

Safety Analysis of an Approach Spacing For Instrument Approaches (ASIA) Application Using ADS-B

**Jonathan Hammer
MITRE/CAASD**

Abstract

This paper illustrates new techniques being adopted by some members of industry for analysis of the safety of aircraft surveillance applications. The techniques are illustrated using the example flight deck application of Approach Spacing for Instrument Approaches (ASIA). The techniques include analysis of the operational procedures, conducting a hazard analysis, and treating identified hazards in a fault-tree analysis. The fault-tree analysis in turn results in requirements on various subsystems that support the operational application.

The specific analysis of the approach spacing application results in a requirement that the probability of presenting hazardously misleading information be held to less than 10^{-5} per operation. The 10^{-5} value represents “major” system criticality, and is a criticality that is considered by avionics vendors to be achievable within reasonable cost constraints. If the benefits of reduced spacing that are offered by the approach spacing concept are significant enough to justify the cost, users may find that it is worthwhile to equip their aircraft with such a capability.

Introduction

The application of automatic dependent surveillance broadcast (ADS-B) offers a wide range of potential improvements to air-traffic control operations. Although much work has been done on developing operational applications for the use of ADS-B [Bone 2000, Bone 2001, Bone 2003, FAA 2000, RTCA 1998, RTCA 1999, RTCA 2000, Olmos 2001], analysis techniques that determine requirements to support the safety of these applications are needed. This paper introduces concepts for analyzing the safety of ADS-B applications, focusing on the specific application of “In-Trail Approach Spacing.” The safety analysis reveals that the procedure can be conducted safely with reasonable requirements on the supporting navigation and ADS-B systems.

[Abbott 1991, 2002] reported on potential runway throughput improvements based on an application of ADS-B termed “In-Trail Approach Spacing.” Among the potential benefits offered by ADS-B is the improvement of operations within terminal airspace. A more specific benefit is the improvement of operations on final approach that enables increased runway throughput. In the Approach Spacing for Instrument Approach (ASIA) application, flight crews are given speed guidance during final approach that is intended to reduce inter-arrival variance at the runway threshold. More specifically, a trailing aircraft is given speed guidance to maintain optimal spacing behind a lead aircraft using information transmitted from the lead aircraft via ADS-B.

This paper uses the in-trail approach spacing application as an example to illustrate the safety analysis process that has been developed by some members of industry for ADS-B applications. This analysis makes use of techniques developed by RTCA and articulated in [RTCA 2000]. These techniques are primarily devoted to analysis of communications systems. Recently, RTCA Special Committee 186 and EUROCAE Working Group 51 extended these analysis methodologies to apply to surveillance systems. These modified techniques are described and applied in this paper.

The analysis technique consists of three steps, depicted in Figure 1: (1) identification of operational phases and processes, (2) hazard analysis, and (3) fault-tree analysis. The identification of operational processes entails the designation of each specific input, communication, or action by flight crews or controllers in support of the procedure. Operational phases are constructed by logically grouping sets of operational processes.

In the second step, the analysis identifies potential *operational hazards* associated with each process that can lead to undesirable *operational consequences*. The failure of an operational process, or the completion of that process based on erroneous information, is defined as an operational hazard. Operational consequences are the potential result of the hazards; it is desired to keep the probability of each consequence at or below specific statistical probabilities, in accordance with [FAA 1988]. For example, the rate of mid-air collisions must be controlled to less than 5 collisions per 10^9 flight hours or 10^9 operations.

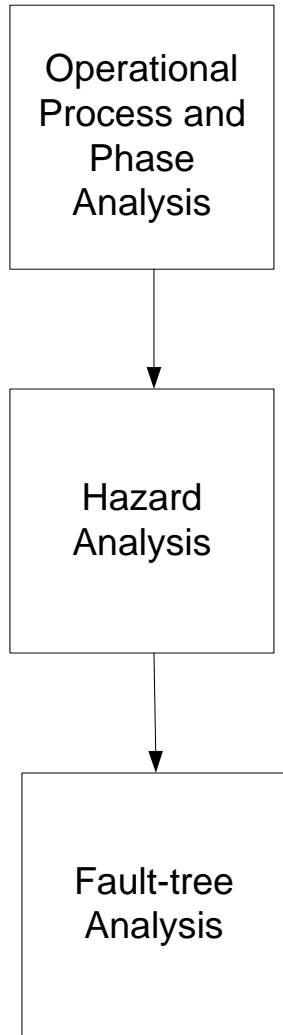


Figure 1. Safety Analysis Process

Determining the statistical probability of the operational consequences through a fault-tree analysis comprises the third and final step of the safety analysis. Operational consequences, identified in the hazard analysis, appear as the top node of the fault trees. The operational hazards, also identified in the hazard analysis, generally appear in the middle or bottom of the fault tree. Working down the fault trees from the operational hazards helps to identify contributory events (the leaves of the fault tree) that can lead to the hazards. Working up the fault trees from the operational hazards leads to the operational consequences. Controlling the probability of the contributory events enables control of the hazards and ultimately control of the probability of the undesirable consequence; the event probabilities then become requirements that are levied on the supporting systems.

The process of the safety analysis is now illustrated through the example of approach spacing. The following sections illustrate the determination of phases and processes for the approach spacing application, then illustrate the hazard identification process, and finally, describe the fault-tree analysis.

Approach Spacing Phases and Processes

Operations supporting the Approach Spacing for Instrument Approaches (ASIA) application can be grouped into four distinct phases, labeled below as P1 – P4; these are:

- P1 Setup for approach spacing procedure,
- P2 Clear for approach spacing procedure,
- P3 Conduct approach spacing procedure,
- P4 Complete approach spacing procedure.

These phases are illustrated in the activity diagram shown in Figure 2, along with the specific responsibilities of both the flight crew and air traffic control.

Phases are further subdivided into processes that are shown in the process diagram of Figure 3. A large rectangular block depicts each phase, while the smaller rectangular blocks represent the processes of each phase.

The setup phase (labeled P1) consists of 8 processes, 7 of which are directly linked. The “ATC Assure Separation” process is a continuous process, based on Air-Traffic Control (ATC) surveillance using secondary radar and is independent of the ADS-B surveillance used in the air-to-air parts of the operation.

Process 1.1 (labeled P1.1) consists of ATC providing standard vectors to an ILS approach. The flight crew prepares as usual for final approach and landing, and performs the additional step of entering the planned final approach speed into the approach spacing system through the Cockpit Display of Traffic Information (CDTI) user interface (P1.2).

In P1.3 ATC provides a call out for the traffic to be followed (labeled TTF in the figure) by the flight crew. The traffic must be identified and selected on the CDTI by the flight crew (P1.4). The flight crew then confirms approach parameters. Once the traffic is identified, the flight crew notifies ATC via an acquisition message (P1.5). If for some reason the traffic can not be identified on the CDTI, the flight crew notifies ATC of an unsuccessful search (P1.6). An unsuccessful search is assumed to result in another search attempt through processes P1.3, P1.4, and P1.5. If the search continues to be unsuccessful, it is assumed that the approach spacing procedure is abandoned, and that normal ATC guidance is provided. The dashed line leading to “revert to standard ATC ops” indicates this outcome.

If the identification process is successful, the crew will be provided with a spacing value by ATC or by an automated lookup based on the weight category of the trail ship and the lead ship (P1.7). (The automated lookup value is based on minimum wake vortex separation standards. ATC, however, might request a larger spacing. This might happen if, for example, ATC desired to leave space in the sequence for a departure on the same runway.)

At this point in the procedure, ATC will provide a clearance to the flight crew to proceed (Phase 2). The flight crew then enters the “conduct approach spacing phase,” (P3), and begins to follow speed guidance cues provided on the CDTI (P3.1). Meanwhile, ATC is expected to continue monitoring the aircraft approach to determine if an unsafe situation is developing (P3.2). The flight crew simultaneously monitors the situation and responds to any alerts issued by the approach spacing system.

If a separation below the minimum wake vortex separation standards is detected by the airborne approach spacing system, an alert is issued to the flight crew and a breakout command is issued. Likewise, if ATC detects an unsafe situation, a command to breakout may be issued by a controller (P3.3). Based on commands from either ASIA or ATC, the flight crew performs a breakout maneuver (P3.4).

If the flight crew follows the guidance provided by the approach spacing system, and that guidance is correct, appropriate spacing will be achieved and phase 4 of the operation, completing the procedure, can proceed. In this case, a clearance for landing is issued by ATC (P4.1), followed by the crew flying the approach at the final approach speed and landing (P4.2). As part of phase 4, ASIA continues to monitor separation (P4.4) and if inadequate spacing is detected, the crew is alerted and may execute a missed approach (P4.3). Note that no active guidance is issued by the approach spacing system after the final approach fix. A command to decelerate to the final approach speed is given at the final approach fix, and it is expected that the flight crew will follow their planned final approach speed through the remainder of the approach.

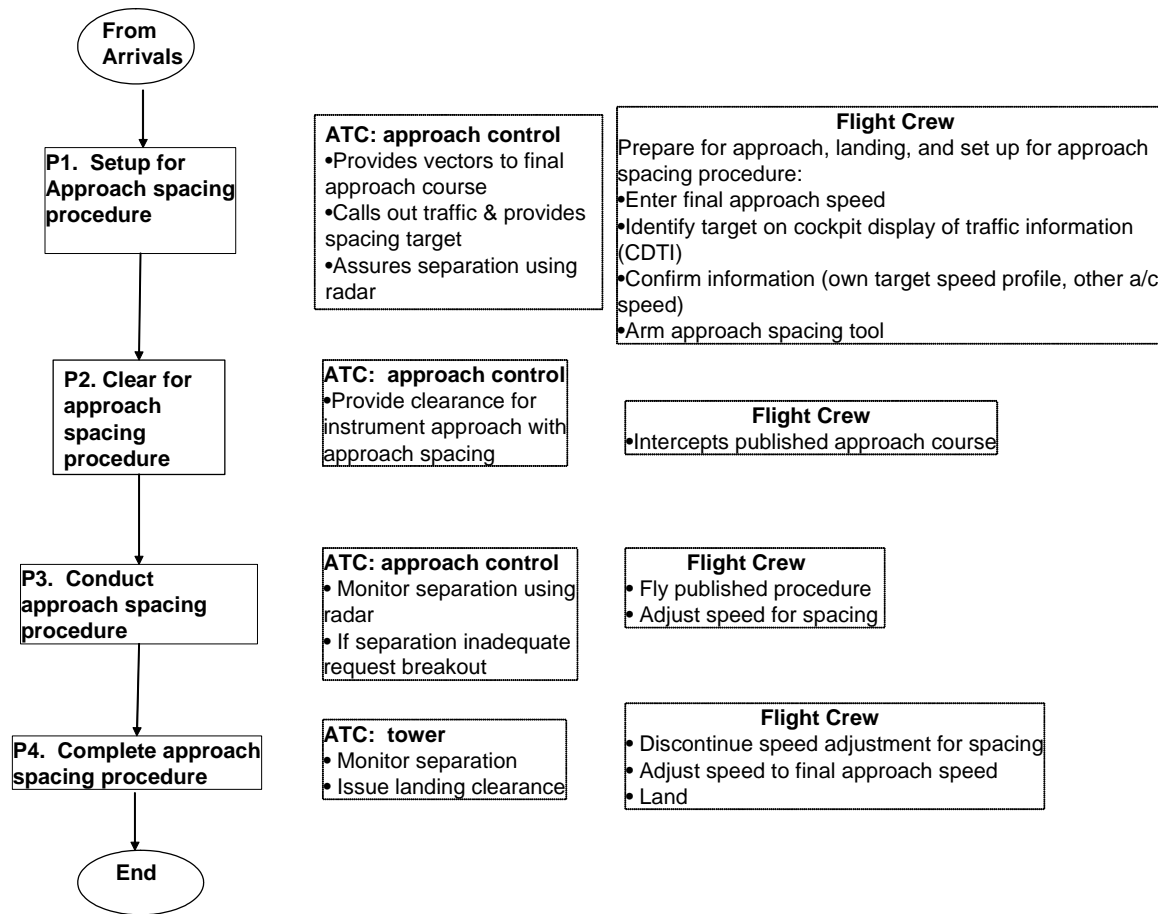


Figure 2. Approach Spacing for Instrument Approach Operational Phases¹

¹ Figure provided courtesy of Mr. William Lee, Boeing Corporation.

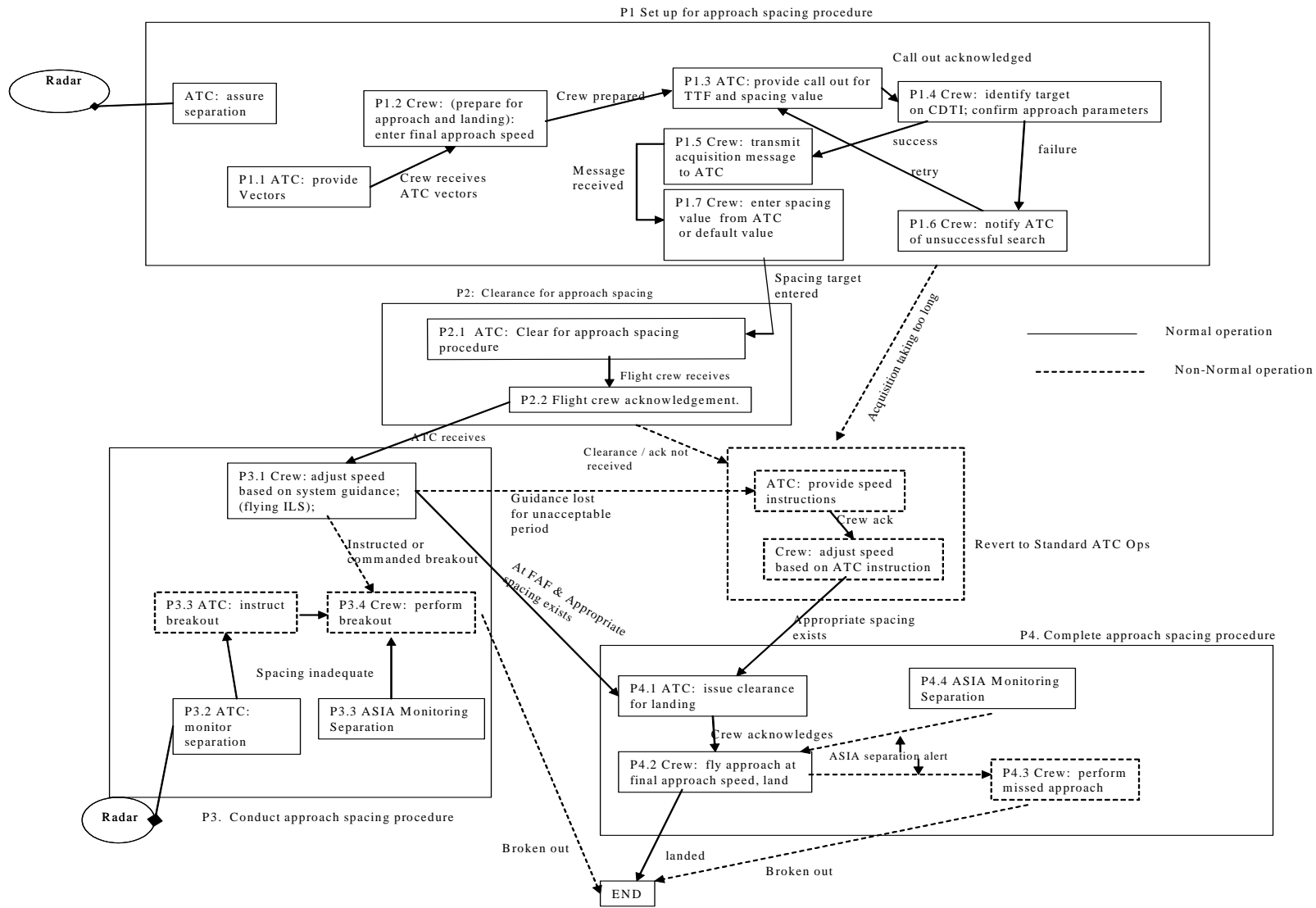


Figure 3. Approach Spacing Processes

1 Operational Hazard Analysis (OHA)

The hazard analysis for ASIA consists primarily of a careful examination for hazards of the phase and process diagrams illustrated above in Figure 2 and Figure 3. Hazards are identified for each process depicted in Figure 3 by posing two hypotheses:

1. The process does not complete normally
2. The process completes based on erroneous information or assumptions.

These two hypotheses form the basis of the hazard analysis that is presented in a safety table (Table 1 below). Each hazard is identified with a unique number relating to the phase and process for reference.

The most notable hazards with ASIA are those in phase 3, where active guidance is being provided to the flight crews. These hazards tend to drive the analysis requirements.

Note the column in the safety table labeled “Potential Operational Consequences.” A consequence of a hazard is not necessarily immediate. A series of events and combinations of hazards is normally required for a consequence to ultimately occur. This series of events and hazards is identified through the fault-tree analysis that is described below. The safety analysis includes, as a mitigation, the intervention of ATC for certain hazards.

Note the column labeled “mitigations/avoidances.” Mitigations are factors that can help to reduce the probability of the hazard from occurring. Avoidances are factors that help to reduce the probability of the operational consequences from resulting once the hazard has occurred. These columns are provided for illustrative purposes and are not exhaustive; the fault-tree analysis described later derives the potential causes of the relevant hazards in detail.

For the purposes of this paper, a few interesting hazards related to phase 3, conducting the approach spacing procedure, are discussed below.

Phase 3 Hazards of ASIA

Phase 3 of the ASIA procedure depends to a large extent on the supporting equipment. This is the most critical phase from the perspective of equipment requirements. The primary process that is of interest to this analysis is the use of the equipment by the flight crew for speed guidance during the approach (P3.1).

Hazard 3.1.1 takes place if the flight crew does not follow the speed guidance; in this case a wake-vortex separation minima violation or a mid-air collision are possible consequences.

Hazard 3.1.2 results if guidance is lost during the procedure. This can occur due to detected equipment failures, and is avoided by requiring minimum equipment continuity. If automated airborne guidance is lost, ATC is expected to provide guidance through the rest of the approach, resulting in what is considered to be a minor increase in ATC workload.

Hazard 3.1.3 results when the ASIA system provides incorrect guidance to the flight crew. This hazard can result in a wake vortex encounter or eventually a mid-air collision. A fault tree containing this hazard will be illustrated in the next section.

Hazards resulting from processes 3.3 and 3.4 are a lack of, or improper execution of, a breakout when instructed. As there is no difference from currently safe existing procedures, there is no safety degradation in executing a missed approach with ASIA. (Note that it is considered a goal of the procedure that no increase in missed approach frequency results from adding the automation).

Phase	Process	Hazard ID	Operational Hazard Description	Potential Operational Consequence	Avoidances / Mitigations
P1: Setup	P1.1 (ATC provides vectors)	H1.1.1	Identical to current operational procedure		
	P1.2 Crew: prepare for approach and landing; enter final approach speed	H1.2.1	No approach speed entered	ASIA fails to engage; Revert to current operational procedure	Crew training
		H1.2.2	Erroneous approach speed entered	Wake vortex encounter Mid-air collision with lead a/c	<ul style="list-style-type: none"> • System check on reasonable approach speed • ASIA separation alert • ATC intervention
	P1.3 ATC: provide callout for traffic to follow	H1.3.1	Erroneous traffic call out	Wake vortex encounter Mid-air collision with lead a/c	<ul style="list-style-type: none"> • Training • ASIA separation alert • ATC intervention
		H1.3.2	Loss of traffic call out	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements
	P1.4 Crew: identify lead traffic on CDTI	H1.4.1	Lead traffic not found by crew	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Integrity and continuity requirements
		H1.4.2	Lead traffic misidentified by crew	Wake vortex encounter Mid-air collision with lead a/c	<ul style="list-style-type: none"> • ASIA separation alert • ATC intervention
	P1.5 Crew: transmit acquisition	H1.5.1	Loss of acquisition message	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements
		H1.5.2	Erroneous acquisition message	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements
	P1.6 Crew: notify ATC	H1.6.1	Loss of notification of unsuccessful search	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements

Phase	Process	Hazard ID	Operational Hazard Description	Potential Operational Consequence	Avoidances / Mitigations
P1: Setup	P1.6 Crew: notify ATC of unsuccessful search	H1.6.2	Erroneous notification of unsuccessful search by crew	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements
		H1.6.3	Delayed notification of unsuccessful search by crew	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements
	P1.7 ATC: provide spacing value, crew, enter spacing value	H1.7.1	Spacing value not received	Revert to current operational procedure	<ul style="list-style-type: none"> • Communications systems requirements
		H1.7.2	Spacing value miscommunication	Wake vortex encounter Mid-air collision with lead a/c	<ul style="list-style-type: none"> • Training • ASIA separation alert • ATC intervention
		H1.7.3	Crew fails to enter spacing value	ASIA fails to engage; Revert to current operational procedure	Crew Training
		H1.7.4	Crew enters incorrect spacing value	Wake vortex encounter Mid-air collision with lead a/c	<ul style="list-style-type: none"> • Training • ASIA separation alert • ATC intervention
	P2: Clearance for procedure	P2.1 Controller issues clearance	H2.1.1	Loss of clearance for ASIA	Revert to current operational procedure
P2.2 Flight crew accepts clearance		H2.1.2	Erroneous clearance for ASIA	Revert to current operational procedure)	<ul style="list-style-type: none"> • Training • Communications systems requirements
		H2.2.1	Loss of flight crew acknowledgement of clearance for ASIA	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements
		H2.2.2	Erroneous acknowledgment of ASIA clearance by flight crew	Revert to current operational procedure	<ul style="list-style-type: none"> • Training • Communications systems requirements
		P3: Conduct Procedure	P3.1 Crew: adjust speed based on system commands	H3.1.1	Erroneous speed maintained by flight crew
H3.1.2	Loss of guidance during ASIA procedure			Revert to current operational procedure	Continuity Requirements
H3.1.3	Erroneous guidance during ASIA procedure			Wake vortex encounter Mid-air collision with lead a/c	Integrity Requirements
P3.2 ATC: monitor separation	Identical to current operational procedure				

Phase	Process	Hazard ID	Operational Hazard Description	Potential Operational Consequence	Avoidances / Mitigations
P3: Conduct Procedure	P3.3 ATC: Instruct breakout	Identical to current operational procedure			
	P3.4 Crew: perform breakout	Identical to current operational procedure			
P4: Complete approach spacing procedure	P4.1 ATC: issue clearance for landing	Identical to current operational procedure			
	P4.2 Crew: fly final approach speed and land	Identical to current operational procedure			
	P4.3 Crew: execute missed approach	H4.3.1	Unnecessary missed approach due to ASIA	Identical to current operational procedure. The major impact is on performance since an unnecessary missed approach is conducted.	ATC vectors
		H4.3.2	Missed approach necessary but not started	Wake vortex encounter midair collision with lead a/c	ATC monitoring

Table 1. Operational Hazard Analysis for Phase 1 of ASIA

2 Fault-Tree Analysis

Two potential operational consequences of significant criticality that are identified above in the hazard analysis are:

1. Wake vortex encounter
2. Mid-air collision.

A significant wake-vortex encounter, i.e., an encounter that can cause a serious aircraft upset resulting in incapacitation of the flight crew, serious injury, or possible death of several aircraft occupants is a severe-major failure requiring a probability less than the order of 10^{-7} per operation as per [FAA 1988]. A mid-air collision is considered catastrophic; the probability is required to be less than the order of 10^{-9} per operation.

The fault-tree analysis of these two operational consequences helps to derive some system requirements. For the purposes of illustrating the techniques, only the analysis of the wake-vortex encounter will be treated in this paper. Note that this analysis was completed based on the assumption that the approach spacing application will last approximately 15 minutes. This is based on an assumption of a 30 NM final approach segment flown at a speed of 125 knots.

Fault-Tree Analysis of Wake Vortex Encounter

The fault-tree analysis begins with an examination of the likelihood of a damaging wake vortex encounter during an approach. Figure 4 presents the high-level fault tree for this consequence. The figure and the associated analysis and requirements described below illustrate that a 10^{-7} per operation failure rate is achievable based on reasonable system requirements.

The notation of the fault-tree figures follows standard logic notation for “and” and “or.” The circles in the figures represent basic events, i.e., the “leaves” of the trees, and triangles represent sub-trees. Note that there are two kinds of triangles: small ones which are extended out from the top or middle of a gate, indicating that what lies below is a sub-tree of some event or gate on another page, and larger ones with a box around them, indicating the further expansion of this part of the fault tree can be found on another page. Some additional notes on the fault trees:

- A given event in the diagrams may have either a fixed probability Q or a failure rate r associated with it.
- The gates will have probabilities Q associated with them, which are calculated based on the specified rates or probabilities for the basic events below the gate.
- The relationship between Q and r is $Q = 1 - e^{-rt}$, where t is the exposure time, taken in this paper to be 15 minutes, or .25 hour. This relationship corresponds to an exponential distribution (constant failure rate) of the time to failure of a component, or the time to occurrence of some event.

What is derived through the analysis provides the basis for sufficient, but not necessary, conditions to achieve the required criticality to prevent a wake encounter, i.e., other combinations of system requirements could possibly achieve the same goal.

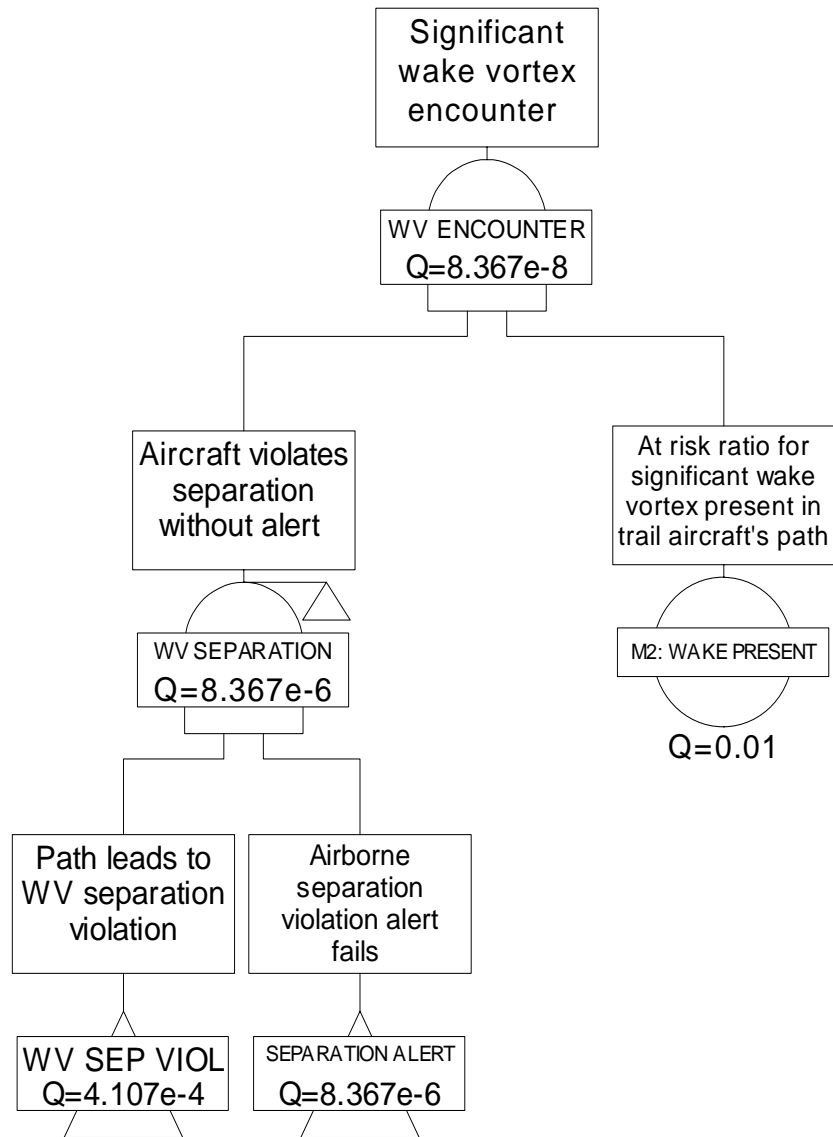


Figure 4. High Level Fault Tree for Wake Vortex Encounter Analysis

The top two gates of Figure 4 illustrate that a damaging wake vortex encounter can occur only when the trail aircraft violates the separation minima and there is a significant wake vortex present to upset the aircraft. Since the ASIA system is designed to avoid wake vortex separation violations, a significant separation violation only occurs if there are unexpected system or operational errors and an airborne violation alert fails.

Although, as indicated in Figure 3, air-traffic control plays a significant monitoring role in the procedure, the analysis specific to a wake vortex encounter assumes no mitigation due to air-traffic control. The reason for this is that the analysis assumes that a wake vortex encounter could take place shortly after a separation violation; it is assumed that

ATC has no responsibility to notice the violation. ATC monitoring is intended to cover more egregious errors that might lead to a possible collision or a runway occupancy problem. The responsibility for avoiding a wake vortex separation violation is assumed to be on the airborne side, i.e., via airborne alerts generated by ASIA.

Another important assumption is the probability of a significant wake being in the trail aircraft's path (the "at risk ratio") Our assumption is that the wake vortex separation that the flight crews have to maintain is numerically equal to the separation that air-traffic control currently has to maintain on approach. Due to the uncertainty of this event, a very conservative number of 10^{-2} was adopted. This assumption was not validated analytically but was derived based on interviews with line pilots. The consensus of the flight crews who discussed this was that 10^{-2} is an extremely conservative assumption.

Another approach indicating that this number is conservative is to recognize that during visual approaches today, the wake vortex minima are generally not applied, and aircraft fly well inside these standards, in many cases, as close as 2 nautical miles in trail (for large aircraft following other large aircraft). If the probability of a wake vortex encounter involving incapacitation of the flight crew or serious injury or deaths to passengers was as high as 0.01, it is likely that there would be dozens of injuries and possibly several deaths each week in the US from hazardous wake vortex encounters during the thousands of visual approaches that take place each day. It is noted, however, that this is one key assumption of the analysis that will need further validation before certification and operational approvals for ASIA can take place.

This at risk ratio requires that operational and system errors be held to 10^{-5} or lower. This value is achievable through a combination of system requirements on guidance, error checking, and alerting. As shown on the left hand side of Figure 4, the analysis assumes that a separation violation occurs when a path that leads to the violation is generated and there is no alert to the flight crew of the violation. It is therefore necessary to have an alert for separation violations, as shown in the figure, as a mitigation to other potential system failures. The failure sub-trees for the operational/system errors and the alert are further analyzed below.

Note that the overall probability of the AND gate labeled "aircraft violates separation without alert" does not equal the multiplicative probability of the two gates below it. This is because the two gates feeding this AND gate are not independent (they contain "common mode" failures). The analysis proceeds to develop the sub-trees that could create a wake vortex separation minima violation; that is, the generation of a path that leads to a separation violation and the failure of the separation violation alert.

Failures Leading to Wake Vortex Encounter Path

Figure 5 shows the fault tree for the left-most branch of Figure 4. The tree is broken into two parts: misleading guidance that results in a path leading to a separation violation (also seen in the hazard analysis as Hazard 3.1.3), and operational errors. Requirements on equipment integrity generally are derived from the left hand sub-tree. Assumed human performance and potential system mitigations for human and operational errors

are contained in the right sub-tree. The sub-tree for misleading guidance is presented in Figure 6, and the sub-tree for operational errors is presented in Figure 7.

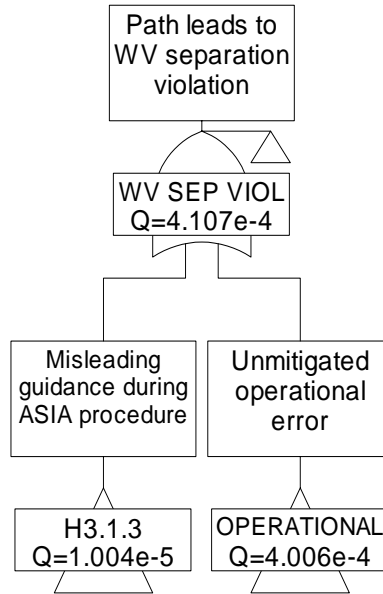


Figure 5. Operational / System Errors Lead to Path That Violates WV Separation Minima

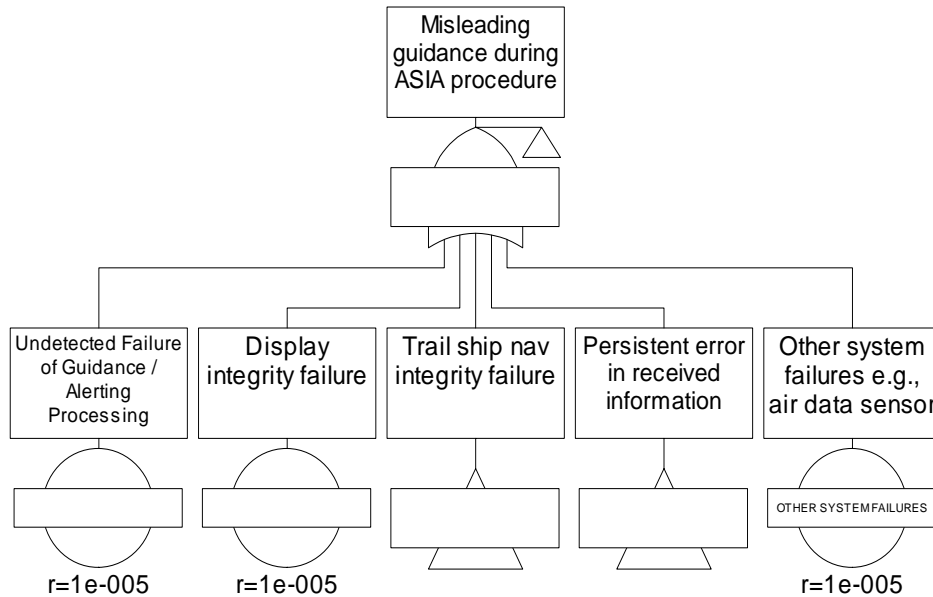


Figure 6. Fault tree for misleading guidance

Misleading Guidance

Figure 6 illustrates the sub-tree for misleading guidance. The leftmost event in the sub-tree is an undetected integrity failure of the guidance processing that results in hazardously misleading guidance. The failure probability is indicated as being 10^{-5} , corresponding to “major” criticality [FAA 1988]. The failure probabilities of the leaf system events are assigned appropriate probabilities in order to assure that the top level event probability (in this case a wake vortex encounter) meets its required probability.

Similarly, the event second from the left indicates an integrity failure of the display system that could lead to hazardous guidance. The display system is the primary interface of ASIA to the flight crew, and indicates the speed guidance to the crew.

The third event from the left is an integrity failure of the navigation system on the trail ship. Navigation information for the trail ship is used to derive the guidance for ASIA.

The branch that is fourth from the left illustrates the faults that result in a persistent error in information transmitted from the lead ship to the trail ship. The information includes state vector information from the lead aircraft that is transmitted to the trail aircraft via ADS-B, containing the lead aircraft's position and velocity. The data also includes plan data, such as the planned final approach speed from the lead ship. This data is fundamental to the speed guidance that is derived for the trail-ship's flight crew to follow.

Finally, integrity failures of other systems that are used to derive information for ASIA are indicated in the rightmost event of Figure 6.

Trail Ship Navigation Failure

Figure 7 illustrates the sub-tree for a trail-ship navigation integrity failure. In this tree there are two bottom level events: an integrity failure of the trail ship's navigation and an area-wide navigation integrity failure. The single ship failure represents an integrity failure of the trail ships' on board navigation system. This failure is assumed to take place with a rate of 10^{-5} per hour. An area navigation failure is a common mode failure with the lead ship, such as an undetected failure of a GPS satellite, and the same failure is included in the fault tree for state vector integrity (Figure 8). An area navigation failure affecting both the lead and trail ship is assumed to occur with a frequency that is two orders of magnitude lower than a single ship failure, i.e., with a per operation rate of 10^{-7} . This is consistent with signal in space integrity requirements for GPS, WAAS, and LAAS [ICAO 2000]. The total of the trail ship's navigation system integrity failure results in a per hour integrity failure rate of 1.01×10^{-5} .

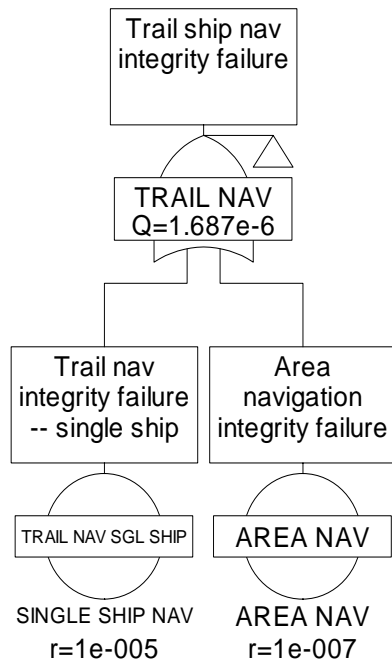


Figure 7. Fault Tree for Navigation Integrity Failure of Trail Ship

Persistent Error In Received Information

A persistent error on the lead ship can disrupt the trail ship’s guidance. State vector and plan data is transmitted from the lead ship to the trail ship via ADS-B. The state vector can be corrupted by a navigation integrity failure of the lead ship, or by corruption introduced by ADS-B itself, and the plan data may be corrupted by ADS-B.

Figure 8 illustrates the fault tree for an error in the received information. Note that the left hand sub-tree (lead ship navigation integrity failure) is nearly identical to the sub-tree for a navigation integrity failure of the trail ship (Figure 7). The difference between the lead ship and trail ship navigation integrity failure is the single ship failure event on the bottom left of Figure 7 and Figure 8. The event labeled “area navigation integrity failure” is a common-mode failure for both ships and is treated as such in the calculations of the overall failure probabilities.

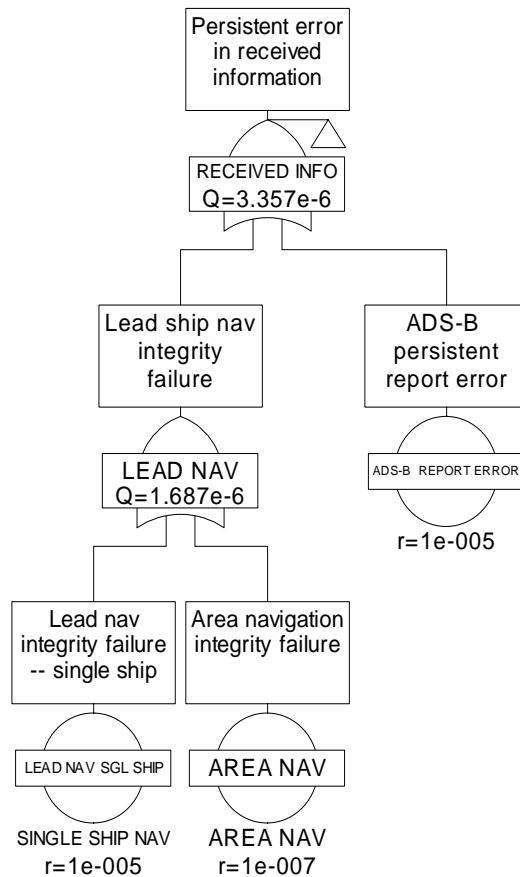


Figure 8. Fault Tree for Persistent Error in Received Information

Unmitigated Operational Error

In addition to accounting for possible system failures, the analysis conducted for ADS-B applications includes consideration of operational failures. The hazard analysis described above included potential errors during the operational procedure that should be considered in a complete safety analysis. The hazards included in the hazard table relevant to a wake vortex encounter are included in the fault tree of Figure 9.

Starting with the left branch in the fault tree of Figure 9, the first potential failure shown is the introduction of an incorrect spacing value to the system. This can take place as a result of hazard 1.7.2 (spacing value miscommunication), or hazard 1.7.4 (crew enters incorrect spacing value). It is recommended that an error check be conducted on the entered value, as indicated in the fault tree, in order to reduce the likelihood that an incorrect value is used by the system.

Our assumptions are that the probability of a human error is on the order of 10^{-2} per communication or data entry. The human error rates are based on estimates [Ashford 2003] based on historical data [Cardosi 1993, 1994, 1996, 2001] for controller-pilot communications.

Moving to the right, the next two branches of Figure 9 cover the possibility that an incorrect value is entered for the approach speed of either the lead or trail aircraft. Error checks on the entered approach speed are required, but are assumed to be far from perfect, with a 10^{-2} error probability.

Finally, the right-most branch of the fault tree of Figure 9 indicates a failure of the flight crew to properly follow the ASIA systems advised speed. A requirement to alert the crew in the event that there is a discrepancy is indicated by the event labeled “crew speed warning system failure.” Although the warning system integrity is likely to be certified to a high integrity (e.g., 10^{-5}), it is assumed that the detection of a discrepancy between the commanded speed and the flown speed has associated failure modes that are unrelated to the certification of the system and occur with higher frequency.

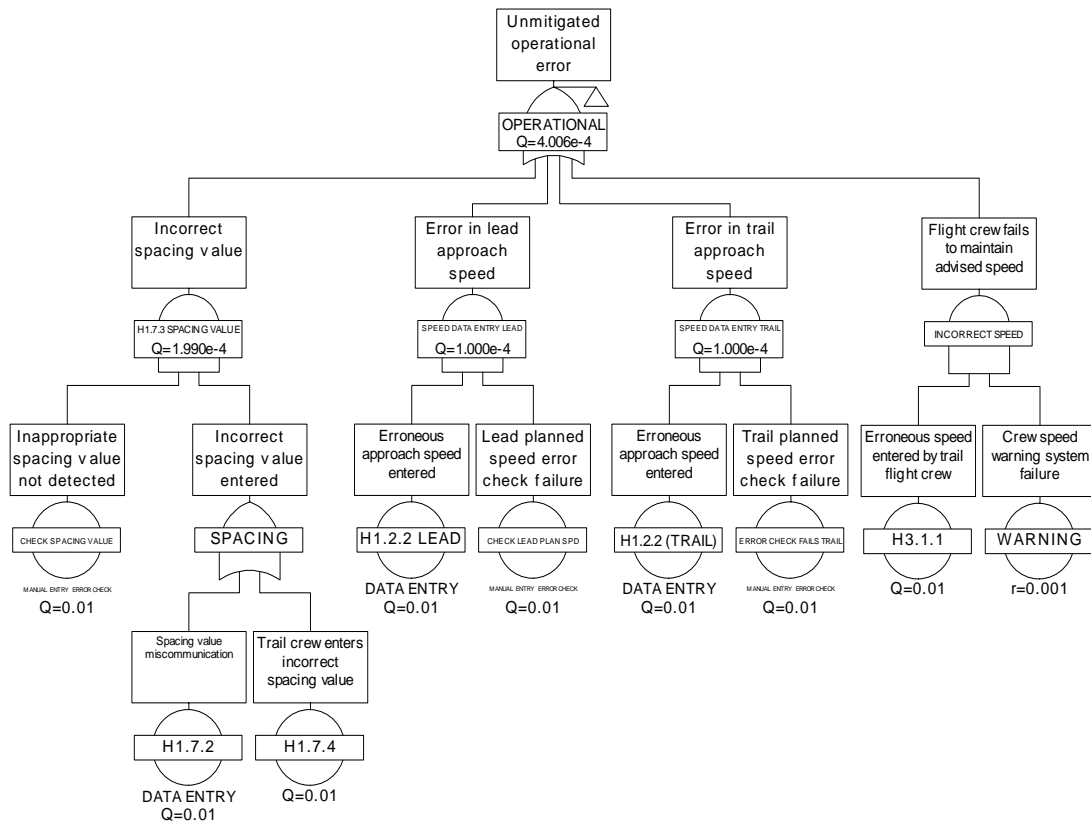


Figure 9. Fault tree for unmitigated operational error

Failure of the Airborne Separation Violation Alert

The failure of the airborne separation violation alert was identified in the first fault tree depicted in Figure 4. Examining Figure 4, observe that an essential mitigation to a wake vortex separation minima violation is that the violation is detected by on-board systems. It is assumed by this analysis that when such a violation is detected an alert is issued to the flight crew and that the minimum separation is promptly reestablished. It is assumed that this sequence of events will avoid a wake vortex encounter provided that the alert is issued before a large violation of the wake vortex minima takes place.

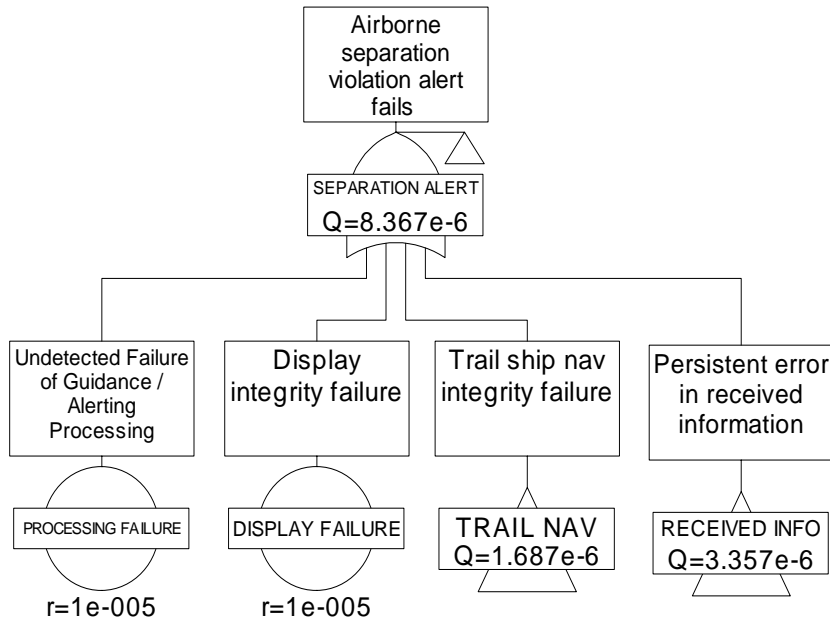


Figure 10. Fault Tree for Airborne Separation Violation Alert Failure

The fault tree of Figure 10 illustrates the failure mechanism for the airborne separation violation alert. The alert is based on current position estimates for both the lead and trail aircraft. Sources of failure include state vector information from the lead aircraft and navigation information from the trail aircraft. In addition, the analysis presumes a failure of the alerting algorithm itself occurs with a 10^{-5} failure rate. The error in received information and navigation integrity failures are common mode failures with the operational and system errors considered earlier. These common mode failures are included in the calculation of the top-level event of a wake vortex encounter shown in Figure 4.

3 Conclusions

This paper has illustrated new techniques being adopted by some members of industry, represented by RTCA, for analysis of the safety of aircraft surveillance applications. The techniques include an analysis of the operational procedures, breaking these procedures into phases and processes, conducting a hazard analysis, and treating the identified hazards in a fault-tree analysis. The fault-tree analysis in turn results in system

requirements on various subsystems that support the operational application.

Observing the fault trees presented in the specific analysis of the approach spacing application, it is notable that the system errors that can lead to a wake-vortex encounter need to be controlled to a level not to exceed 10^{-5} per operation. The 10^{-5} value represents the probability that hazardously misleading information is provided, during an approach spacing operation, from one of the systems represented at the bottom level of the fault trees, for example, a failure of the lead or trail ship's navigation system, or a persistent error in the ADS-B system's report information. The 10^{-5} value can alternatively be thought of as the system integrity. In essence, this value dictates the required certification level of the hardware and software that will make up the approach spacing system components; the 10^{-5} value represent a "major" level criticality, and consequent requirements on software and hardware assurance are specified by FAA.

The major level criticality is one that is considered by avionics vendors to be achievable within reasonable cost constraints. If the benefits of reduced spacing that are offered by the approach spacing concept are significant enough to justify the cost, users may find that it is worthwhile to equip their aircraft with such a capability.

ACKNOWLEDGEMENTS

This work is the result of the efforts and deliberations of many individuals involved in RTCA Special Committee 186 and EUROCAE Working Group 51. The techniques developed here, particularly the development of the activity diagrams, the identification of hazards associated with the diagrams, and the fault-tree process all resulted from numerous and lengthy committee meetings that involved members from industry organizations both in the US and Europe. The author would especially like to thank his co-chair of RTCA SC186 Working Group 4, Stephan Koczo, for his unfaltering support and patience with these efforts.

This work was produced for the US government under contract number DTFA01-01-C-00001. The contents of this material reflect the views of the author. Neither the Federal Aviation Administration nor the Department of transportation, makes any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein.

LIST OF REFERENCES

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

Abbott, Terence S. (2002), *Speed Control Law for Precision Terminal Area In-Trail Self Spacing*, NASA Technical Memorandum 2002-211742, National Aeronautics and Space

Administration, Langley, VA.

Ashford (2003), *Communication and Input Errors for Spacing Applications*, RTCA SC186 Working Group 4 Paper #2003-SC186-WG4-1, April, 2003.

Bone, R., Olmos, O., Mundra, A., Hammer, J., Stassen, H. P., and Pollack, M. (2000), *Paired Approach Operational Concept- Version 7*. MITRE Paper 00W0000210, The MITRE Corporation Center for Advanced Aviation System Development, McLean, VA.

Bone, R., Mundra, A., and Olmos, O. (2001), *Paired Approach Operational Concept. Proceedings of Digital Avionics Systems Conference 2001*, Daytona Beach, FL.

Bone, R., Helleberg, J., and Domino, D. (2003) (in preparation). *Safe Flight 21 Ohio River Valley MITRE CAASD Flight Simulations: Approach Spacing and Surface Moving Map Preliminary Findings*. MITRE Paper, The MITRE Corporation Center for Advanced Aviation System Development, McLean, VA.

Cardosi, K. 1993. *An analysis of en route controller-pilot voice communications*. DOT/FAA/RD-94/15, Cambridge, MA.

Cardosi, K. 1994. *An analysis of tower (local) controller-pilot voice communications*. DOT/FAA/RD-93/11, Cambridge, MA.

Cardosi, K., Brett, B., and Han, S. 1996. *An analysis of TRACON (Terminal Radar Approach Control) controller-pilot voice communications*. DOT/FAA/AR-96/66, Cambridge, MA.

Cardosi, K., and Yost, A. 2001. *Controller and Pilot Error in Airport Communications: A Review of Previous Research and Analysis of Safety Data*. DOT/FAA/AR-00/51, Cambridge, MA.

FAA (1988), Advisory Circular Number 25-1309, *System Design and Analysis*, US Department of Transportation, Washington, DC.

FAA (2000). *SafeFlight 21 Master Plan, version 2.0, April, 2000*, Department of Transportation Federal Aviation Administration Safe Flight 21 Program Office, AND-510, Washington, DC.

ICAO Annex 10 (2000) *Aeronautical Telecommunications. Volume I (Radio Navigation Aids)*, Montreal, Canada.

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

RTCA (1998). *Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)*, Document No. RTCA/DO-242, Washington, DC.

RTCA (1999). *Development and Implementation Planning Guide for Automatic Dependent Surveillance – Broadcast (ADS-B) Applications* RTCA/DO-249, RTCA, Washington, DC.

RTCA (2000). *Application Descriptions for Initial Cockpit Display of Traffic Information (CDTI) Applications*, Document No. RTCA/DO-242, Washington, DC.

RTCA (2000), *Guidelines for the Approval of the Provision and Use of Air Traffic Services Supported by Data Communications*, RTCA DO-264, RTCA Inc., Washington, DC.

BIOGRAPHY

Jonathan Hammer has been involved in the analysis of air-traffic control surveillance requirements and procedure development for approximately 20 years. Mr. Hammer has developed algorithms, requirements, and analysis of operational procedures for air-traffic control multi-sensor tracking, TCAS, and ADS-B. Mr. Hammer is co-chairman of RTCA Special Committee 186's Airborne Surveillance Requirements working group, and is the secretary for the committee's plenary (special committee 186 develops requirements for ADS-B). Mr. Hammer holds three US patents for Air-Traffic related developments, one of which was for the invention of a horizontal miss distance filter for TCAS. Mr. Hammer has been an employee of the MITRE Corporation for the past 10 years.