NASA/TM–2016-219176

Preliminary Assessment of Operational Hazards and Safety Requirements for Airborne Trajectory Management (ABTM) Roadmap Applications

William B. Cotton and Robert Hilb
National Institute of Aerospace, Hampton, Virginia

Stefan Koczo, Jr.
Rockwell Collins, Inc., Cedar Rapids, Iowa

David J. Wing
Langley Research Center, Hampton, Virginia

March 2016

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question to help@sti.nasa.gov

- Phone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM–2016-219176

Preliminary Assessment of Operational Hazards and Safety Requirements for Airborne Trajectory Management (ABTM) Roadmap Applications

William B. Cotton and Robert Hilb
National Institute of Aerospace, Hampton, Virginia

Stefan Koczo, Jr.
Rockwell Collins, Inc., Cedar Rapids, Iowa

David J. Wing
Langley Research Center, Hampton, Virginia

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

March 2016

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Table of Contents

1. Introduction 1
2. Approach to Safety Assessment 2
   2.1 Method 1 Safety Assessment 2
   2.2 Method 2 Safety Assessment 2
      2.2.1 Perform an Operational Hazard Assessment (OHA) 3
      2.2.2 Allocate Safety Objectives and Safety Requirements 3
3. Trajectory Change Requests – Today's Operations 3
4. ABTM Application Roadmap High-Level Descriptions 4
   4.1 ABTM 1 – Basic TASAR 4
   4.2 ABTM 2 – Digital TASAR 5
   4.3 ABTM 3 – 4D TASAR 6
   4.4 ABTM 4 – Strategic ABTM 6
   4.5 ABTM 5 – Full ABTM 7
5. Airborne Trajectory Management "Intended Function" Descriptions 7
   5.1 Basic TASAR - Intended Function Description 7
   5.2 Digital TASAR – Intended Function Description 8
   5.3 4D TASAR – Intended Function Description 8
   5.4 Strategic ABTM – Intended Function Description 9
   5.5 Full ABTM – Intended Function Description 9
6. Method 1 Safety Analysis – Conventional Method 10
   6.1 Key Factors that Influence FEC of ABTM 1-4 10
   6.2 Failure Effects Classification 11
   6.3 ABTM 1-3 Applications Internal Mitigation Means 13
   6.4 Procedural Mitigations Available to the Pilot 13
   6.5 ABTM 1-4 Phase of Flight Considerations 14
   6.6 ABTM 1-3 Information Source Quality 14
   6.7 ABTM 1-3 Undetected Failure – Worst Case Effect 14
7. Method 2 Safety Analysis – Operational Safety Assessment Process 15

7.1 Operational Hazards Identification 17
7.1.1 Human Actions Potentially Leading to Abnormal Events 18
7.1.2 ABTM Automation Processing Actions Potentially Leading to Basic Causes 19
7.2 Potential Basic Causes for ABTM 1-3 – Detailed Assessment 19
7.3 Detailed List of Potential ABTM 1-3 Operational Hazards 20
7.4 Operational Hazards Identification, ABTM 4 21
7.5 ABTM Automation Processing Actions Potentially Leading to Basic Causes 21
7.6 Operational Hazards Identification, ABTM 5 22
7.6.1 Human Actions Potentially Leading to Abnormal Events 22
7.6.2 ABTM 5 Automation Processing Actions Potentially Leading to Basic Causes . 22
8. Summary 23
9. References 24

1. Introduction

This report presents the preliminary safety assessment of an Airborne Trajectory Management (ABTM) roadmap of applications [1]. In prior work, a set of five developmental steps building from the NASA TASAR (Traffic Aware Strategic Aircrew Requests) concept were described, each providing incrementally more efficiency and capacity benefits to airspace system users and service providers leading to a Full Airborne Trajectory Management capability. ABTM 1 is referred to as Basic TASAR, an Electronic Flight Bag (EFB) hosted optimization application described in [2] and [3]. ABTM 2 is referred to as Digital TASAR and adds data communications (including Data Comm) to Basic TASAR used in the request to Air Traffic Control (ATC) for trajectory change and for the re-clearance. ABTM 3 is referred to as Four Dimensional (4D) TASAR and adds the longitudinal element permitting optimization in route, altitude, and speed. ABTM 3 also permits airline network optimization to be considered and coordinates the time along track with the Federal Aviation Administration (FAA) TBFM (Time Based Flow Management) and FIM (Flight Deck Interval Management) capabilities when those procedures are available in the ground system. ABTM 4 is referred to as Strategic ABTM and capitalizes on the experience using ABTM 1-3 to justify sending future trajectory changes from the aircraft directly to the enroute automation system simultaneously with entering them into the Flight Management System (FMS). Because separation responsibility remains with the controller in ABTM 4, these changes must originate no closer than the next sector beyond the one currently occupied. ABTM 5 is Full Airborne Traffic Management and, as described in [4] and [5], incorporates the separation functions, both tactical and strategic, to provide full time flight guidance along de-conflicted, optimized trajectories. For each step in the roadmap, the incremental Operational Hazards and Safety Requirements are identified in this report for use in future formal safety assessments intended to lead to certification and operational approval of the equipment and the associated procedures. The assessments of this report are consistent with two safety assessment methodologies that are compliant with the FAA's Safety Management System:

Method 1: A traditional safety assessment identification of hazards for the Intended Function of the system being developed, determination of worst credible effect due to the hazard, and subsequent Failure Effects Classification using ARP 4761 [6], AC 25-1309 [7] and AC 23-1309 [8] for Part 23 and Part 25 aircraft operations.

Method 2: RTCA DO-264 / EUROCAE ED 78A Operational Safety Analysis [9].

Section 2 of this report provides a high-level description and assessment of the two safety methodologies. Section 3 reviews the processes used today to define and fly a business-case flight trajectory to the extent permitted in current air traffic operations. Section 4 provides a high-level overview and description of the concept of operations for each of the five steps in the ABTM roadmap. Section 5 describes the intended functions of the ABTM applications whose safety cases are evaluated. Section 6 presents the safety assessments using Method 1. Section 7 performs the assessments using Method 2. Section 8 provides a report summary, followed by a list of references in Section 9.

2. Approach to Safety Assessment

Two safety assessment approaches were used to determine the anticipated Failure Effects Classifications (FEC) for the ABTM roadmap applications, building on a similar analysis performed for Basic TASAR [10]. These FECs are based on Operational Hazards and available mitigations that are identified using these two methods. As will be shown in this report, both safety analyses conclude that the worst case FEC for ABTM 1-3 will likely be No Effect and no higher than Minor. ABTM 4 will likely be Minor, and ABTM 5 will likely be Major. These assessments are likelihoods based on the preliminary analysis performed here. The final determinations are subject to evaluation and approval by cognizant FAA certification and operational approval organizations responsible for authorization of these applications. Supporting rationale for these designations is provided in the safety assessments in Sections 6 and 7.

2.1 Method 1 Safety Assessment

Method 1 represents the traditional system safety process for airborne systems and equipment, e.g., TASAR. This method performs the following steps relative to the Intended Function of the new system capability:

1) Evaluate the Intended Function per phase of flight
2) Identify failure events, e.g., loss of function; undetected, erroneous Trajectory Change Requests
3) Examine the effect of these failures on aircraft, pilot (or flight crew), and ATC
4) Determine the Hazard Classification, e.g., Major, Minor, No Effect
5) Determine frequency of occurrence, e.g., per flight hour, per operation
6) Provide rationale for hazard assessment.

2.2 Method 2 Safety Assessment

Method 2 represents a system-of-systems analysis approach that is well-suited for allocating safety requirements across a multiple-system function. This allows a more balanced allocation of safety requirements across systems and sub-systems, which is particularly beneficial for higher criticality systems. While an excellent approach for systems analysis, it is not as well suited for lower criticality systems such as ABTM 1-3. This is particularly true in the realm of “Minor” criticality systems, where this approach puts excessive emphasis on formal analysis related to operational effects such as workload (pilots and air traffic controllers), which are often highly subjective and difficult to assess in a quantitative manner. The method is better suited to an analysis of ABTM 4-5 in which trajectory modifications are made without first obtaining explicit ATC approval.

Method 2 employs the following evaluation steps:

2.2.1 Perform an Operational Hazard Assessment (OHA)

a. Identify Operational Hazards

b. Determine the worst credible outcome of the Operational Hazard, i.e., the Operational Effect, e.g., collision, loss of separation, workload

c. Determine the Severity Classes for each Operational Effect, e.g., Catastrophic, Major, Minor, and identify the maximum allowable probability of occurrence of the Operational Effect

d. Determine the Effects Probabilities, which represent the probabilities of available mitigations to the system to help reduce the probability of occurrence of the Operational Effect due to the Operational Hazard

e. Assign Safety Objectives, which represent the probability of occurrence of each Operational Hazard that is allowable for ensuring the safety of the application

f. Identify External Mitigation Means, i.e., barriers external to the application that reduce the adverse effects and impact to safety when Operational Hazards occur.

2.2.2 Allocate Safety Objectives and Safety Requirements

a. Identify Abnormal Events and Basic Causes internal to the applications that could lead to the occurrence of each Operational Hazard

b. Identify Internal Mitigation Means, i.e., barriers internal to the application that reduce the probability of the Operational Hazard from occurring in order to achieve the required Safety Objective

c. Allocate Safety Requirements to the sub-functions comprising the application.

3. Trajectory Change Requests – Today's Operations

This section briefly describes the Trajectory Change Request process in today's operations between the pilot and ATC for making Change Requests to the current ATC clearance. As conditions change during flight, it is common for the pilot to request an amendment to the ATC-cleared trajectory, e.g., to meet some need for safety, efficiency, or ride quality / comfort for passengers.

In today's operations, Trajectory Change Requests are made by pilots with little or no awareness of the traffic situation, flow management routings, or ATC sector considerations. Some of these Change Requests are denied by ATC for the following reasons:

1) Change Request conflicts with other traffic
2) Change Request conflicts with static or dynamic restrictions in use by ATC
3) Change Request is requested too close to the next sector handoff

The effects of denial of a Change Request by ATC to the pilot are:

1) Unnecessary workload burden on the pilot without a beneficial result

2) Discourages the pilot from making future Change Requests to improve their flight efficiency
3) Flight improvement opportunities are often unrealized because the pilot may not be aware of changes that would improve efficiency and be ATC approvable
4) Unnecessary workload burden on ATC.

In general, the pilot seeking opportunities to improve safety, efficiency or ride quality has very limited awareness of many of the factors that would adversely affect ATC acceptability of Change Requests to the current flight plan. This environment is not conducive for the pilot to seek operational efficiency improvements due to a lack of situational awareness of the external environment that may constrain changes to the flight plan.

The next section explores the new capabilities that incrementally provide an increasing influence and control over the trajectory flown for safety, efficiency and capacity gains within the ATC construct.

4. ABTM Application Roadmap High-Level Descriptions

4.1 ABTM 1 – Basic TASAR

Basic TASAR (ABTM 1) is an EFB application being developed by NASA and is designed to optimize the flight trajectory for cost benefits in current flight operations [1][2]. Among the systems and technologies that comprise or support TASAR are: flight-optimizing software algorithms, a software-hosting device such as a portable or installed EFB, Automatic Dependent Surveillance Broadcast (ADS-B) IN and other sources of traffic information, and additional ground-based information obtained via data link or internet connectivity. TASAR seeks to provide cost-beneficial optimization with respect to the current active trajectory, taking traffic and other constraints into account. The TASAR application, using these information sources, has the ability to react in an agile manner to changes in the external airspace environment (e.g., adverse weather, winds, and airspace constraints).

Utilizing available information of own-ship flight status, flight plan, and airspace environment (e.g., proximate traffic, weather, winds, and ATC system status), Basic TASAR seeks to identify and recommend candidate trajectory changes for consideration by the pilot that have a high probability of ATC approval.

The pilot, at his or her discretion, can choose to make a Change Request to ATC based on TASAR recommended trajectory change candidates.

Prior to recommending optimized trajectory change candidates to the pilot, Basic TASAR evaluates the proposed trajectory changes against available on-board traffic and airspace hazard data for potential conflicts, and it may account for known ATC sector rules and own-ship flight position relative to the sector boundaries. Thus, recommended trajectory change candidates from

TASAR to the pilot are expected to have the following characteristics that will encourage increased pursuit of flight plan improvements by the pilot from ATC via voice requests:

1) Meet optimization goals for the flight, as provided by operator preferences that are input to TASAR by the pilot, providing improvement to the current flight plan in terms of time and / or fuel saved or other desired attributes such as passenger comfort and safety.

2) Have a high potential for approval by ATC by considering ATC preferences in the identification process

Basic TASAR trajectory change candidates are advisory-only to the pilot, and the pilot has full discretion on whether or not to use a TASAR-provided trajectory change in a Change Request to ATC. Pilot training ensures that normal priorities to aviate, navigate, and communicate are followed as in today's operations. The pilot has a responsibility to evaluate TASAR-provided trajectory change candidates before making a Change Request to ATC to minimize spurious Change Requests.

As in today's operations, ATC has separation responsibility and will not approve Change Requests from the pilot that do not meet ATC constraints and separation requirements.

4.2 ABTM 2 – Digital TASAR

Digital TASAR (ABTM 2) is an extension of Basic TASAR to enable more complex, and therefore more valuable, Trajectory Change Requests to ATC by the use of data communications (including Data Comm) to request the trajectory change and to receive the amended clearance from ATC. For ABTM 2 data communications, whether through the use of Data Comm or other internet-based services that are available and cost beneficial, several improvements to the request/re-clearance process are achieved:

1) Removing the restriction of using named waypoints, necessary to facilitate voice requests.
2) Removing the length limitation on route descriptions, necessary to keep voice requests to a manageable size.
3) Removing the need to manually enter descriptive trajectory elements by the controller into his/her automation system and by the pilot into the FMS or navigation system. This eliminates manual entry errors.
4) Speeding the request/re-clearance process by taking it off the voice channel.
5) Speeding the controller's evaluation process through the use of a graphical descriptive format and potential use of ATC automation assistance for evaluation of the request.

The same roles and responsibilities described for Basic TASAR remain in Digital TASAR operations. The trajectory change candidates are still advisory-only to the pilot and may be requested at his/her discretion, but voice frequency congestion is no longer a consideration. Digital TASAR may still be an EFB-hosted application or may be contained in other certified avionics.

4.3 ABTM 3 – 4D TASAR

4D TASAR (ABTM 3) further extends the capability of the optimization algorithm through the inclusion of the longitudinal element – speed and time along track. This additional optimization dimension enables the operator to specify objectives for that flight's efficiency and for total network efficiency. It also enables coordination of the trajectory optimization with the automated ATC arrival scheduler, such as TBFM, and future FIM operations. Even in the absence of ATC-imposed arrival time constraints, 4D TASAR gives the operator a powerful new tool to optimize flights within its total network operation, taking company resource constraints, such as gate availability and connection times, into consideration during the optimization process.

4D TASAR connectivity to TBFM and FIM to ensure achieving the respective goals of these functions is not expected to raise the safety criticality of 4D TASAR. The safety assessment of TBFM and FIM are separate exercises with their own set of hazards and risk assessments. The use of Required Time of Arrival (RTA) functionality to comply with flow and interval management clearances will take place in the FMS, not the ABTM system. However, as the 4D TASAR trajectory solutions will contain speed guidance as well as lateral and vertical guidance to carry out the requested re-clearance, the implementation will likely include more integration with existing avionics and cockpit automation than Digital TASAR. Pilot and controller roles and responsibilities remain unchanged, and so even though the trajectory optimization and negotiation process becomes much more ubiquitous, the safety aspects of traffic separation remain unchanged.

4.4 ABTM 4 – Strategic ABTM

Strategic Airborne Trajectory Management (ABTM 4) represents a significant change in ATC operations by introducing blanket approval of "strategic" Change Requests to the flight trajectory, defined as those beginning in the next sector (or beyond) after the one currently occupied. The de-conflicted time horizon is extended to accommodate the later maneuver. Strategic ABTM is enabled by receipt of intent information on other traffic from the ATC computer system via data link or potentially through System Wide Information Management (SWIM). The acceptability of these changes will have been verified by years of collected data on Change Requests during Basic and Digital TASAR operations. Because these trajectory changes will originate beyond the sector currently occupied, they will not impact the traffic situation of the current controller. In the time period envisioned for ABTM 4, the ground-based ATC automation will be capable of evaluating the impact of the trajectory change, and the airborne system will be capable of generating conflict-free trajectory solutions to the appropriate time horizon with the required integrity to permit their blanket approval. Because these trajectory changes begin in the next sector, tactical separation responsibility remains with the air traffic controller. ABTM automation will continue to recommend improved trajectories for request in the current sector (as in ABTM 1-3) and these will connect to the downstream strategic changes of ABTM 4.

4.5 ABTM 5 – Full ABTM

Full Airborne Trajectory Management (ABTM 5) adds full-time tactical separation functionality to the Airborne Trajectory Management automation system and therefore responsibility for separation assurance. At this stage, the airborne system has been collecting background data during years of operations in hundreds of aircraft, sufficient to validate the tactical separation system performance for use in certification and operational approval of airborne separation systems. The ABTM software is now totally integrated with the cockpit communication, navigation, and surveillance systems such that continuous trajectory optimization is performed from takeoff to touchdown including both strategic and tactical de-confliction. To ensure sufficient operational benefits justifying equipage, this airborne capability should permit the elimination of ATC structural constraints (e.g., departure fix, overhead slots, and Center and sector boundary Miles-In-Trail restrictions) from the operations of Full ABTM flights. Arrival integration of these flights with unequipped traffic being conventionally managed by the ATC system is accomplished through the 4D TASAR (ABTM 3) coordination with TBFM at the arrival station. Full ABTM is no longer an EFB application. Total integration with the certified avionics using dual redundancy and system cross-checking of tactical separation is expected.

5. Airborne Trajectory Management "Intended Function" Descriptions

5.1 Basic TASAR - Intended Function Description

Basic TASAR (ABTM 1) is a flight deck-based decision aid consisting of software automation algorithms and both text and graphic displays intended to provide an advisory-only service to the pilot to seek trajectory improvement opportunities over the current active route. Basic TASAR is expected to be a hosted software application on an EFB, either installed or uninstalled, with Basic TASAR operating as a Type B EFB software application. Refer to [11] for a comprehensive assessment of FAA regulations and guidance on EFB-based flight deck applications. The Basic TASAR EFB will interface with avionics as read-only (i.e., it will not transmit to avionics) as defined in the current concept of operations.

Based on inputs provided by 1) the pilot (in the form of company flight objectives and optimization criteria), 2) on-board avionics systems including surveillance, and 3) airborne internet data connectivity, the Basic TASAR application computes available trajectory change candidates (solutions) that may improve fuel and/or time performance over the current active route. Trajectory change candidates provided by Basic TASAR are designed to have relatively high probability of ATC approval by considering nearby traffic and airspace constraints during formulation.

Pilots have full discretion whether to use Basic TASAR-provided, Trajectory Change Request information; they can choose to use the recommended trajectory change candidates in a verbal communication with ATC, or they can choose to ignore them. Basic TASAR can be manually inhibited at any time, for any reason. Thus, in the event of observed spurious behavior of Basic TASAR due to any system failure, inaccurate data obtained via network enabled information

sources, or Basic TASAR being a source of distraction to the flight crew, the pilot can simply inhibit or ignore it. By following their training, the pilots can manage the use of Basic TASAR in such a way that it will result in little or no workload increase on the flight deck.

Basic TASAR is a supplemental system intended to provide operational benefits without adversely impacting safe operations, and it does not replace any aircraft system or procedure needed for flight operations. The Basic TASAR display is passive with no display of "ownship" or audible alerting. Loss of the Basic TASAR EFB application for any reason does not affect the Minimum Equipment List (MEL) and does not affect normal flight operations.

Basic TASAR information sources may include the following:

1) Own ship systems (aircraft state, auto-flight settings, active route from FMS, etc.)
2) Traffic data via ADS-B IN, Traffic Information Service Broadcast (TIS-B), or other sources such as airborne internet
3) Airspace system status and forecast (sector use and configuration, Traffic Management Initiatives, Special Use Airspace activity, etc.)
4) Weather status and forecast
5) Wind status and forecast
6) Operator's resource and network planning, preferences, and objectives.

5.2 Digital TASAR – Intended Function Description

The Intended Function of Digital TASAR (ABTM 2) is the same as Basic TASAR, only the added data link capability will permit it to perform better, resulting in greater benefits from its use. The same statements regarding its optional use hold true, and the pilots may still ignore or disable the system in the event of failure or spurious output. Inputs to Digital TASAR are essentially the same, but the airborne surveillance is expected to be more comprehensive in the timeframe of expected operations because of the ADS-B OUT mandate. Deployment of SWIM will likely improve the quality and timeliness of ground-derived information used in the Digital TASAR algorithms.

The solutions provided by Digital TASAR will still be evaluated by the pilot for acceptability before making a Trajectory Change Request to ATC, but the communication with ATC will be via some form of datalink for the request, and approved via Data Comm for the re-clearance. These systems will already have their own approvals separate from Digital TASAR. The separation function responsibility remains with ATC. Digital TASAR is a supplemental system, not replacing any system required for operation of the aircraft. It is not required per the MEL.

5.3 4D TASAR – Intended Function Description

The Intended Function of 4D TASAR (ABTM 3) remains the same as Basic TASAR and Digital TASAR but adds the capability to optimize with respect to speed and to coordinate with TBFM and FIM requirements, further improving the achievable benefits. 4D TASAR may still be a

supplemental system with the same qualification as Basic TASAR for being advisory only and optional. It may connect with other cockpit avionics through approved interface devices or be designed from the outset as an integrated system. When connected to FIM, the responsibility for aircraft separation (as currently planned) will remain with the controller, and the RTA function will reside in the FMS. Even if air-to-air spacing in FIM becomes an aircraft separation function, it will be separately certified from the 4D TASAR optimization function. Thus ABTM 1-3 all have the same Intended Function and lack of safety criticality.

5.4 Strategic ABTM – Intended Function Description

Strategic Airborne Trajectory Management (ABTM 4) has two intended functions: first, to optimize the future trajectory in route, speed, and altitude starting from an initial maneuver in a downstream sector forward to the destination, while de-conflicting that trajectory out to an appropriate time horizon from other known aircraft trajectories and fixed airspace constraints; and second, to send the trajectory directly into the ground-based ATC enroute automation as the updated active route. Supplementing the airborne surveillance from ADS-B IN, the planned trajectories (or intent) of potentially conflicting traffic aircraft are to be obtained through SWIM and input to the airborne system for use in the evaluation of trajectory change candidates. These functions enable a further increase in operational benefit to the aircraft operator and also reduce controller workload by eliminating potential traffic conflicts before they are detected in the downstream sector. However, even with the blanket approval for change to the future trajectory in this fashion, the tactical separation responsibility remains with the controller, keeping the safety evaluation of this system in the supplemental systems category. A failure of the Strategic ABTM system to de-conflict the future trajectory would place the aircraft in the same situation as non-equipped traffic, incapable of performing this function and requiring the downstream sector controller to resolve the conflict. As the de-confliction software used in Basic TASAR contains both strategic and tactical separation algorithms, the performance of these algorithms in performing their separation functions will be recorded during all of their operations for several years, even though it is not used in the actual separation of traffic. This data will be used in subsequent validation of the airborne separation system to perform those functions in the next and final step of the roadmap, Full Airborne Trajectory Management (ABTM 5).

5.5 Full ABTM – Intended Function Description

The intended function of Full Airborne Trajectory Management (ABTM 5) is to provide optimized and deconflicted flight guidance throughout the flight within a mixed airspace environment of equipped and unequipped airspace users, the latter being managed by conventional ATC. Dynamic flight trajectory optimization is the first objective, modified as required to meet safety of flight needs and destination runway scheduling. Full integration with TBFM and FIM are part of the Full ABTM concept. Tactical separation is added to the Strategic ABTM capability as an a priori objective function. The operational benefits are maximized in this operation by the elimination of all trajectory constraints that are artifacts of ATC separation responsibility. Both flight efficiency and major capacity increases are enabled by this means, and these benefits can be used in justifying

the equipment costs and the higher certification needed to approve these functions on the aircraft. It is expected that these functions will be implemented through integrated avionics systems with already high certification levels and that the separation function will not change that level. Redundant avionics provide backup separation safety, and multiple independent surveillance systems to complement ADS-B (such as the Traffic Alert and Collision Avoidance System (TCAS) surveillance in the aircraft and Conflict Alert on the ground for a possible safety advisory) could be used in the safety assessment of these operations.

Note: TCAS consists of both surveillance processing and a collision avoidance function. TCAS surveillance processing represents the acquisition and tracking of TCAS targets, and may be fused with ADS-B surveillance data to support the separation function of ABTM 5. TCAS surveillance processing is identified in the safety analysis for some hazards as a form of mitigation. No credit is taken for the TCAS collision avoidance function in this safety analysis as an explicit mitigation, but it serves as a last resort safety function as mandated by ICAO.

6. Method 1 Safety Analysis – Conventional Method

This section addresses the safety assessment of the five ABTM roadmap steps using the traditional system safety process based on ARP 4761 [6], AC 25-1309 [7], and AC 23-1309 [8]. As noted earlier in Section 2, this safety assessment method analyzes the intended functions of each system in Section 5 using the steps outlined in Section 2.

The key outcome of this safety assessment process is the determination of the Failure Effects Classification (FEC) of each ABTM application. The FEC then drives the development and validation requirements and processes to be followed in integrating these applications into the flight deck to gain certification and operational approval.

Using this safety assessment process (i.e., Method 1), applicants and certification and operational authorities (i.e., FAA aircraft certification and flight standards organizations) follow the process of assessing the new application and attendant procedures for potential failure modes and their impact on safety.

6.1 Key Factors that Influence FEC of ABTM 1-4

The following list represents key factors that influence the determination of FEC for ABTM 1-4:

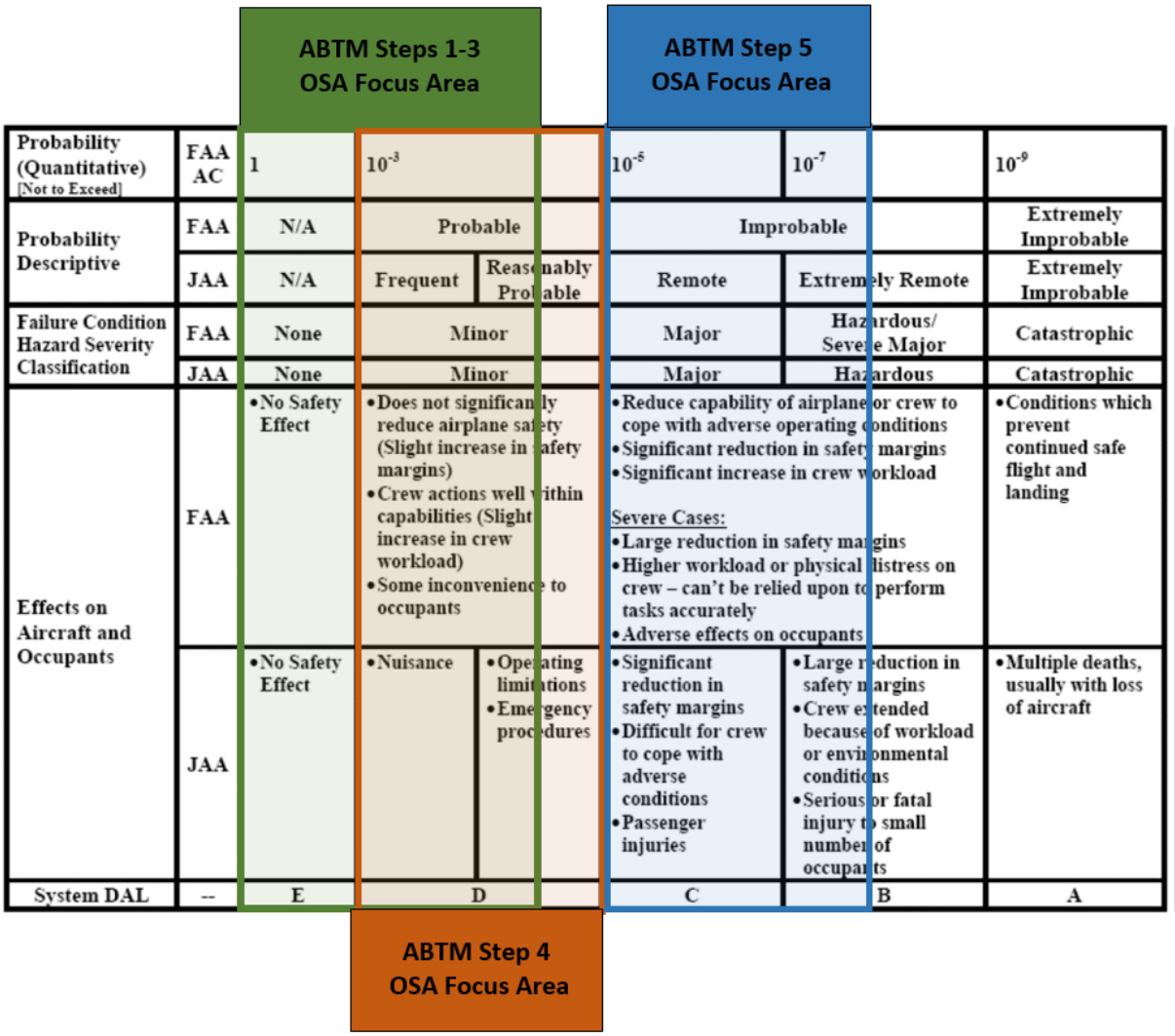
1) ABTM 1-4 systems are supplemental systems not relied on by critical functions supporting flight deck operations.
2) ABTM 1-4 systems are optional, i.e., not required for flight operations. In the event of failures of the system, it can be ignored or disabled without adversely affecting operations.
3) ABTM 1-4 applications have no MEL requirement.

4) ABTM 1-4 systems can be manually inhibited at any time, for any reason
    a. Detected failure of the ABTM 1-4 systems.
    b. Detected failure of the host EFB. If hosted in another certified avionics box, this failure does not only apply to ABTM, but to its other functions.
    c. Spurious or inconsistent performance of trajectory change candidates.
    d. Distracting effects of ABTM systems to the pilot.
5) Presence or loss of ABTM 1-4 systems does not change responsibilities of the pilot for flight operations.
6) ABTM 1-4 systems are "advisory-only" (i.e., does not provide flight guidance information)
    a. Pilot is not reliant on ABTM 1-4 system outputs to perform safe flight operations.
    b. Pilot can choose to either use or ignore trajectory change candidate recommendations from ABTM 1-3 systems when communicating Change Requests to ATC. In ABTM 4, once the trajectory change is sent, it must be followed unless an amended clearance is received. Since it would already be the active route in the FMS, this requirement is routine.
7) Change Request procedures are unchanged in ABTM 1-3.
    a. Pilot must direct all Change Requests to ATC using approved means.
    b. ATC is responsible for reviewing Change Requests for acceptability, including separation from traffic.
    c. ATC either 1) approves request and issues clearance, 2) provides an amended clearance, 3) defers request to next controller, or 4) denies request.
8) In ABTM 4,
    a. Pilot will send the revised trajectory (that starts in the next sector or beyond) to ATC by approved means.
    b. The change is simultaneously executed as the active route in the FMS.
    c. A trajectory change from present position to connect to the ABTM 4 change in the next sector must be requested and approved in the same fashion as in ABTM 1-3.
9) Undetected, misleading information associated with ABTM 1-4 solutions, i.e., with one or more trajectory change candidates, will have "No Effect" on the pilot, aircraft, and/or on ATC. Whether due to failure of one of the ABTM sub-systems and associated automation processing, or being the result of inaccurate data obtained from ground-based or flight deck systems, spurious Change Requests are mitigated by flight crew inspection of the recommended trajectory change and (for ABTM 1-3) by mitigation associated with the existing Change Request process.

6.2 Failure Effects Classification

Figure 1 (from AC 25-1309 [7]) provides a mapping of the "Effects" due to failures and the allowable "Probability of Occurrence" that lead to the determination of the FEC of the planned

application (i.e., ABTM 1-5). The anticipated regions where the various ABTM roadmap application steps fall are highlighted in Figure 1.



Probability (Quantitative) [Not to Exceed]	FAA AC	1	10^{-3}	10^{-5}	10^{-7}	10^{-9}
Probability Descriptive	FAA	N/A	Probable	Improbable		Extremely Improbable
	JAA	N/A	Frequent / Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Hazard Severity Classification	FAA	None	Minor	Major	Hazardous/ Severe Major	Catastrophic
	JAA	None	Minor	Major	Hazardous	Catastrophic
Effects on Aircraft and Occupants	FAA	•No Safety Effect	•Does not significantly reduce airplane safety (Slight increase in safety margins) •Crew actions well within capabilities (Slight increase in crew workload) •Some inconvenience to occupants	•Reduce capability of airplane or crew to cope with adverse operating conditions •Significant reduction in safety margins •Significant increase in crew workload <u>Severe Cases:</u> •Large reduction in safety margins •Higher workload or physical distress on crew – can't be relied upon to perform tasks accurately •Adverse effects on occupants		•Conditions which prevent continued safe flight and landing
	JAA	•No Safety Effect	•Nuisance •Operating limitations •Emergency procedures	•Significant reduction in safety margins •Difficult for crew to cope with adverse conditions •Passenger injuries	•Large reduction in safety margins •Crew extended because of workload or environmental conditions •Serious or fatal injury to small number of occupants	•Multiple deaths, usually with loss of aircraft
System DAL	--	E	D	C	B	A

Figure 1 Acceptable Risk versus Potential Effects *(As defined for Civil Aviation)*. Modified from [7].

Based on the above noted factors alone, this safety analysis (Method 1) comes to the conclusion that ABTM 1-3 can likely be developed and implemented with a No Effect FEC designation. Potentially, in the worst case, ABTM 1-3 could rise to a Minor FEC designation in the event of inconsistent candidate Trajectory Change Request recommendation(s), which could result in workload issues (for the pilot and / or ATC). However, workload issues are not anticipated to be an issue for the pilot's use of ABTM 1-3, as the pilot can simply ignore the ABTM system for any reason. Through proper training in the use of ABTM 1-3, the pilot should not be distracted or be adversely influenced in using ABTM while conducting flight operations. From an ATC perspective, controllers will continue to conduct the Trajectory Change Request process as in

today's operation and are not expected to experience a workload issue due to ABTM. In the future Data Comm operation (ABTM 2 and beyond), the workload for both pilots and controllers should go down through the use of ABTM due to its ability to automatically create the trajectory change and not require it to be manually input by any person.

Final determination of the FEC for ABTM 1-3 will require a dialog between the applicant and FAA Certification and Operational Approval authorities using the results of the safety analysis, which will result in a final designation by FAA.

Because the strategic trajectory changes in ABTM 4 (that begin in a downstream sector) may be accepted without ATC evaluation, they must be found to have the integrity expected in this operation. Failure to provide this level of integrity could result in a subsequent trajectory amendment by ATC when the discrepancy came to light. Because of this, the FEC could be classified as Minor due to ATC workload considerations. As the separation responsibility never leaves the controller, roles and responsibilities remain unchanged, so ABTM 4 FEC should not require classification higher than Minor.

ABTM 5 adds the tactical separation function and airborne responsibility for its normal execution to prevent loss of separation events. For this reason, it is expected that the FEC for ABTM 5 will be Major.

6.3 ABTM 1-3 Applications Internal Mitigation Means

The ABTM applications themselves provide additional inherent capabilities that further reduce the possibility of unintended adverse effects and are expected to enhance the usability of the applications. These further serve to strengthen and support the No Effect FEC for ABTM 1-3:

1) In order to prevent errors in communicating the Trajectory Change Requests to ATC, ABTM 2-3 utilize standard Data Comm protocols for trajectory exchange without requiring data entry by the pilot.

2) ABTM 1-3 systems display flight path change opportunities using standard graphical formats to facilitate pilot understanding and comparison to the active route.

3) ABTM 1-3 will use its capabilities to assess sector complexity, known rigid ATC constraints, and own ship's proximity to sector handoff to only recommend Change Requests that have a high likelihood of being approved by ATC.

6.4 Procedural Mitigations Available to the Pilot

1) An additional characteristic of ABTM 1-4 is that there is no "recovery" time required for the flight crew following an ABTM 1-4 system failure. In other words, in using ABTM 1-4, the pilot remains on an ATC-cleared trajectory at all times. In the event of a system fault, the pilot need only remain on the current clearance while disregarding the ABTM 1-4

system output. A ***simple reset of the ABTM 1-4 system or simply choosing to ignore its outputs*** (e.g., by not looking at the display) allows the pilot to continue to focus on aviate, navigate, and communicate tasks in conducting flight operations (whether during normal operations or in the event of abnormal or emergency situations)

2) The pilot has ***responsibility to evaluate ABTM 1-4 trajectory change candidates before sending a Change Request*** *(or sending the change itself in ABTM 4)* to ATC, providing cross-check opportunities to detect spurious or false trajectory change candidates being offered by the system. The graphical comparison to the active route and the display of time and fuel outcomes provide a simple means for the pilots to perform this 'reasonableness' check.

3) Other aircraft systems, e.g., FMS and weather radar, serve as higher integrity systems for conducting a ***quick check on acceptability*** and performance impacts of ABTM 1-4 Trajectory Changes.

6.5 ABTM 1-4 Phase of Flight Considerations

From a phase of flight perspective, ABTM 1-4 is intended for use primarily outside of Terminal Airspace

1) Trajectory Change solutions are offered by ABTM 1-4 systems during climb, while enroute, and into the early portion of descent operations.
2) ABTM 1-4 is thus used primarily during non-critical phases of flight, i.e., above 10,000 ft.

6.6 ABTM 1-3 Information Source Quality

Due to the No Effect / Minor FEC anticipated for ABTM 1-4, its information source quality and integrity must be commensurate to support this FEC.

1) ABTM 1-4 input information quality and integrity requirements are not driven as much by safety considerations as by operational use issues.
2) Low quality and/or misleading information can result in poor recommendations to the pilot for candidate Trajectory Change Requests. The net effect is that ABTM 1-4 will not be as effective in achieving envisioned operational benefits (e.g., time or fuel saved).

6.7 ABTM 1-3 Undetected Failure – Worst Case Effect

From an Undetected Failure perspective, inefficient routing is the only adverse outcome. Existing mitigation of any safety hazards is provided by ATC, as is already done for Trajectory Change Requests today. The same is true for ABTM 4, but the ATC recognition may be delayed. Because it only applies to a strategic trajectory change, the impact of this delay is small.

Note: The Safety Analysis using Method 2 (based on the Operational Safety Assessment of DO-264 / ED-78A) described in the next section takes a closer look at specific failure modes of ABTM.

7. Method 2 Safety Analysis – Operational Safety Assessment Process

This section provides the safety analysis of TASAR using the Operational Safety Assessment (OSA) process from RTCA DO-264 / EUROCAE ED-78A [9], referred to as Method 2 in this report. Figure 2 illustrates the process at a high-level using the 'bow-tie' model.

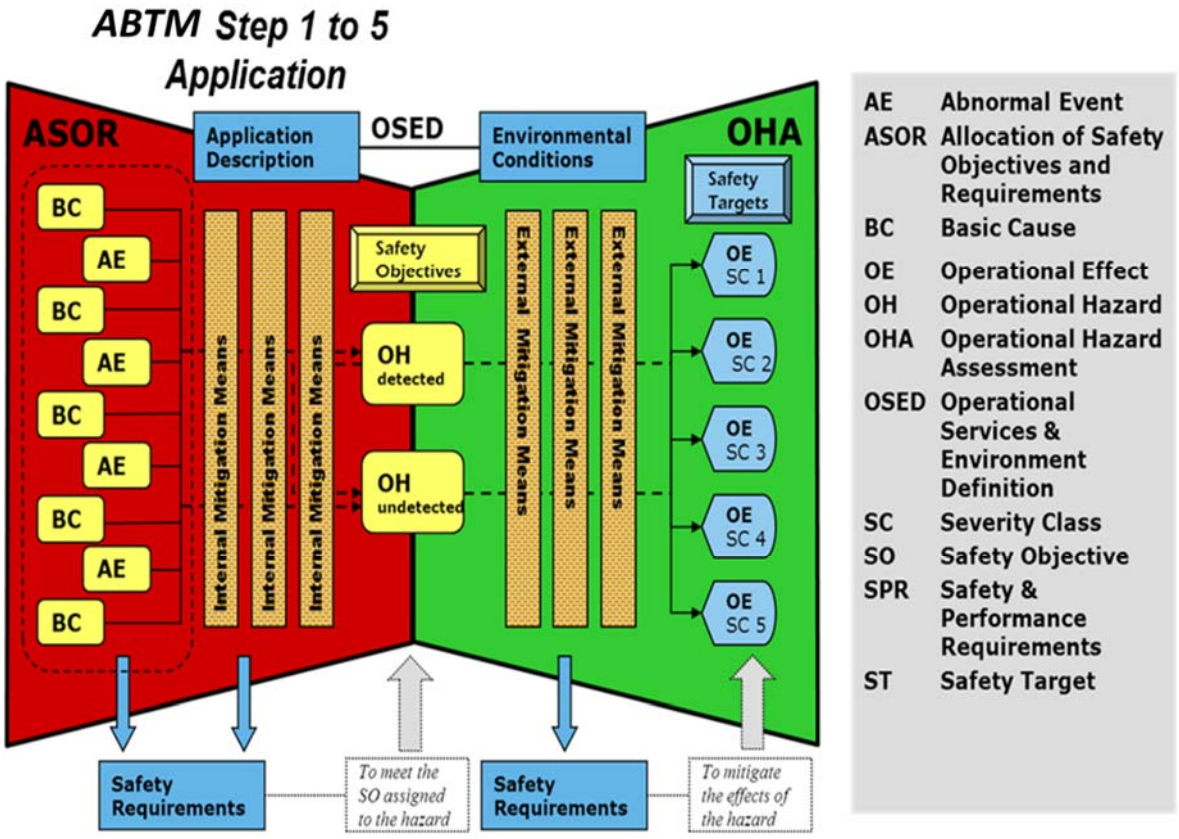


Figure 2 Operational Safety Assessment Process – Method 2. From [9].

In Figure 2, the system of interest, in this case the ABTM applications, is represented in the left-hand side of the "bow-tie". The external environment in which the applications operate, including environmental conditions (e.g., airspace influences, weather, traffic) and the external systems that are part of the overall operational concept (e.g., aircraft systems and ATC systems), are represented by the right-hand side of the "bow-tie".

The OSA process consists of the following major sub-processes: 1) the Operational Hazard Assessment (OHA), and 2) Allocation of Safety Objectives and {Safety} Requirements (ASOR).

In performing the OHA, the first step is to use operational experts from all stakeholder communities to identify potential Operational Hazards that may result from the application (e.g., ABTM). For each identified Operational Hazard, the next step is to determine the worst "credible" outcome, also referred to as the Operational Effect. Examples are collision, loss of separation (major loss versus minor loss), and workload.

For each Operational Hazard and associated Operational Effect, the Severity Class is determined. Severity Classes include Catastrophic, Severe Major, Major, Minor, and No Effect. For each Operational Effect and associated Severity Class, a "Probability of Occurrence" not to be exceeded to assure safety of operations is established (e.g., 10^{-9}, 10^{-7}, 10^{-5}, 10^{-3}) for occurrence of the Operational Effect. The Operational Effects and Severity Classes are noted in Figure 2 on the right side of the bow-tie.

Figure 3 provides a mapping of hazards to the associated effects on operations due to each hazard class. The likely regions of applicability for the ABTM 1-3 OSA process described in this section and for ABTM 4-5 described in following sections, are highlighted in Figure 3. The highlighted regions represent Major, Minor, and No Effect FECs.

From the OHA sub-process, each Operational Hazard is assigned a Safety Objective that it must meet in order to assure safe operations. It is the task of the ASOR to ensure that the Safety Objective is met. It is noted that for each Operational Hazard, there could be multiple Operational Effects, thus resulting in multiple Safety Objectives being assigned to each Operational Hazard. The ASOR must assure that all Safety Objectives are met for each Operational Hazard.

In order to mitigate the effects of the Abnormal Events and Basic Causes identified as root causes of failures, it will be necessary to identify relevant mitigations internal to the application, denoted as Internal Mitigation Means. These mitigate the effects of Abnormal Events and Basic Causes to achieve the Safety Objectives for each Operational Hazard. This then also allows specifying Safety Requirements that are associated with sub-system elements internal to the application. The combination of Abnormal Events, Basic Causes, Internal Mitigation Means, Safety Objectives, and Safety Requirements are illustrated by the left-side of the bow-tie.

The OSA process is beginning to be widely used by EUROCONTROL and FAA in the development of Safety, Performance, and Interoperability Requirements for ADS-B IN applications. This process is well suited for higher criticality system-of-systems and allows a more formal analysis process using fault trees and event trees. Fault Trees are typically used to capture the left-hand side "bow-tie" process of the ASOR, while Event Trees are typically used to represent the OHA process characterizing the external environmental factors represented by the right-hand side of the bow-tie.

Hazard Class	1 (most severe)	2	3	4	5 (least severe)
Effect on Operations	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety.
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
Effect on Air crew	Fatalities or incapacitation.	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or slight reduction in air traffic control capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.

ABTM Step 5 OSA Focus Area

ABTM Step 4 OSA Focus Area

ABTM Steps 1-3 OSA Focus Area

Figure 3 Hazard Classification Matrix. From [9].

While the strength of the OSA process is its usefulness in analyzing complex, high-criticality system-of-systems and that it allows for a relatively balanced approach for allocating integrity requirements across all systems, the process may not be as well suited for lower-criticality systems, e.g., ABTM 1-3, as the fault tree and event tree methodologies and associated calculations begin to become onerous in terms of their ability to analyze the more qualitative and subjective aspects of these types of applications. It is also often quite difficult to quantitatively prove probabilities associated with workload factors and ability of the human to perform various routine existing functions. This often times becomes a significant and time consuming (and costly) issue in gaining approval for new safety requirements that result from using the methodology.

Considerable attention has been given in this report to the identification of Operational Hazards potentially associated with ABTM. However, the report intentionally stops short of performing a quantitative analysis of the Safety Objectives and probabilities of the barriers provided by the mitigations identified, since ABTM 1-3 were determined to have a No Effect or in worst case a Minor FEC, and Minor for ABTM 4 as well. The OSA presented is thus an abbreviated OSA relative to [9].

7.1 Operational Hazards Identification

Before commencing with the identification of Operational Hazards using the Method 2 OSA approach in this section, it is noted that the same high-level factors and mitigation already described in Section 6 also apply here. This step takes a closer look at Operational Hazards that could occur within the ABTM applications.

As indicated previously, Operational Hazards result from Abnormal Events and Basic Causes, which represent errors and failures in actions associated with the human operator (e.g., the pilot), or systems functions (e.g., ABTM automation). Abnormal Events include both errors by the pilot in relation to ABTM system use and in interactions with ATC as part of the Change Request/re-clearance and autonomous trajectory change procedures of ABTM 4-5.

In order to more closely examine potential sources of errors associated with actions by humans and ABTM 1-3 automation processing, Figure 4 illustrates the potential information flows within ABTM 1-3.

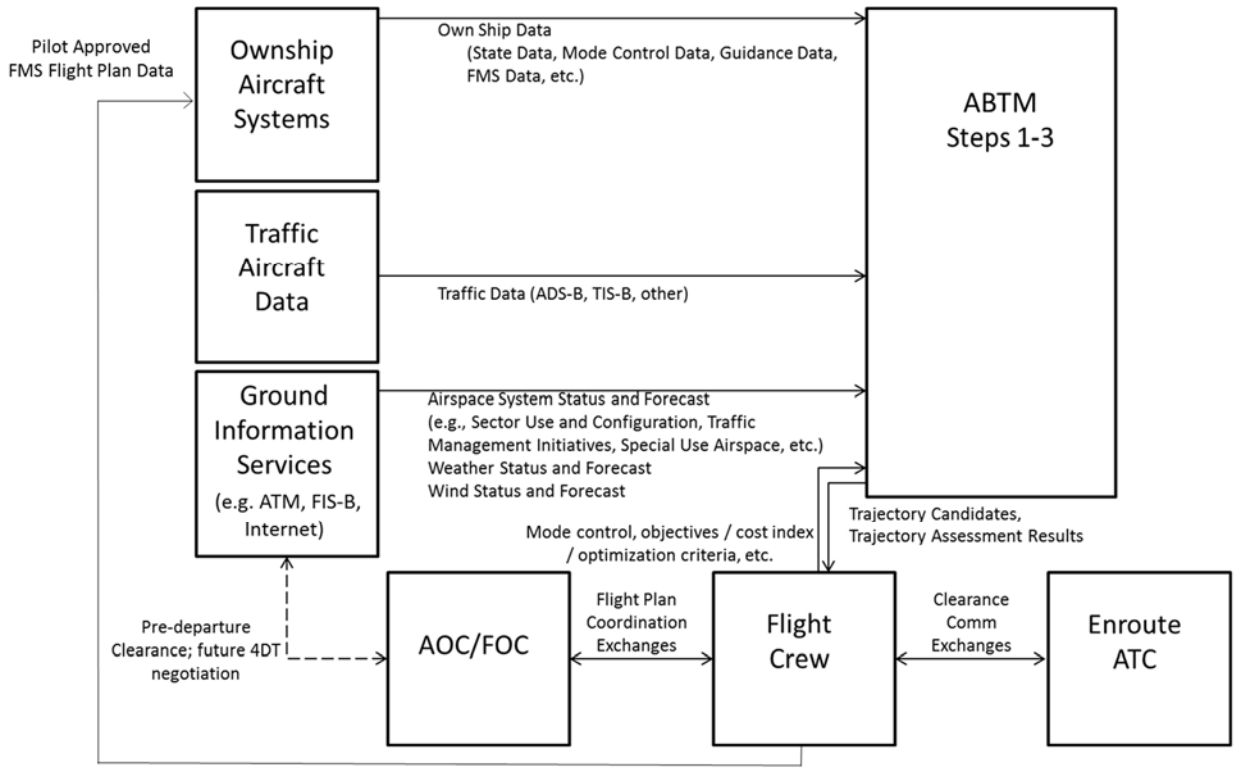


Figure 4 ABTM Functional Diagram*

*Note: The information elements identified in Figure 4 are notional at this point and are being refined as part of the detailed design of ABTM 1-3.

From Figure 4, the following information exchanges associated with human and automation processing actions represent potential sources for errors and misleading information that may result in Operational Hazards:

7.1.1 Human Actions Potentially Leading to Abnormal Events

The following list identifies human actions that provide the opportunity for occurrence of Abnormal Events (i.e., when human actions are performed in error) in ABTM 1-3:

1. Pilot, flight crew
    a. Enters ABTM configuration, objectives, and optimization criteria via the ABTM Human Machine Interface (HMI).
    b. Receives and interprets ABTM system data via the ABTM HMI, e.g., recommended trajectories, conflict status, and outcomes.
    c. Communicates Change Requests to ATC (via data link in ABTM 2-3).
2. Air Traffic Controller (enroute)
    a. Provides separation assurance services.
    b. Communicates Change Request clearances to pilots (via Data Comm in ABTM 2-3).

7.1.2 ABTM Automation Processing Actions Potentially Leading to Basic Causes

The following action performed by the ABTM 1-3 automation (i.e., decision support algorithms) provides the opportunity for occurrence of Basic Causes (i.e., when actions by automation are erroneous):

ABTM 1-3-Related Processing that could result in Undetected Misleading Information

Any misleading information provided by information sources to ABTM 1-3 automation, or errors and failures in ABTM 1-3 automation processing, could potentially result in misleading trajectory change candidates being recommended to the pilot for consideration. Such misleading information may detract from the ability of ABTM 1-3 to achieve operational benefits. However, since the flight crew has no authority to deviate from their ATC clearance, regardless of the information provided by ABTM 1-3 systems, any occurrence of misleading information from ABTM 1-3 systems will be non-hazardous in nature and is completely mitigated by the ATC clearance procedure. Erroneous Change Requests that are ATC approvable but have higher than predicted fuel burn or flight time would be caught when input to the FMS, which would show a different result.

7.2 Potential Basic Causes for ABTM 1-3 – Detailed Assessment

The following represent potential Basic Causes associated with ABTM 1-3 erroneous information:

1. Own ship and/or traffic information (e.g., state, intent) are incorrect or incomplete, leading to trajectory change candidates that have a conflict but are represented as conflict free.

2) Wind data is of poor quality or is incorrect leading to Change Requests that are conflicted.

3) Convective weather information is of poor quality or is incorrect leading to Change Requests toward hazardous airspace.

4) Airspace status information is incorrect leading to Change Requests toward active Special Use Airspace.

5) Detected errors, failures, or poor quality ABTM 1-3 recommendations leading to pilot troubleshooting and therefore additional workload.

6) Undetected errors or failures of ABTM 1-3 computations leading to poor or multiple Change Requests and additional pilot or ATC workload.

7) Undetected errors or failures of ABTM 1-3 computations leading to acceptance of trajectory changes that result in decreased fuel reserves.

8) ABTM 1-3 application preoccupies the pilot from observing flight-deck hazard alerts.

7.3 Detailed List of Potential ABTM 1-3 Operational Hazards

The following represents the detailed list of Operational Hazards that have been identified using the OSA process described in this section. Associated mitigations, internal or external to ABTM 1-3, are also identified.

OH – 1: ABTM 1-3 provides one or more trajectory change candidates that are not conflict free.

This OH is the result of poor information quality and/or mixed ADS-B OUT equipage environment where not all traffic is known.

Mitigation – ATC provides separation assurance independent of ABTM 1-3.

OH – 2: ATC, somehow being aware of ABTM 1-3 capability for the aircraft / pilot requesting a Change Request to the flight plan, is less vigilant in providing separation assurance.

The concern is whether ATC could become complacent over time, when receiving ABTM 1-3 Change Requests. Note that ABTM equipage is not specified on filed flight plans or included in Change Requests.

Mitigation – Existing ATC procedure is to check all Change Requests for separation compliance.

Note: This is not a credible Operational Hazard because separation assurance is ATC's primary responsibility.

OH – 3: ABTM 1-3 provides numerous spurious and/or inconsistent series of trajectory change candidates. If trajectory change candidates are not reinforced from one request to the next, multiple counteracting Change Requests could be issued.

These Change Requests become a nuisance issue and potentially could lead to a workload issue for ATC.

Mitigation - Pilot will recognize spurious and inconsistent trajectory change candidates and simply not request them.

Mitigation – ATC denies Change Requests if workload is too high.

OH – 4: ABTM 1-3 recommends a trajectory change candidate with miscomputation of fuel burn.

Pilot reliance on ABTM fuel burn estimates (presented to help pilots choose between multiple trajectory change candidate options) could lead to greater fuel burn than expected.

Mitigation – Pilot uses the FMS to crosscheck prediction of fuel burn.

OH – 5: Unexpected weather develops on ABTM 1-3 recommended route after ATC approval.

Unexpected weather could require additional Change Requests and therefore more fuel to be used.

Mitigation – normal procedures for responding to unexpected weather.

Reviewing the above Operational Hazards, it is noted that due to the very strong and significant mitigations already provided by ATC separation assurance and pilot procedures in today's very safe operations, the worst case safety effect could be a workload increase for pilots and controllers. Since ABTM 1-3 automation are advisory-only systems and can be manually inhibited by the pilot at any time, for any reason, the most likely FEC for ABTM 1-3 would be No Effect. With the No Effect or perhaps Minor FEC, ABTM 1-3 is amenable for integration as an EFB application (as noted previously, for an installed EFB and Type B software application).

7.4 Operational Hazards Identification, ABTM 4

Human Actions Potentially Leading to Abnormal Events are the same as for ABTM 1-3. Mitigations are also the same.

7.5 ABTM Automation Processing Actions Potentially Leading to Basic Causes

OH-6: ABTM 4 automation fails to de-conflict the strategic route sent to ATC. Since the change occurs in the next sector, that controller may have to take action to de-conflict the changed route.

Mitigation - Controller de-conflicts traffic as though no change had ever been made to the trajectory. It was not de-conflicted in the first place before the change was made.

OH-7: ABTM 4 solution is inaccurate leading to lower fuel reserves. An error in the optimization software or the input data used in that software creates an erroneously low fuel burn estimate for the changed trajectory.

Mitigation - When the new route is loaded into the FMS, its separate, independent calculation of flight time and fuel burn catches the error. The pilot's normal review of the solution outcome would also catch large errors as being unreasonable.

OH-8: Distraction/workload increase for pilot or controller. The change has to be reviewed by the pilot before sending. If it is in error for being conflicted or in violation of a letter of agreement constraint, the controller will have to deal with it.

Mitigation - Procedures and training plus experience with earlier versions of ABTM will have made this a non-issue.

7.6 Operational Hazards Identification, ABTM 5

7.6.1 Human Actions Potentially Leading to Abnormal Events

OH-9: Pilot fails to follow guidance for conflict resolution.

Mitigations - Conformance monitoring by the ABTM system alerts the pilot to compliance with the flight guidance. TCAS surveillance processing and see and avoid prevent a loss of separation from becoming a near mid-air collision. Ground-based, independent conflict alert warns controller, who could provide a safety advisory as an additional duty. The TCAS collision avoidance function is not explicitly utilized as a mitigation but serves as a last resort safety function.

7.6.2 ABTM 5 Automation Processing Actions Potentially Leading to Basic Causes

OH-10: ABTM 5 surveillance fails to detect conflicting traffic.

Mitigations - ADS-B supported by TIS-B and TCAS surveillance processing make this extremely remote. If the traffic aircraft have both a transponder and ADS-B OUT failure, they must notify ATC and receive special handling. Ground-based, independent conflict alert warns controller, who could provide a safety advisory as an additional duty.

OH-11: ABTM 5 separation automation fails to detect and resolve a conflict with known traffic leading to a potential loss of separation.

Mitigations - Dual, redundant ABTM 5 systems constantly monitor the traffic and cross check the solutions and separation system performance. Data collections in the years preceding this operation on hundreds of aircraft validate the failure rate to be extremely remote. Ground-based, independent conflict alert warns controller, who could provide a safety advisory as an additional duty.

8. Summary

This report provides the results of preliminary safety assessments of five Airborne Trajectory Management roadmap applications. ABTM applications 1-4 may be hosted in an installed EFB or in another certified avionics box. ABTM 1-4 are optional, advisory-only decision support tools to recommend trajectory change improvement opportunities to the pilot for operational efficiency improvements during flight. As such, ABTM 1-4 systems are supplemental equipment, do not replace any required avionics functions, and are not needed as part of the MEL for flight operations. Use of ABTM 1-4 is at the discretion of the pilot, i.e., the pilot may choose to ignore ABTM 1-4 or can manually inhibit its operation at any time for any reason.

ABTM 5 is a dual-redundant, safety-certified system intended for continual use in flight for trajectory management. ABTM 5 system output is in the form of flight guidance, optimizing the trajectory and modifying it to the extent necessary to avoid weather and airspace hazards and to prevent and resolve conflicts with other aircraft.

Two safety analysis methods were followed to determine the expected Failure Effects Classification for the five ABTM applications: 1) a traditional system safety process, and 2) an Operational Safety Assessment. Due to the relatively low-criticality of the ABTM 1-4 applications per the description of the ABTM Intended Functions in Section 5, and the availability of a number of significant mitigation barriers used in today's operations that greatly reduce the probability of ABTM 1-4-induced safety effects, both analyses support an ABTM 1-3 FEC of No Effect and no higher than Minor.

ABTM 4 FEC will likely be Minor to reflect the higher integrity needed to prevent controller workload increases when faced with trajectory changes being entered into the ground automation directly from the aircraft rather than the prior controller. The frequency of occurrence of these changes being unacceptable and requiring controller modification will have to be very low. Final determination of the ABTM 1-4 FEC will require FAA review and assessment of the ABTM safety cases similar to what is presented in this report, but in greater detail and with risk quantification.

The Intended Function of ABTM 5 and analysis of the induced safety effects supports a FEC of Major. This finding results from analysis of the Intended Functions of ABTM 5 including both tactical and strategic primary separation. It is expected that a much more thorough formal safety assessment of ABTM 5 will be performed, supported by performance data collected from the separation software through years of its use in ABTM 1-4.

9. References

[1] Cotton, W.B., Hilb, R., Koczo, S., and Wing, D. *A Vision and Roadmap for Increasing User Autonomy in Flight Operations in the National Airspace.* Accepted to the AIAA 16th Aviation Technology, Integration, and Operations Conference, Washington DC, 2016.

[2] Ballin, M.G., and Wing, D.J., Traffic Aware Strategic Aircrew Requests (TASAR), AIAA-2012-5623, AIAA 12th Aircraft Technology, Integration, and Operations Conference (ATIO), Indianapolis, IN, September 2012.

[3] Henderson, J. Traffic Aware Strategic Aircrew Requests (TASAR) Concept of Operations, NASA/CR=2013-218001, Engility Corporation, May 2013.

[4] Wing, D.J. and Cotton, W.B., For Spacious Skies: Self-Separation with "Autonomous Flight Rules" in US Domestic Airspace, AIAA-2011-6865. 11th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference, Virginia Beach, VA, 2011.

[5] Wing, D.J. and Cotton, W.B., Autonomous Flight Rules: A Concept for Self-Separation in U.S. Domestic Airspace, NASA/TP-2011-217174, November 2011.

[6] Society of Automotive Engineers (SAE), Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE Aviation Recommended Practice (ARP) 4761, SAE International, 1996.

[7] Federal Aviation Administration, System Design Analysis, Advisory Circular (AC) 25.1309-1, 1982.

[8] Federal Aviation Administration, System Safety Analysis and Assessment for Part 23 Airplanes, AC 23.1309-1, 2011.

[9] RTCA, Guidelines for Approval of the Provision and Use of Air Traffic Services supported by Data Communications, DO-264 (also EUROCAE ED-78A), 2000.

[10] Koczo, S., TASAR Certification and Operational Approval Requirements – Analyses and Results, NASA/CR-2015-218708, May 2015.

[11] Koczo, S., Analysis of Operational Hazards and Safety Requirements for Traffic Aware Strategic Aircrew Requests (TASAR), NASA/CR-2013-218002, May 2013.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 04 - 2016	Technical Memorandum	09/01/2015 to 01/31/2016

4. TITLE AND SUBTITLE

Preliminary Assessment of Operational Hazards and Safety Requirements for Airborne Trajectory Management (ABTM) Roadmap Applications

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Cotton, William B.; Hilb, Robert; Koczo, Stefan; Wing, David J.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

330693.04.30.07.05

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER

L-20681

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)

NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

NASA-TM-2016-219176

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 03
Availability: NASA STI Program (757) 864-9658

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A set of five developmental steps building from the NASA TASAR (Traffic Aware Strategic Aircrew Requests) concept are described, each providing incrementally more efficiency and capacity benefits to airspace system users and service providers, culminating in a Full Airborne Trajectory Management capability. For each of these steps, the incremental Operational Hazards and Safety Requirements are identified for later use in future formal safety assessments intended to lead to certification and operational approval of the equipment and the associated procedures. Two established safety assessment methodologies that are compliant with the FAA's Safety Management System were used leading to Failure Effects Classifications (FEC) for each of the steps. The most likely FEC for the first three steps, Basic TASAR, Digital TASAR, and 4D TASAR, is "No effect". For step four, Strategic Airborne Trajectory Management, the likely FEC is "Minor". For Full Airborne Trajectory Management (Step 5), the most likely FEC is "Major".

15. SUBJECT TERMS

Airborne trajectory management; Autonomy; Operational hazards; Roadmap; Safety requirements; TASAR

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	31	(757) 864-9658