Corporation.

[11] McLaughlin, M. and A. Zeitlin, 1992, *Safety Study of TCAS II for Logic Version 6.04*, U.S. Department of Transportation Report DOT/FAA/RD-92/22.

[12] Zeitlin, A., S. Creaghan, and M. Skavicus, 2001, *Comparative Safety Assessment of Collision Avoidance Using TCAS and Conflict Detection and Resolution Using Automatic Dependent Surveillance Broadcast (ADS-B) Airborne Conflict Management (ACM)*, MITRE Technical Report, McLean, VA, The MITRE Corporation.

[13] Hammer, J., 2003, *Safety Analysis of an Approach Spacing System For Instrument Approaches (ASIA) Application Using ADS-B*, Air Traffic Control Quarterly, Vol. 11(3) 000–000.

[14] Rognin, L., Isabelle Grimaud, Eric Hoffman, and Karim Keghal, October 2002, *Impact of Delegation of Spacing Tasks on Safety Issues*, Irvine, CA, 21st Digital Avionics Systems Conference.

[15] RTCA, May 2004, *Safety and Performance Requirements Standard for Initial Air-Traffic DLS In Continental Airspace*, DO-290 / EUROCAE ED-120, Paris, France, EUROCAE, Inc.

[16] RTCA, December, 2003, *DO-289 Minimum Aviation System Performance Standards for Aircraft Surveillance Applications*, Washington, DC, RTCA Incorporated.

[17] MIL-STD-882C, January, 1993, *Military Standard – System Safety Program Requirements*, Washington, DC, US Department of Defense.

[18] FAA, June, 1988, *System Design and Analysis*, Advisory Circular 25-1309A, Washington, DC, Federal Aviation Administration.

[19] FAA, March, 1999, *Equipment, Systems, and Installations in Part 23 Airplanes,"* JAR, Advisory Circular 23-1309C, Washington, DC, Federal Aviation Administration.

[20] RTCA, EUROCAE, December, 2000, *DO-264 / ED-78A Guidelines for the Approval and Use of Air Traffic Services Supported by Data Communications*, Washington, DC, RTCA Incorporated.

[21] FAA, May 2004, *FAA Safety Management System Manual*, Version 1.1, Washington, DC, Federal Aviation Administration.

[22] RTCA/EUROCAE, January 2007, *ED126 / DO-303, Safety, Performance, and Interoperability Requirements for ADS-B NRA Application*, Washington, DC, RTCA/ EUROCAE.

[23] EUROCONTROL, October 2006, *Air Navigation Safety Assessment Methodology – SAF.ET1.ST03.1000 MEN01, V2.1 - October 2006*, Brussels, Belgium, EUROCONTROL.

[24] EUROCAE ED 125 – *To Be Published*, Paris, France, EUROCAE Inc.

Key Words

Safety analysis, non-radar airspace, hazard analysis, Operational Hazard (OH), safety allocation, fault trees, ADS-B.

Biographies

Jonathan Hammer focuses on ADS-B applications development and standards. Mr. Hammer works for MITRE/CAASD where he manages a team of engineers focused on ADS-B. He earned a BSEE degree from Lehigh University, in Bethlehem, Pennsylvania, and an MSEE degree from the University of Maryland in College Park, Maryland.

Gilbert Caligaris joined EUROCONTROL in 1992 after working for Thales and Syseca . He is part of the CASCADE Programme (**C**o-operative **A**TS through **S**urveillance and **C**ommunication **A**pplications **D**eployed in **E**CAC). He is a graduate of ISI (Informatique et Sciences de l´Ingénieur – Sophia Antipolis).

Marta Llobet focuses on ADS-B application safety and operational aspects. She works for Sofréavia where she belongs to a safety and reliability team. Ms. Llobet is a graduate of the French Engineering School of Civil Aviation (ENAC) and is a graduate of the Industrial Engineering University (ETSEIB) in Barcelona.