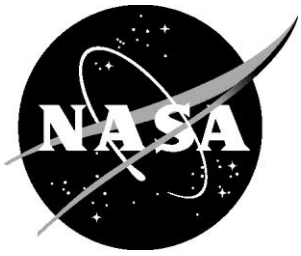
NASA/CR–2013-218002



Analysis of Operational Hazards and Safety Requirements for Traffic Aware Strategic Aircrew Requests (TASAR)

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

May 2013

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 NASA Aeronautics and Space Database and its public interface, the NASA Technical Report 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 counterpart of peer-reviewed formal professional papers, but having 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*

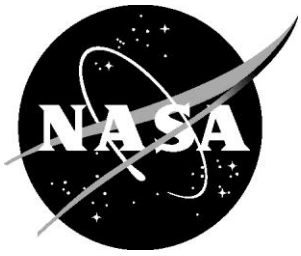
- E-mail your question to help@sti.nasa.gov

- Fax your question to the NASA STI Information Desk at 443-757-5803

- Phone the NASA STI Information Desk at 443-757-5802

- Write to:
  STI Information Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/CR–2013-218002



Analysis of Operational Hazards and Safety Requirements for Traffic Aware Strategic Aircrew Requests (TASAR)

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

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

Prepared for Langley Research Center
under Contract NNL12AA11C

May 2013

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

Preface

This document presents results of an analysis of operational hazards and safety requirements for Traffic Aware Strategic Aircrew Requests (TASAR). The document was prepared by Rockwell Collins, Inc., Cedar Rapids, IA under Contract No. NNL12AA11C with NASA Langley Research Center, Hampton, VA. The NASA Technical Monitor is David J. Wing.

Table of Contents

List of Figures

1. Introduction

This report provides the results of safety analyses performed for the NASA Traffic Aware Strategic Aircrew Requests (TASAR) application [1] to identify Operational Hazards and Safety Requirements for TASAR as an application that can be hosted on a Portable Electronic Device (PED) / Portable Electronic Flight Bag (EFB). Two safety assessment methodologies were used that are compliant with the Safety Management System (SMS) of the Federal Aviation Administration (FAA):

Method 1 A traditional safety assessment featuring an 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 Aviation Recommended Practice (ARP) 4761 [2], Advisory Circular (AC) 25-1309 [3] and AC 23-1309 [4] for Part 23 and Part 25 aircraft operations

Method 2 Operational Safety Analysis according to RTCA DO-264 / EUROCAE Document (ED) 178A [5].

Section 2 of this report provides a high-level description and assessment of the two safety methodologies.

The intended function of TASAR is to serve as an advisory-only, decision support tool to the pilot / flight crew to offer trajectory change request (Change Request) recommendations for improvement opportunities to the current flight plan. Section 3 briefly reviews the Change Request process as it is used in today"s operations.

Section 4 provides a high-level overview and description of the TASAR concept of operation. Section 5 describes the intended function of TASAR whose safety case is evaluated. The safety analyses using Method 1 and Method 2 are presented in Sections 6 and 7, respectively. Section 8 serves as a report summary, followed by list of references in Section 9.

2. Approach to Safety Assessment

Two safety assessment approaches were used to determine the Failure Effects Classification for TASAR. The Failure Effects Classifications are based on Operational Hazards and available mitigations that were identified using these two methods. The two safety analyses conclude that the worst case failure effects for TASAR will likely be of "No Effect" Failure Effect Classification and no higher than "Minor" Failure Effect Classification. This determination is subject to evaluation and approval by cognizant FAA certification and operational approval organizations responsible for authorization of EFB applications. Supporting rationale for the "No Effect" designation is provided in the safety analyses in Sections 5 and 6.

Note: In addition to the safety analyses documented in this report, a parallel effort examined "EFB Standards Adherence Requirements for TASAR" [6]. The analysis identifies requirements for TASAR as an EFB application, while considering EFB hardware, software, mounting, Class of EFB (i.e., 1, 2, 3), Type of EFB software (i.e., A, B), etc. The results from [6] and from this report designate TASAR as likely a "No Effect" Failure Effect Classification and no higher than "Minor" Failure Effect Classification. Additional efforts are in progress that will result in artifacts appropriate for seeking TASAR EFB certification and operational approval.

2.1. Method 1 Safety Assessment

Method 1 is based on the analyses indicated by ARP-4761, AC 25-1309, AC 23-1309 and 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 Change Request(s), etc.

3) Examine the effect of the these failures on aircraft, pilot (or flight crew), and Air Traffic Control (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 is based on RTCA DO-164 / ED-78A and represents a system-of-systems analysis approach that is well-suited for allocating safety requirements across a high-criticality, 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 TASAR. 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.

Method 2 follows the following evaluation steps:

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, etc.
   c. Determine the Severity Classes for each Operational Effect, e.g., Catastrophic, Major, Minor, etc., and identify the maximum allowable probability of occurrence of the Operational Effect
   d. Determine the Effects Probabilities, which represent the probabilities of available mitigation(s) 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) 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 Change Request process in today"s operations between the pilot and ATC for making Change Requests to the current flight plan. 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, pilot requests are often made with little or no awareness of the traffic situation 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 sector procedures 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 ATC
2) Discourages the pilot from making future requests to improve their flight
3) Flight improvement opportunities are often unrealized because pilot may not be aware of requests that would improve efficiency and be ATC approvable.

In general, the pilot seeking opportunities of improved safety, efficiency, or ride quality has rather 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 lack of situational awareness of the external environment that may constrain changes to the flight plan.

The next section explores a new TASAR capability that serves as an advisory-only tool to the pilot, providing informed Change Request candidates for pilot consideration as possible Change Requests to ATC for operational benefit.

4. TASAR Overview / High-Level Description

The TASAR EFB application [1] is currently being developed by NASA in order to leverage emerging flight deck technologies for cost benefits to current flight operations [7,8]. Among the systems technologies that comprise or support TASAR are flight-optimizing software algorithms, a software hosting device such as a PED EFB, Automatic Dependent Surveillance Broadcast (ADS-B) In and other sources of traffic information, and additional ground-based information via data link, internet connectivity, etc. TASAR seeks to provide cost-beneficial optimization with respect to the current flight plan, 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, airspace constraints, and / or improved timeliness and accuracy of information about factors that affect the aircraft‟s execution of its flight plan).

The TASAR EFB application (referred to here as TASAR) is a flight deck-based decision support tool that seeks to identify and recommend trajectory improvement opportunities to the pilot that have high probability of approval by ATC. Utilizing available information of own-ship flight status and plan, and airspace environment (e.g., proximate traffic, weather, winds, ATC system status, etc.), TASAR seeks to identify and recommend candidate trajectories for consideration by the pilot that have higher probability of ATC approval. The pilot, at his or her discretion, can choose to issue a Change Request to ATC based on TASAR recommended trajectory change candidates.

Prior to recommending trajectory change candidates to the pilot, TASAR performs the following steps, 1) it evaluates the proposed trajectory change(s) against available on-board traffic data for potential conflicts, and 2) it may account for known ATC sector rules and own-ship flight position relative to the sector. Thus, recommended Trajectories Change Request 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 Change Requests:

1) Have a high potential for approval by ATC by considering ATC preferences in the identification process
2) Meet operational goals for the flight, as provided by pilot preferences that are input to TASAR
3) Provide improvement to the current flight plan in terms of time and / or fuel saved or other desired attributes such as passenger comfort.

TASAR Change Request candidates are advisory-only to the pilot, and the pilot has full discretion on whether or not to select a TASAR-provided trajectory change for a subsequent Change Request to ATC. Pilot training ensures that aviate-navigate-communicate piloting tasks, procedures, and coordination with ATC (e.g., Change Requests) are followed as in today‟s operations. The pilot has responsibility to evaluate TASAR-provided trajectory change candidates before making a Change Request to ATC to minimize spurious Change Requests from being made to ATC. As in today‟s operations, ATC has separation responsibility, and ATC will not approve Change Requests from the pilot that do not meet ATC constraints and requirements.

5. Intended Function Description

TASAR is a flight deck-based decision aid consisting of software automation algorithms and a textual display and is intended as an advisory-only service to the pilot to seek trajectory improvement opportunities over the current flight plan. TASAR is expected to be implemented as a hosted software application on an EFB. A Class 2 EFB installation is anticipated, with TASAR becoming a future Type B software application, pending successful certification and operational approvals by FAA (refer to [6] for a comprehensive assessment of FAA EFB regulations and guidance on PED / Portable EFB-based flight deck applications). The TASAR EFB will interface to 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 flight objectives and optimization criteria), 2) on-board avionics systems, and 3) airborne internet data connectivity, the TASAR application computes available Change Request candidates that may improve the current flight plan. Change Request candidates provided by TASAR are intended to have relatively high probability of ATC approval if requested by the pilot, as TASAR seeks to provide flight-optimizing, traffic-avoiding recommended trajectory candidates that anticipate ATC and airspace constraints.

The pilot has full discretion on the use of TASAR-provided Change Request information; they can choose to use TASAR-recommended Change Request candidates as part of a Change Request to ATC, or they can choose to ignore them. TASAR can be manually inhibited at any time, for any reason. Thus, in the event of observed spurious behavior of TASAR due to any system failure, inaccurate data obtained via network enabled information sources, or TASAR being a source of distraction to the flight crew, the pilot can simply inhibit or ignore TASAR. By following their training, the pilot can manage the use of TASAR in such away so that TASAR will not result in any workload increase in the flight deck.

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 TASAR display is passive with no graphical display of traffic or audible alerting. Loss of the TASAR EFB application for any reason does not affect the Minimum Equipment List (MEL) and does not affect normal flight operations.

TASAR information sources may include the following:

1) Own-ship systems (aircraft state, auto-flight settings, flight plan and performance information from Flight Management System (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 Activity Airspace, etc.)
4) Weather status / forecast
5) Wind status / forecast
6) Operator flight planning, preferences, and objectives.

6. Method 1 Safety Analysis – Conventional Method

This section addresses the safety assessment of TASAR using the traditional system safety process based on ARP 4761 [2], AC 25-1309 [3], and AC 23-1309 [4]. As noted earlier in Section 2, this safety assessment method analyzes the TASAR intended function (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 of the TASAR application. The Failure Effects Classification then drives the development and validation requirements and processes to be followed in integrating TASAR 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 Failure Effect Classification of TASAR

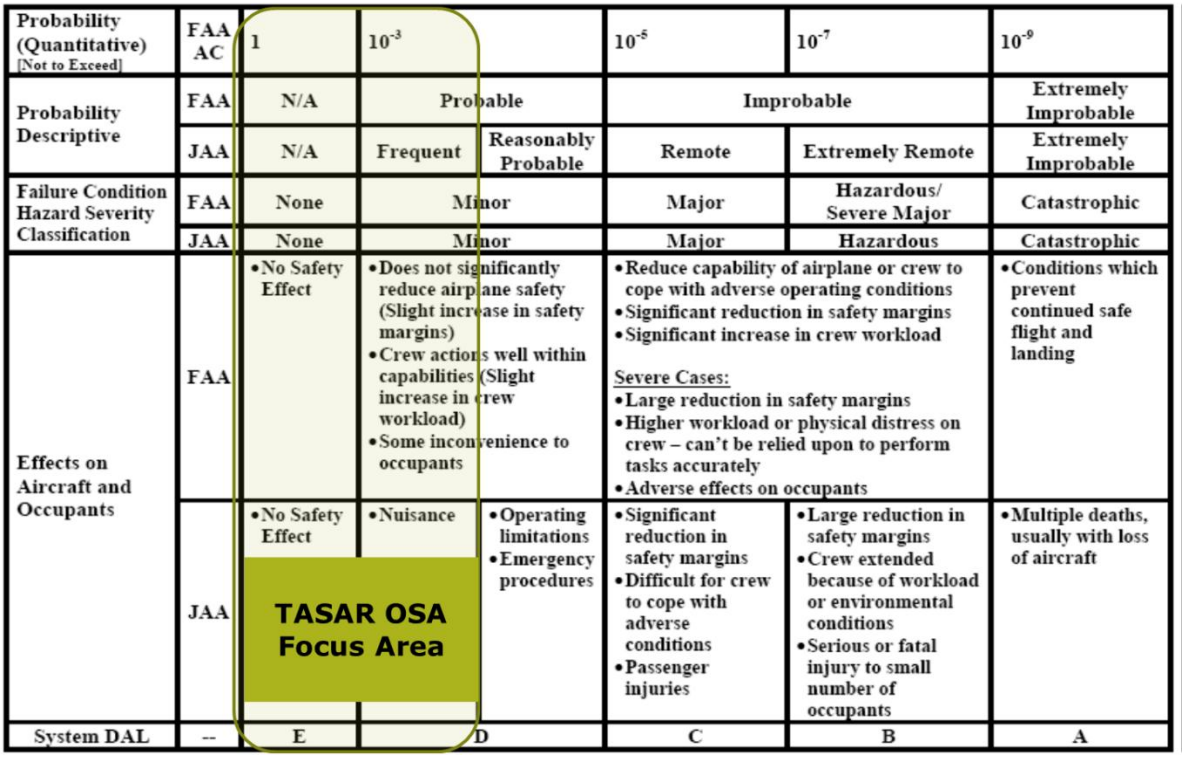
The following list represents key factors that influence the determination of the Failure Effect Classification for TASAR:

1) TASAR is a supplemental system and thus is not relied on by critical functions supporting flight deck operations
2) TASAR is optional, i.e., not a required system for flight operations. In the event of failures of the TASAR system, TASAR can be ignored or disabled without adversely affecting operations
3) TASAR has no MEL requirement
4) TASAR can be manually inhibited at any time, for any reason:
   a. Detected failure of the TASAR application
   b. Detected failure of the host EFB
   c. Spurious or inconsistent performance of recommended Change Requests
   d. Distracting effects of TASAR to the pilot
5) Presence or loss of TASAR does not change responsibilities of the pilot for flight operations
6) TASAR is an "advisory-only" system (i.e., does not provide guidance information):
   a. Pilot is not reliant on TASAR outputs to any extent to perform flight operations
   b. Pilot can choose to either utilize or ignore Change Requests candidates recommended by TASAR as part of Change Requests to ATC
7) Change Request procedures are unchanged:
   a. Pilot must direct all Change Requests to ATC using conventional means
   b. ATC is responsible for reviewing request 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) Undetected, misleading information associated with TASAR outputs, i.e., with one or more candidate Change Request recommendations, will have "No Effect" on the pilot, aircraft, and/or on ATC. Whether due to failure of one of the TASAR 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 by mitigation associated with the existing Change Request process.

6.2. Failure Effects Classification

Figure 1 (from [3]) provides a mapping of the "Effects" due to failures and the allowable "Probability of Occurrence" that lead to the determination of the Failure Effects Classification of the planned application (i.e., TASAR). Based on the above noted factors alone, this safety analysis (Method 1) concludes that TASAR can be safely developed and implemented with a "No Effect" designation. Potentially, in the worst case, TASAR could rise to a "Minor Effect" designation in event of inconsistent candidate 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 TASAR, as the pilot can simply ignore TASAR for any reason. Through proper training in the use of TASAR, the pilot should not allow to be distracted or be adversely influenced in using TASAR while conducting flight operations. From an ATC perspective, controllers will continue to conduct the Change Request process as in today"s operation and are not expected to experience a workload issue due to TASAR.

Final determination of the Failure Effects Classification for TASAR 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.



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 Severe Cases: •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) (from [3])

6.3. Internal Mitigation Means

The TASAR application itself provides additional inherent capabilities that further reduce the possibility of unintended adverse effects and are expected to enhance the usability of the application. The following TASAR capabilities further serve to strengthen and support the "No Effects" Failure Effects Classification for TASAR:

1) In order to prevent lengthy, complex Change Requests from the pilot to ATC, TASAR utilizes standard navigation databases and places limits on excessive waypoints included in the recommended Change Requests it provides

2) TASAR displays flight path change opportunities using standard flight planning textual depictions to facilitate voice communications

3) TASAR may include capabilities to assess sector complexity and own-ship"s proximity to the sector boundary in order 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 TASAR is that there is no "recovery" time required for the flight crew associated with its use. In other words, in using TASAR, the pilot remains on an ATC-cleared trajectory at all times. In the event of a TASAR system fault, the pilot need only remain on the current clearance while disregarding the TASAR display. A ***simple reset of TASAR, or by simply choosing to ignore TASAR inputs*** (e.g., by not looking at the TASAR display) allows the pilot to continue to focus on aviate-navigate-communicate priorities in conducting flight operations (whether during normal operations or in the event of abnormal or emergency situations).

2) The pilot has ***responsibility to evaluate TASAR-provided Trajectory Change Request candidates before making a Change Request*** to ATC, providing cross-check opportunities to detect spurious or false Trajectory Change Request candidates being offered by TASAR

3) Aircraft systems, e.g., FMS, weather radar, serve as available, higher integrity information allowing ***quick check on acceptability*** and performance impacts of TASAR recommended Change Requests

6.5. Phase of Flight Considerations

From a phase of flight perspective, TASAR is intended for use primarily during en-route operations. Change Request candidates are offered by TASAR during the later portion of climb, while en-route, and to a lesser extent, into the early portion of descent operations. TASAR is thus used primarily during non-critical phases of flight, i.e., above 10,000 ft.

6.6. Information Source Quality

Due to the "No Effect / Minor Effect" Failure Effects Classification anticipated for TASAR, information source quality and integrity must be commensurate to support this Failure Effects Classification. TASAR input information quality and integrity requirements are driven more by operational use issues than by safety considerations. Low quality and/or misleading information can result in poor recommendations to the pilot for candidate Change Requests. The net effect is that TASAR will not be as effective in achieving envisioned operational benefits (e.g., time or fuel saved).

6.7. Undetected Failure – Worst Case Effect

In the event of an undetected failure of the TASAR automation, inefficient routing is the only adverse outcome. Existing mitigation of any safety hazards is provided by ATC, as already is done for Change Requests today without TASAR.

Note: The Safety Analysis using Method 2 described in the next section takes a closer look at specific failure modes of TASAR.

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 [5], referred to as Method 2 in this report. Figure 2 illustrates the process at a high-level using the „bow-tie" model.

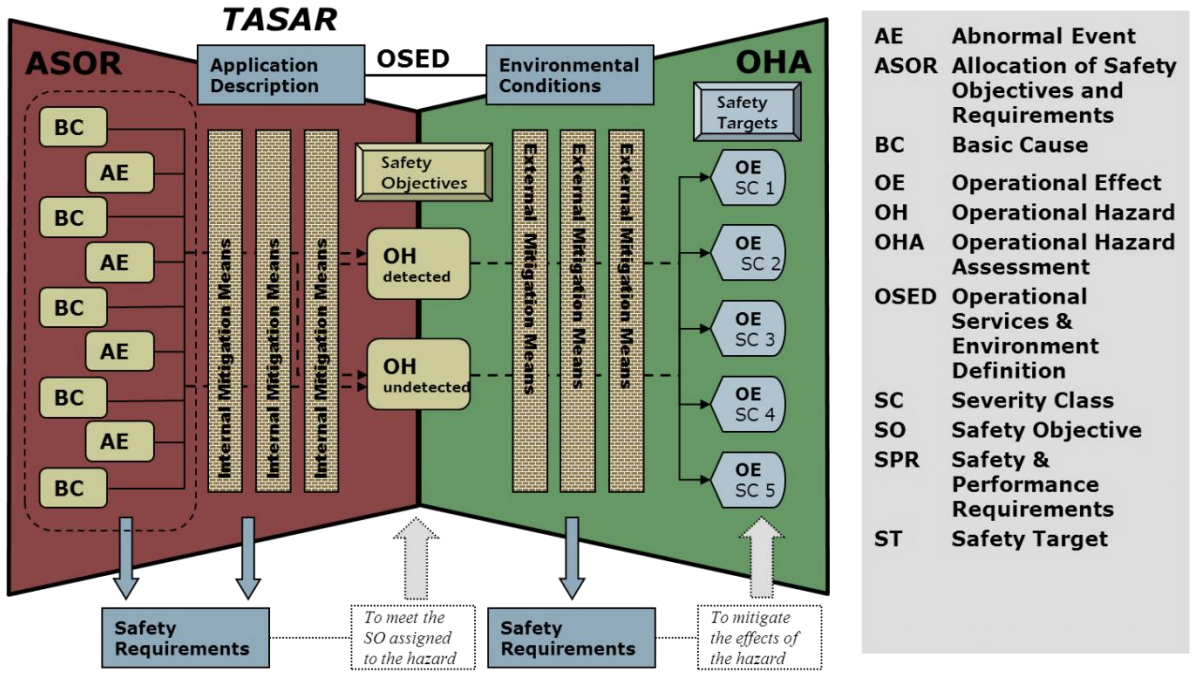


Figure 2 Operational Safety Assessment Process – Method 2

In Figure 2, the system of interest, in this case the TASAR application, is represented in the left-hand side of the bow-tie. The external environment in which the application operates, 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., TASAR). For each identified Operational Hazard, the next step is to determine the worst "credible" outcome, also referred to as the Operational Effect (OE). Examples are collision, loss of separation (major loss versus minor loss), workload, etc.

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 are established, ranging from 10^{-9}, 10^{-7}, 10^{-5}, 10^{-3}, etc. 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 TASAR Operational Safety Assessment process described in this section are highlighted in Figure 3. The highlighted regions represent "Minor" and "No Effects" Failure Effect Classifications.

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 in ATC capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.
Example of ASAS operational consequences	• Mid-air collision • Controlled flight into terrain • Total loss of flight control • High speed surface movement collision (i.e. collision in runway) • Leaving a prepared surface at high speed.	• Large reduction in separation or safety margins • Loss of separation resulting in wake vortex encounter at low altitude. • Large reduction in safety margins like abrupt manoeuvre is required to avoid mid-air collision or CFIT (e.g. one or more aircraft deviating from their intended clearance) • Large reduction in aircraft functional capabilities • Total loss of air traffic control for a significant period of time	• Significant reduction in separation or safety margins • Loss of separation resulting in wake vortex encounter at high altitude. • Low speed surface movement collision (i.e. collision in taxiway) • Leaving a prepared surface at low speed • Significant reduction in aircraft functional capabilities • Significant reduction in air traffic control capability	• Slight reduction in separation or safety margins • Significant increase in air traffic controller workload • Slight increase in flight crew workload	• No effect on operations /traffic • Slight increase in air traffic controller workload • No effect on flight crew

TASAR OSA Focus Areas

Figure 3 ED78A/DO264 Based Hazard Classification Matrix

From the OHA sub-process, each Operational Hazard is assigned a Safety Objective that must be met 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 the specification of 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 in [5] 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 of the 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.

While the strength of the OSA process is that it is able to analyze complex, high-criticality system-of-systems and 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., TASAR, 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 performance of the human to perform various functions. This often times becomes a significant and time consuming (and costly) issue in gaining approval for the safety requirements that result from using the methodology.

Note: Considerable consideration has been given in this report to the identification of operational hazards potentially associated with TASAR. 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 TASAR was determined to have a "No Effect" or in worst case a "Minor" Failure Effects Classification. The OSA presented is thus an abbreviated OSA relative to [5].

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. The next step takes a closer look at Operational Hazards that could occur using the TASAR application.

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., TASAR automation). Abnormal Events include both errors by the pilot in relation to TASAR use and in interactions with ATC as part of the Change Request procedure.

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

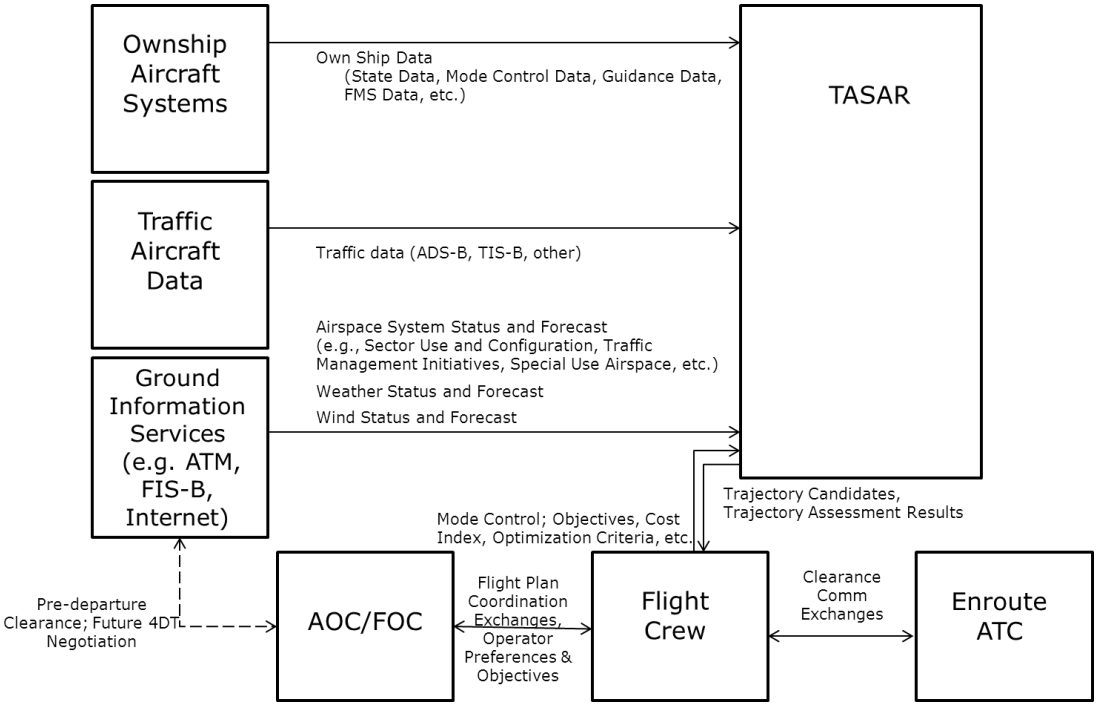


Figure 4 TASAR Functional Diagram

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

The following sections address potential sources for errors and misleading information that may result in Operational Hazards stemming from information exchanges associated with human and automation processing actions as illustrated in Figure 4.

7.2. 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):

1) Pilot, flight crew

   a. Enters TASAR configuration, objectives, and optimization criteria via the TASAR human machine interface (HMI)

   b. Receives and interprets TASAR data via the TASAR HMI (e.g., recommended trajectories, conflict status, fuel reserve status, etc.)

   c. Communicates Change Requests to ATC

2) Air Traffic Controller (en-route)

   a. Provides separation assurance services

   b. Communicates Change Request clearances to pilots

Note: As the detailed design for TASAR is being developed, there is a concern that some route and constraint data may not be readily accessible from onboard systems and that it may be necessary that some of this data be manually entered by the pilot. This raises the potential of increased pilot workload that may become a concern for usability of the TASAR application and could factor into the operational safety assessment as a workload issue; it may also increase the possibility of false data entry by the pilot.

7.3. Automation Processing Actions Potentially Leading to Basic Causes

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

TASAR-related processing that could result in undetected misleading information.

Any misleading information provided by information sources to TASAR, or errors and failures in TASAR automation processing, could potentially result in misleading Change Request candidates being recommended to the pilot for consideration. Such misleading information may detract from the usability of TASAR to achieve operational benefits. However, since the flight crew has no authority to deviate from their ATC clearance, regardless of the information provided by TASAR, any occurrence of misleading information from TASAR will be non-hazardous in nature and is completely mitigated by the ATC clearance procedure.

7.4. Potential Basic Causes

The following represent potential Basic Causes associated with TASAR erroneous information:

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

2) Wind data is of poor quality or is incorrect leading to Change Requests that are conflicted or lead towards hazardous airspace

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 hazardous airspace

5) Detected errors, failures, or poor quality TASAR recommendations leading to pilot troubleshooting and therefore additional workload

6) Undetected errors or failures of TASAR computations leading to poor or multiple Change Requests and additional pilot or ATC workload

7) Undetected errors or failures of TASAR computations leading to hazardous encounters with weather, terrain, Special Activity Airspace, etc.

8) TASAR application preoccupies the pilot from observing flight-deck hazard alerts

7.5. Potential Operational Hazards and Mitigations

The following represents the detailed list of Operational Hazards (OH) that have been identified using the OSA process described in this section. Associated mitigations, internal or external to TASAR, are also identified.

OH – 1: TASAR provides one or more Change Request candidates that are not conflict free

This Operational Hazard 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 TASAR.*

OH – 2: Pilot misinterprets TASAR candidate and unknowingly requests a trajectory clearance that is not conflict free or leads toward hazardous airspace

TASAR "inadvertently" misleads or confuses pilot who misrepresents TASAR Change Request recommendation to ATC.

Mitigation *– ATC provides separation assurance independent of TASAR*.

Mitigation *– Aircraft safety systems (e.g., Traffic Alert and Collision Avoidance System, weather radar, Terrain Awareness and Warning System) provide hazard detection and alerting.*

OH – 3: Pilot follows the wrong trajectory clearance following receipt of amended clearance from ATC

The pilot requests a change recommended by the TASAR system, and although ATC amends the request, TASAR-induced confusion leads the pilot to follow the request instead of the clearance.

Mitigation *– ATC monitors execution and intercedes (same as today)*.

Mitigation *– Pilot training*.

Mitigation *– Pilot crosschecks clearance with FMS*.

OH – 4: ATC, somehow being aware of TASAR capability for the aircraft / pilot requesting a Change Request to the flight plan, is less vigilant to provide separation assurance

The concern is whether ATC could become complacent over time, when receiving TASAR requests. Note that TASAR equipage is not specified on filed flight plans or included in pilot-request verbiage.

Mitigation *– Existing ATC procedure to check all requests for separation*.

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

OH – 5: TASAR provides numerous spurious and/or inconsistent series of Change Request candidates leading to multiple requests

If Change Request recommendations are not reinforced from one request to the next, multiple counteracting requests could be issued.

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

Mitigation *– ATC denies user requests if workload is too high*.

OH – 6: TASAR recommends a trajectory candidate with miscomputation of fuel burn

Pilot reliance on TASAR fuel burn estimates (prevented to help pilots choose between multiple request options) could lead to greater fuel burn than expected.

Mitigation *– Pilot crosschecks of FMS prediction of fuel burn*.

OH – 7: Unexpected weather develops on TASAR 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 potentially be workload for pilot and controllers. Since TASAR is an advisory-only system and can be manually inhibited by the pilot at any time, for any reason, the most likely Failure Effect Classification for TASAR would be "No Effect". With the "No Effect" or perhaps "Minor" Failure Effect Classification, TASAR is amenable for integration as an EFB application. As noted previously, TASAR is intended for a Class 2 EFB and Type B software application or an equivalent type of software category yet to be determined by FAA approvers.

8. Summary

This report provides the results of safety analyses of the NASA TASAR application. TASAR is intended to be integrated as a PED EFB software application. TASAR is an optional, advisory-only decision support tool to recommend trajectory change improvement opportunities to the pilot for operational efficiency improvements to flight operations. As such, TASAR is supplemental equipment, does not replace any required avionics functions, and is not needed as part of the MEL for flight operations. Use of TASAR is at the discretion of the pilot, i.e., the pilot may choose to ignore TASAR or can manually inhibit its operation at any time for any reason.

Two safety analysis methods were followed to determine the expected Failure Effects Classification for TASAR, 1) a traditional system safety process based on ARP 4761 [2], AC 25-1309 [3], and AC 23-1309 [4], and 2) an Operational Safety Assessment using the methodology of RTCA DO-264 / EUROCAE ED-78A [5]. Due to the relatively low-criticality of the TASAR application per the description of the TASAR Intended Function in Section 5, and the availability of a number of significant mitigation barriers used in today"s operations that greatly reduce the probability of TASAR-induced safety effects, **both analyses support a TASAR Failure Effects Classification of "No Effect" and no higher than a "Minor" effect.** Final determination of the TASAR Failure Effects Classification will require FAA"s review and assessment of the TASAR safety case similar to what is presented in the report.

In a separate companion study to this report, an assessment of TASAR was made to determine EFB Standards Adherence Requirements [6]. From an EFB software and application perspective, TASAR, as a new application, does not map directly into already defined Type A or Type B applications. The TASAR application has many of the characteristics of a Type B application, yet it is somewhat less stringent than typical Type B applications in terms of Failure Effect Classification per its intended function. In addition, TASAR is expected to be implemented as a Class 2 PED EFB. The Class 2 EFB requirement is due to the read-only interface needed by TASAR to on-board avionics systems, and data link connectivity via installed antennas for accessible information sources, e.g., weather information, etc. As a Class 2 EFB, a mounting device is required for operators to use TASAR. The safety assessments made in this report are consistent with the EFB Standards Adherence Requirements identified in [6].

Following the assessments made and documented in this report, and in conjunction with the analysis of EFB Standards Adherence Requirements, the next steps of the TASAR EFB Certification and Operational Approval process are to 1) develop a plan for TASAR certification and operational approval, and 2) develop representative artifacts for such approvals in order to conduct an approval „dry run" with a Designated Engineering Representative. The resulting artifacts will serve as initial inputs in support of initial applicants engaging with FAA for actual TASAR certification and operational approval.

9. References

[1] Henderson, J., *Traffic Aware Strategic Aircrew Requests (TASAR) Concept of Operations*, NASA Contractor Report submitted for publication, NASA Contract NNL12AA06C, 2013.

[2] Society of Automotive Engineers, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, SAE ARP 4761, December 1996.

[3] Federal Aviation Administration, *System Design and Analysis*, AC 25.1309-1, September 1982.

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

[5] RTCA, *Guidelines for Approval of the Provision and Use of Air Traffic Services supported by Data Communications*, DO-264 / EUROCAE ED-78A, March 2002.

[6] Koczo, Stefan, *EFB Standards Adherence Requirements for TASAR*, NASA Contract NNL12AA11C, Deliverable #5 Report, Rockwell Collins, October 2012.

[7] 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.

[8] Henderson, J., Wing, D.J., and Idris, H., *Preliminary Benefits Assessment of Traffic Aware Strategic Aircrew Requests (TASAR)*, AIAA-2012-5684, AIAA 12th Aircraft Technology, Integration, and Operations Conference (ATIO), Indianapolis, IN, September 2012.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 05 - 2013	Contractor Report	

4. TITLE AND SUBTITLE

Analysis of Operational Hazards and Safety Requirements for Traffic Aware Strategic Aircrew Requests (TASAR)

5a. CONTRACT NUMBER

NNL12AA11C

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Koczo, Stefan, Jr.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

411931.02.03.07.13.03

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

NASA Langley Research Center
Hampton, Virginia 23681

8. PERFORMING ORGANIZATION REPORT NUMBER

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/CR-2013-218002

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 03
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

Langley Technical Monitor: David J. Wing

14. ABSTRACT

Safety analyses of the Traffic Aware Strategic Aircrew Requests (TASAR) Electronic Flight Bag (EFB) application are provided to establish its Failure Effects Classification which affects certification and operational approval requirements. TASAR was developed by NASA Langley Research Center to offer flight path improvement opportunities to the pilot during flight for operational benefits (e.g., reduced fuel, flight time). TASAR, using own-ship and network-enabled information concerning the flight and its environment, including weather and Air Traffic Control (ATC) system constraints, provides recommended improvements to the flight trajectory that the pilot can choose to request via Change Requests to ATC for revised clearance. This study reviews the Change Request process of requesting updates to the current clearance, examines the intended function of TASAR, and utilizes two safety assessment methods to establish the Failure Effects Classification of TASAR. Considerable attention has been given in this report to the identification of operational hazards potentially associated with TASAR.

15. SUBJECT TERMS

ADS-B; Air traffic control; Operational hazards; Optimization; Safety; 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	21	(443) 757-5802