Aviation Rulemaking Advisory Committee (ARAC)
Transport Airplane and Engine (TAE) Issues Area

Meeting Minutes

Date: May 20, 2008 (ad hoc)
Time: 10:30 a.m. EDT
Location: Washington, DC

Call to Order/Administrative Reporting

Mr. Craig Bolt (Assistant Chair) called the meeting (teleconference) to order at 10:30 a.m. Mr. Mike Kaszycki (Assistant Executive Director) read the Federal Advisory Committee Act statement.

Craig Bolt	Assistant Chair	Keith Barnett	Bombardier
Mike Kaszycki	Assistant Executive Director	Walter Desrosier	GAMA
Reid Barton	SMA Group	Rolf Greiner	Airbus
Sarah Knife	GE Aviation	Linh Le	FAA
Bill Ertle	PATS DAS	CW Robertson	Cessna
Doug Kihm	Boeing	Tom Peters	Embraer
Rob Skresvig	Gulfstream	Halls Larsen	FAA
Roger Knepper	Airbus (ASAWG Co-chair)	Mike Bartron	PW
Ranee Carr	AIA	Dave Lotterer	RAA
Suzanne Masterson	FAA	Joe Bracken	ALPA
Nic Davidson	FAA	Web Heath	Boeing

Mr. Bolt began the discussion by stating that there was only one agenda item for this ad hoc meeting of the TAEIG, and that item he said concerned the Airplane Level Safety Analysis Working Group (ASAWG). He continued by stating that the working group had submitted its report on Task 3 **[handout #1]** and that the intent of this meeting was to discuss that report and then proceed with a vote regarding submission of the report to the FAA.

Mr. Bolt then asked for introductions from the participants in the teleconference and then stated that Mr. Roger Knepper (Airbus), co-chair of the ASAWG would conduct a briefing, and then Mr. Doug Kihm from Boeing would also share some information as well. Mr. Knepper began his summary presentation which was also available to participants by "Webex" with a review of the Statement of Issue and the assignment of the Specific Risk Tasking by the FAA in March 2006. Mr. Knepper continued with a review of the scope of the tasking, and group membership, adding that there had been very good participation within the group.

He stated that tasks 1 & 2 had been completed and reported to the TAEIG in March and October 2007 respectively. Mr. Knepper further added that Task 2 focused on identifying the relevant

requirements, guidance and recommendations that related to specific risk and its use. He continued, stating that Task 3 had been completed in April, 2008 according to plan. Mr. Knepper reminded all that for the purpose of its work, the ASAWG had been subdivided into four working groups, with each evaluating adequacy, appropriateness and applicability across systems, as a means of identifying "fundamental issues". From these fundamental issues, the subgroups were to summarize, evaluate and provide recommendations for the Task 4 work. Mr. Knepper also advised that the Task 3 report included comments from throughout industry and from regulators and had been dispositioned by the Working Goup. Mr. Knepper added that moving intoTask 4, the Latent and Active failure subgroups would be merged due to their similarities. Mr. Knepper stated that the ASAWG had four meetings remaining and was attempting to complete Task 4 by March 2009.

Mr. Kaszycki asked Mr. Knepper if all the working group reports through Task 3 had the full concurrence of all the working group members, to which Mr. Knepper replied that though there was some controversy, the final reports did have full consensus of all working group members. Ms. Sarah Knife (GE Aviation) indicated to Mr. Knepper that regarding the matter of consensus she had been informed otherwise. Ms. Knife stated that she had been informed of instances in which "a majority of team members" had recommended that certain issues be "closed" but group chairs insisted on moving those issues to Task 4. Mr. Walt Derossier (GAMA) mentioned that he knew comments were dispositioned as part Task 3, and asked Mr. Knepper if there was still a consensus within the group after that point. Mr. Knepper replied that it was his own "understanding" that such was the case. He expounded on this point by using MMEL as an example of what he considered to have been the most controversial subject, having reached a recommendation through consensus. Mr. Knepper stated that a similar situation had occurred with "aging and wear" but that consensus was finally achieved in that subject area as well. Ms. Knife then inquired of Mr. Knepper as to how much time the working group members had to review the final Task 3 report. Mr. Knepper responded that it was approximately a week for the actual report, however much of the report's contents (approximately 80%) had been made available to all group members months in advance.

Mr. Kihm stated that it was not clear how general consensus versus minority opinion were handled on the working group and that it was perceived by some members that approximately 20% of the decisions made in the development of the Task 3 report were made in the latter stages, and that those decisions were not necessarily consensus decisions. Ms. Knife added that this was also the information she had received. Mr. Knepper reiterated that the only subjects that were decided in the last working group meeting were MMEL and aging and wear (both of which were earlier identified as consensus decisions).

Mr. Kihm then asked Mr. Knepper to clarify some perceived conflicting information on the MMEL Task Group slide in his summary presentation. He indicated to Mr. Knepper that the text in the presentation appeared to advocate standards which required the use of numerical probability analysis for evaluating a specific risk MMEL dispatch condition as opposed to that analysis being an option. Mr. Kaszycki stated that his understanding of this text was that it was not meant to mandate numerical probability analysis, but instead only state that a policy should exist if the analysis is used. Mr. Knepper indicated that Mr. Kaszycki's assessment was correct.

Mr. Kihm stated that his expectation at this point was that a determination as to the necessity of numerical probability analysis would already have been reached. Mr. Knepper responded that he felt the actions of the Working Group were consistent with the guidelines established in the Task 3 notice, and that these actions will result in a more "consistent approach" which he said was necessary. In response to a question from Ms. Knife as to why it was necessary for a more consistent approach, Mr. Knepper used the examples of certifications within EASA and the FAA as an illustration as to why a consistent approach in identifying risks would be beneficial.

Mr. Derossier asked about the participation levels from operators and Flight Standards in working MMEL issues, both at the sub-group and full group level. Mr. Knepper responded that there was no operator level participation in the working groups.

Mr. Dave Lotterer (RAA) stated that he felt any concerns about inconsistency around MMEL's could be resolved by flight standards based on what they (standards) considered was acceptable from manufacturers. Mr. Kasyzcki suggested that language in this report appeared consistent with Mr. Lotterer's comments, in that it was in fact structured only as a recommendation to be reviewed by Flight Standards. Web Heath suggested that this approach to MMEL could result certification to regularly fly an aircraft with inoperative equipment which would be at odds with the true intent of an MMEL. Mr. Kaszycki agreed that this was not the intent of the MMEL, and again asserted that the group's work had been within the scope of the tasking.

Ms. Knife suggested that the MMEL presentation was possibly too detailed and as such might invite the expectation for the requirement of numerical analysis which she felt was incongruent with the "safety case". Mr. Kaszycki stated that this was only being presented as a recommendation and would still required consensus from the working group and a vote from the TAEIG during the closing of Task 4. Mr. Kaszycki again asserted that he felt this work was consistent with the scope of the original tasking.

Mr. Bolt stated that he felt the ASAWG had done an "excellent job this far" with what he acknowledged to be a very controversial task. He suggested that consistent with the upcoming TAEIG meeting in fall 2008, some additional time should be arranged to allow the ASAWG to discuss its progress, thus allowing the TAEIG to assess the group's progress relative to its scheduled task completion date in March 2009.

Mr. Knepper indicated that the ASAWG was scheduled to meet in Cologne, Germany in June 2008 and then again in October 2008. He stated that he anticipated the workings group's next presentation to the TAEIG would involve determining which regulations and guidance materials were affected. He felt that the group was on schedule for its presentation to the TAEIG in Fall 2008. Mr. Bolt clarified to Mr. Knepper, that he felt that some in this meeting of the TAEIG were expecting that some of the issues proposed for Task 4 would already have been completed in Task 3. He indicated that he personally felt the working group had acted according to the scope of the original tasking, but suggested that perhaps another ad hoc TAEIG meeting might be helpful to evaluate the progress of Task 4 given the concerns. Mr. Knepper stated that the ASAWG would be willing to make an additional presentation to the TAEIG if necessary.

Mr. Derossier advised Mr. Knepper that his (Mr. Derossier's) understanding of this subject as presented during this meeting of the TAEIG was somewhat different than what he had perceived in reading the Task 3 report. He added that he thought it would be helpful for the working group to present a more "targeted" understanding of the specific recommendations regarding regulatory and guidance changes during the next TAEIG meeting. This he said would better allow him and others to represent their constituents. Ms. Knife added that she agreed with Mr. Derossier on this request. She added that she felt the current form of the Task 3 report was too difficult to understand. Mr. Knepper acknowledged that the report was complex and cited some particular examples of methodologies, such as latent failure, to illustrate these complexities. Mr. Kihm said these examples were descriptive of issues that he perceived were scheduled to be completed in Task 3. He added that he had provided some charts to the working group, and it now appeared that most of the "difficult" issues would be presented in Task 4.

Relative to Task 4, it was suggested by the group that perhaps an additional milestone within that task should be identified which could help facilitate the work of the group. Mr. Bolt agreed that it was very important for the briefing to the TAEIG in the fall of 2008 to show that the group is on target. This he said should help to preclude any "surprises" in March 2009, when Task 4 is expected to close. He added that this is a very tough subject, and that it was very important to produce the correct results. Regarding the scheduled Task 4 completion date in March 2009, Mr. Kaszycki stated that he felt there appeared to be a "disconnect" with respect to the efforts of the working group and the expectations of some members within the TAEIG. He acknowledged the contentiousness of work, but asked the working group and the TAEIG to work very closely together in continuance of this task. Mr. Kaszycki emphasized that despite the March 2009 schedule, it was more important to reach proper consensus than to produce a premature product.

Mr. Kihm suggested that there existed a certain "events list" that was available to some members on the working groups but not all. This created the potential for certain decisions to me made based on information known only to some while others were operating devoid of this same information. In discussing some informational bullets on his slide, Mr. Kihm provided further clarification to Mr. Knepper stating it had been reported that some subject matter experts (SME's) on the working group may have been using information that was not available to others, and were "rationalizing their positions" through the use of this information. Mr. Kihm said that since it had been decided earlier that such information was not to be used in the working group discussions then it was improper for such actions to occur. Mr. Kaszycki and Mr. Derossier both expressed agreement that such actions should not occur. Mr. Knepper stated that he understood that purpose of the tasking was to focus on inconsistencies, and while he acknowledged that it was not possible to exclude all accidents, he said as far as he could recall, accidents and incidents were never major points of discussions in the working groups.

Mr. Kihm also asked about criteria for determining consistency and wanted to know if this would involve selecting a most conservative methodology and then applying that to all systems. Mr. Knepper emphasized to Mr. Kihm that this would not be the case and that it would instead be a very comprehensive process. Ms. Knife asked Mr. Knepper if adequacy meant consistency. Mr. Knepper responded that *adequacy* referred to being complete and that *appropriate* referred to being correct.

In responding to a question from Mr. Kihm, Mr. Knepper clarified that "evaluation of average risk criteria" was not a part of this task.

Regarding a question from Mr. Kihm on consistency, Mr. Kaszycki clarified that in the case of critical systems industry had requested that "commonality on approaches" was necessary. However, he added that consistency would not be driven by the "highest common denominator". Mr. Knepper once again emphasized that the working group has and will continue to carefully address these concerns. Mr. Kihm also mentioned that it was very important for the working groups to follow the ARAC process.

In a response to a question from Ms. Knife regarding votes in a working group, Mr. Bolts said that working groups are supposed to reach a consensus and not vote per se. Mr. Knepper added that the working group will only vote if a consensus cannot be reached.

Mr. Bolt then asked for the TAEIG to bring Task 3 to a vote. With the understanding that during the next TAEIG there will be very detailed discussion to provide a better understanding plans and specific elements to be addressed in Task 4, voting members from the following entities voted for acceptance of the Task 3 report: AIA, Airbus, ALPA, Boeing, Embraer, and GAMA. There was no dissent.

Mr. Bolt stated that working group would move forward to Task 4, and also advised that the next briefing from the ASAWG to the TAEIG was scheduled for September 2008*.

*Since this meeting, the next regular TAEIG meeting has been rescheduled to October 1, 2008

Adjourned at 12:10 pm

Public Notification

The *Federal Register* published a notice of this meeting on April 25, 2008 (73 FR 22454).

Approval

I certify the minutes are accurate.

Craig R. Bolt

2/5/09

Craig R. Bolt
Assistant Chair, ARAC

ARAC ASAWG Report

Specific Risk Tasking

(Rev. 3.0)

Apr 2008

Ed Wineman ASAWG Co-chair	Roger Knepper ASAWG Co-chair

REVISION SHEET

Rev	Description Summary	Date
1.0	Basic Release	Nov 2006
2.5	Updated with comments included up to Web Meeting #5	May 2007
2.7	Comments provided up to Meeting #4 (Merignac) - Included Fig 6-1 (Design risk). - "Increase" wording was excluded from SR definition. - SRC (Specific Risk of Concern) definition was introduced along with the revision of Fig 6-2 (Task 3 entry flow diagram). - It was identified additional conditions for further considerations (Operating Mode, Flight Condition, Flight Phase, and At Risk Time), based on the review of SR definition.	Jun 2007
	Addressed Rev 2.7 comments provided by: Rod L., Alain C, Christophe G, Roger K, David M, Jim M, Linh L, Mike M, Nelson W, Ramesh N and Jim M.	Jul 2007
	Incorporate comments discussed during WM6, WM7 and WM8.	Aug 2007
3.0X	Version of the report reviewed by members for closure of the Task 1 and Task 2. Cleaned up version sent out for TAEIG review	Oct 2007
3.0	Task 3 report version (Seattle Meeting)	Apr 2008

TABLE OF CONTENT

Contributing organizations and individuals

Name	Company	Member Status
Knepper, Roger	*Airbus*	*ASAWG (Co-chair)*
Lalley, Rod	*Airbus*	*SME*
Sek, Joachim	*Airbus*	*SME*
Vigarios, Philippe	*Airbus*	*SME*
Haraguchi, Nelshio	*ANAC*	*ASAWG*
Merdgen, David	*Boeing*	*ASAWG (Flight Sub Team Chair)*
Schultz, Larry	*Boeing*	*ASAWG*
Tritz, Terry	*Boeing*	*SME*
Nordstrom, Paul	*Boeing*	*SME*
Robertson, CW	*Cessna*	*ASAWG (Design Sub Team Chair)*
Montgomery, Scott	*Cessna*	*SME*
Giraudeau, Christophe	*Dassault Aviation*	*ASAWG (MMEL Sub Team Chair)*
Cabasson, Alain	*Dassault Aviation*	*SME (Latent Sub Team Co-Chair)*
Robinson, Steve	*Hawker Beechcraft*	*SME*
Michael, Branch	*Honeywell*	*ASAWG*
Mattei, Patrick	*EASA*	*ASAWG*
Polano, Nadine	*EASA*	*SME*
Hancock, Colin	*EASA-Flight Standards*	*SME*
Paik, Ji	*Embraer*	*ASAWG (Report Issuer)*

Name	Company	Member Status
Azevedo, Ann	*FAA – CSTA*	*O/A*
Lambregt, Tony	*FAA – CSTA*	*O/A*
Larsen, Hals	*FAA – CSTA*	*O/A*
Sheppard, James	*FAA - AEG SEA*	*SME*
Grant, Bob	*FAA - E&PD*	*SME*
Le, Linh	*FAA – TAD*	*ASAWG*
Martin, Todd	*FAA – TAD*	*SME*
McRae, Mike	*FAA - TAD*	*SME*
Narine, Rameshwar	*Garmin*	*SME*
Mingler, Paul	*GE*	*ASAWG*
Wineman, Ed	*Gulfstream*	*ASAWG* *(Co-chair)*
Peterson, Michael	*Rockwell Collins*	*ASAWG* *(Latent Sub Team Co-Chair)*
Prasuhn, Warren	*Rockwell Collins*	*SME*
Burkett, Michael	*Rolls Royce*	*ASAWG*
Marko, Jim	*TCCA*	*ASAWG*

1 Executive Summary

This tasking is to direct the Aviation Rulemaking Advisory Committee (ARAC) to provide information about specific risk assessment and make recommendations for revising requirements or guidance material as appropriate.

An “Airplane-level Safety Analysis Working Group” (ASAWG) was asked to perform the following tasks:

- Task 1: Develop definition of specific risk and catalog examples of its application.
- Task 2: Identify relevant requirements, guidance and recommendations related to specific risk and its use.
- Task 3: Determine adequacy of the existing/proposed standards and if a change is warranted.
- Task 4: Develop recommendations for rulemaking and guidance material.

The results of Task 1 to 3 are summarized herein. Concurrence from the TAE Issues Group and the FAA is required before continuing to Task 4.

Tasking boundaries are:

- Issues outside the flight envelope or outside design specifications are not addressed,
- Methodologies not covering airplane certification but currently being employed to handle conditions such as manufacturing defects, quality escapes, etc. (i.e. Gunstone / CAAM) are not addressed,
- Specific risks, if they lead to a failure condition of Major or less severe criticality, are not addressed,
- Specific risks associated with airframe structures are not addressed.

Task 1 defined Specific Risk in general terms as “The risk on a given flight due to a particular condition”. The Specific Risks of Concern (SRC) are when the airplane is one failure away from a catastrophe, or when the risk is greater than the average probability criteria provided in AC 25.1309 Arsenal for hazardous and catastrophic failure conditions, on a given flight due to a particular condition.

Examples of regulations, guidance and industry practices provided the correct and concise understanding of the specific risk definition.

The particular conditions identified for detailed considerations were:

- Latent Failure,
- MMEL,
- Active Failure / Design Variability / Flight Condition / Operating Mode,
- Flight Time / Diversion Time / Flight Phase / At Risk Time.

The ASAWG reviewed during Task 2 the background and intent of relevant existing requirements, existing guidance material, and ARAC recommendations and explained how specific risk is addressed.

The ASAWG reviewed during Task 3 the results of Tasks 1 & 2 and determined the appropriateness, adequacy, and consistency of the relevant existing regulations, existing guidance material, ARAC recommendations, and industry practices for airplane-level safety analysis. The key approaches to addressing Specific Risk were identified as "fundamental issues". For each fundamental issue recommendations for Task 4 were developed and reviewed by industry. This review generated comments, the disposition of which is documented in this report. The final recommendations from Task 3 focus on establishing consistent guidance / regulation for:

- Conducting specific risk evaluations of latent and active failures.
- Conducting specific risk evaluation for dispatch under a MEL.
- FHA development when dealing with intensifying factors such as flight length, flight phase and diversions.
- Documenting component life limits that are necessary to protect against aging and wear out.

These recommendations for Task 4 demonstrate where a more consistent approach across systems is necessary to:

- Assure a warranted level of specific risk regulation, i.e. inconsistency potentially results in over- or under-regulation, and
- Avoid undue burden on the applicant and regulatory authorities.

2 Purpose / Background

The FAA established the Aviation Rulemaking Advisory Committee (ARAC) to provide advice and recommendations to the FAA Administrator on the FAA's rulemaking activities for aviation-related issues. Previous ARAC harmonization working groups (Flight Controls, Power Plant Installations, and Systems Design and Analysis) produced varying recommendations regarding the safety of critical airplane systems. Although the subject of specific risk analysis was addressed in those working groups, the recommendations were

not consistent. Regulations and Policies developed from within the FAA also provide approaches different from those recommended by ARAC.

If these different approaches are applied on a typical certification project, they could result in non-standardized system safety assessments across various critical systems. This could cause conflicting interpretations for conducting system safety assessments in future aircraft certification programs. After reviewing the existing regulations and the recommendations from the various harmonization-working groups, the FAA Transport Airplane Directorate, along with the European, Canadian, and Brazilian civil aviation authorities, identified a need to clarify and standardize safety assessment criteria. The FAA decided to use a new ARAC tasking to integrate the safety assessment criteria from various system disciplines. In July 2005, an industry group comprised of the Aerospace Industries Association (AIA), General Aviation Manufacturers Association (GAMA), and several aircraft and engine manufacturers, proposed a new tasking. The FAA agreed with the industry group proposal, and has based this tasking on that proposal.

3 Scope

This tasking is to direct ARAC to provide information about specific risk assessment and make recommendations for revising requirements or guidance material as appropriate. An "Airplane-level Safety Analysis Working Group" (ASAWG) is to perform the following tasks:

Task 1: The ASAWG is to establish a definition for specific risk. It is to provide relevant examples of its application in today's aircraft certification, FAA Flight Operations Evaluation Board (FOEB), and Maintenance Review Board (MRB) activities.

Task 2: The ASAWG is to review the background and intent of relevant existing requirements, existing guidance material, and ARAC recommendations and explain how specific risk is addressed. In Task 2, the ASAWG is to document all current and proposed approaches to specific risk but should not establish how specific risk should be assessed.

Task 3: The ASAWG is to review the results of Tasks 1 & 2 and determine the appropriateness and adequacy of existing and proposed airworthiness standards for airplane-level safety analysis. This task is to demonstrate if a more consistent approach across systems is necessary. Concurrence from the TAE Issues Group and the FAA is required before continuing to Task 4.

Task 4: The ASAWG is to develop a report containing recommendations for rulemaking or guidance material and explain the rationale and safety benefits for each proposed change. The report is to define a standardized approach for applying specific risk in the appropriate circumstances. The FAA is to define the report format to ensure the report contains the necessary information for developing a Notice of Proposed Rulemaking (NPRM), and/or ACs.

Unlike the tasking statements above, following boundaries were not defined within the tasking, but rather derived by the ARAC ASAWG and agreed by ARAC TAEIG to further bound the tasking. These boundaries are the ARAC Specific Risk tasking should not address issues outside the flight envelope nor outside design specifications. Methodologies currently being employed to handle conditions such as manufacturing defects, quality escapes, etc. (i.e. Gunstone / CAAM) are not covered under Certification of the airplane; therefore, they are also beyond the scope of the ARAC tasking. The ARAC Specific Risk Tasking should not address specific risks, if they lead to a failure condition of Major or less severe criticality.

In addition, specific risk associated with airframe structures should not be addressed by this Tasking. Many of the transport category airplane airworthiness rules, policies and practices used to establish a minimum acceptable level of safety for airframe structure involve regulating what we have defined as a "specific risk". These rules, policies and practices are often intended to prevent the occurrence of a particular failure (e.g. fracture of a primary structural element) given below average parts (e.g. those with maximum undetectable flaws and/or likely damage) are exposed to above average stresses (e.g. limit and/or ultimate loads). However, as indicated by the following statement from Task 3: *"This task is to demonstrate if a more consistent approach across systems is necessary"*; this overall tasking is focused on "systems" related rules, policies and practices. Consequently, while structural examples may ultimately provide some valuable insights as to how failure prevention might be undertaken for a particular critical part within airplane systems, such examples were not included in Task 2.

Note: This document contains a vast amount of "historical" information generated in the process of reaching the set of recommendations coming out of the tasks. This information is contained in the form of Word tables and Excel workbooks. Due to the size of this information, these files are embedded within the text of this document. Therefore, each of these tables will need to be printed individually if the reader wants a hard copy of this data.

4 Abbreviations

AC	Advisory Circular
AD	Airworthiness Directive
AEG	Aircraft Evaluation Groups
AFM	Aircraft Flight Manual
AIA	Aerospace Industries Association
ANAC	Agência Nacional de Aviação Civil
ARAC	Rulemaking Advisory Committee
ASAWG	Airplane-level Safety Analysis Working Group
CAAM	Continued Airworthiness Assessment Methodology
CFR	Code of Federal Regulations
CMR	Certification Maintenance Requirement
CS (JAR)	Certification Standard (Joint Aviation Requirements)
CSTA	Chief Scientist Technical Advisor
E&PD	Engine and Propeller Directorate
EASA	European Aviation Safety Agency
EPRD	Electronic Part Reliability Data
ETOPS	Extended Range Operation
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FHA	Functional Hazard Assessment
FMEA	Failure Mode Effect Analysis
FOEB	Flight Operations Evaluation Board
GAMA	General Aviation Manufacturers Association
HIRF/IEL	High Intensity Radio Frequency
IAW	In Accordance With
JOEB	Joint Operations Evaluation Board
LRU	Line Replaceable Unit
MMEL	Master Minimum Equipment List
MIL HDBK	Military Handbook
MOC	Means of Compliance

MRB	Maintenance Review Board
MTBF	Mean Time Between Failure
NPRD	Non Electronic Part Reliability Data
NPRM	Notice of Proposed Rulemaking
OEM	Original Equipment Manufacturer's
PSE	Primary Structural Element
SME	Subject Matter Expert
SR	Specific Risk
SRC	Specific Risk of Concern
SSA	System Safety Assessment
STC	Supplemental Type Certification
TAD	Transport Aircraft Directorate
TAEIG	Transport Airplane Engine Issues Group
TBD	To Be Defined
TCCA	Transport Canada Civil Aviation

5 Bibliography

ARP 4761	
AC 25.1309	
Gunstone	
CAAM	

6 Development

6.1 Task 1

6.1.1 Introduction

The ASAWG had to establish during Task 1 a definition for specific risk and provide relevant examples of its application.

Firstly, available specific risk definitions were reviewed and specific risk related regulations, guidance and industry practices were discussed. Then a specific risk and specific risk of concern definitions have been established by the ASAWG. Further on potential relevant conditions for specific risk were identified. These conditions were guided by the ARAC tasking notice. It identifies potential relevant conditions for specific risk as follows: Latent failure, MMEL, Airplane configurations, and Flight conditions.

The specific risk definition was applied to each condition and vice versa with the support of key questions. These questions were crucial for the scope of the ARAC Tasking such as compliance with average probability criteria of 25.1309 Arsenal. This application identified how relevant these conditions were, given the specific risk definition, and whether they would have to be addressed further under ARAC Specific Risk Task 3.

Examples of regulations, guidance and industry practices helped for the correct and concise understanding of the specific risk definition.

6.1.2 SR & SRC definitions

The ARAC Tasking notice required the development of a definition for Specific Risk that considered the certification aspects, operational aspects and maintenance aspects used in today's aircraft design development and certification processes.

The definition for Specific Risk is: ***"The risk on a given flight due to a particular condition".*** The **Specific Risks of Concern (SRC)** are when the airplane is one failure away from a catastrophe, or when the risk is greater than the average probability criteria provided in AC/AMJ 25.1309 Arsenal for hazardous and catastrophic failure conditions, on a given flight due to a particular condition.

6.1.2.1 History

In order to develop the definition for specific risk that was thorough yet concise a complete understanding of what went before had to be understood by the ASAWG members.

The genesis of Specific Risk tasking date's back to 1993 with a FAA statement of work to ARAC to develop guidance for specific risk bridging the requirements of 14CFR 25.901(c), 14CFR 25.1309 and MMEL development. The ARAC Working Group (WG) could not close its deliberations by 1998 and recommended guidance in the form of a draft AC (Diamond version of AC/AMJ 25.1309) that supported average risk assessment methodology. In 2001, the FAA proposed revisions to the 1998 ARAC recommendations to cover specific risk. This guidance was introduced into a preliminary Draft AC 25.1309-1BX which lead to draft arsenal version of AC/AMJ 25.1309.

Meanwhile the Diamond version developed in 1998 by the ARAC WG was adopted by the European community and was included with EASA's CS 25.1309 in October of 2003. Also during this time, guidance and policy was being recommended and/or released in the areas of thrust reversers (FAR 25.933 and AC 25.933X), fuel tank ignition (SFAR 88, FAR 25.981 and AC25.981-1B), powerplant installations (FAR 25.901(c) policy), flight controls (FAR 25.671) and MMEL policy prohibiting dispatch in catastrophic single-failure conditions.

In the end, it had become apparent that the various approaches were inconsistent when viewed together at the airplane level. In addition, there was no stated common definition or general understanding of "Specific Risk".

6.1.2.2 Rationale

The basic precepts provided to the ASAWG when developing the definition for Specific Risk was it must be thorough yet concise. The definition should not invalidate previous work. The definition should not encompass methodology nor describe how specific risk should be addressed. The goal was to encompass the definition into a single sentence. Finally, the definition had to stand up to a review process that ensured the basic precepts were maintained.

To discuss specific risk at the aircraft level, it was decided to compare it to the quantitative average probability criteria as defined by AC/AMJ 25.1309 Arsenal. The term "Average Risk" is understood to represent the average probability of failure for some baseline population of airplanes over their entire life. Specific risk may be above, below or equal to this average. However, it was recognized that any Specific Risk of Concern must increase the risk relative to the average probability criteria as defined by AC/AMJ 25.1309 Arsenal.

Figure 6-1 illustrates the relationship between the specific risks of concern and the average probability criteria of AC/AMJ 25.1309 arsenal. The Specific Risk of Concern (SRC) depicted represent deviation that can occur on specific flights.

A basic assumption was the baseline population would be defined as any aircraft configuration used in the average risk calculation. Aircraft that encompass additional Supplemental Type Certifications (STCs) and/or production options that constitute a different configuration would then just be considered a new population and not a subset of the baseline configuration. Thus, the definition above was developed.

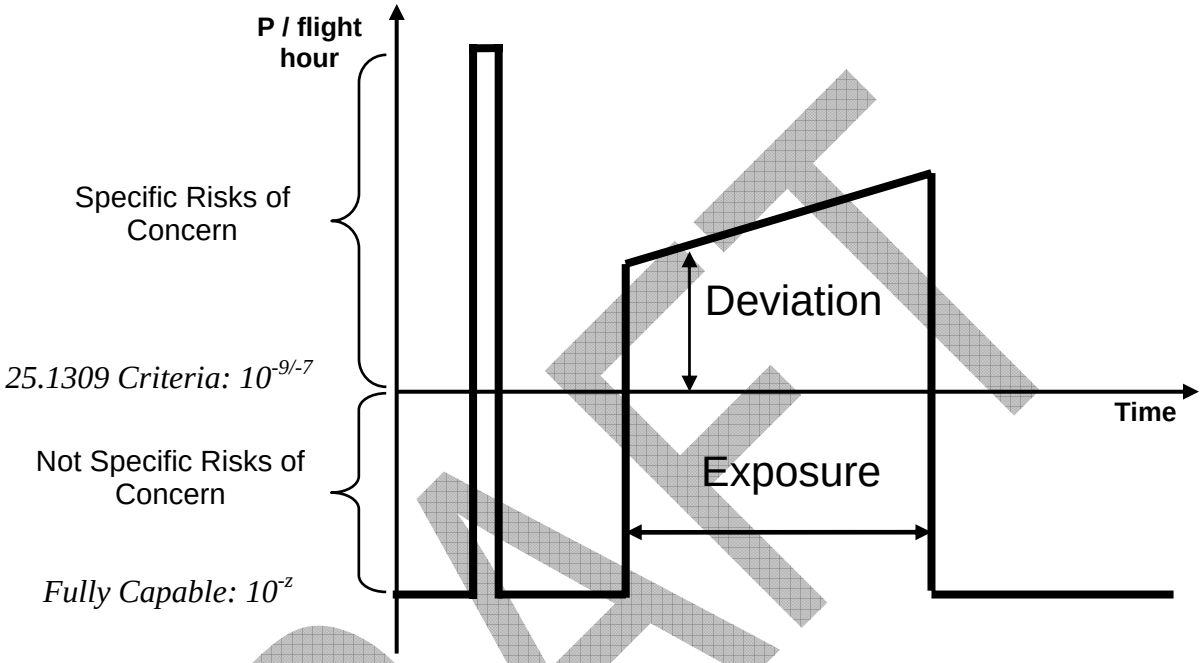


Figure 6-1: Design Risk for a Failure Condition

6.1.3 Application of the Definition

Specific Risk is the risk on a given flight due to a particular condition. Of interest are the **Specific Risks of Concern (SRC)** when the airplane is one failure away from a catastrophe, or when the risk is greater than the average probability criteria provided in AC/AMJ 25.1309 Arsenal for hazardous and catastrophic failure conditions, on a given flight due to a particular condition. Therefore, this leaves the process related to the identification of the particular conditions as being critical to the definition.

6.1.3.1 Particular Condition Development

The identification of the conditions potentially relevant to specific risk was guided by the ARAC tasking notice. Latent Failures and MMEL relief was immediately recognized as relevant. Various airplane configurations and flight conditions were also identified as potentially relevant conditions. Environmental or operating conditions that were outside the flight envelope and/or design specification of the baseline aircraft were ground ruled out as

particular conditions that would be identified and reviewed by the ASAWG for specific risk conditions. Some of these include flight into volcanic ash, flight into icing in excess of the conditions defined in Appendix C of 14CFR25, etc.

Various airplane configurations and flight conditions were further broken down into subsets to include such items as operating modes, active failure conditions, design variability, flight phase, flight time, diversions / return to land conditions and flight conditions. Design variability included design characteristics such as aging and wear that may impact the assumption of a component operating under a random failure distribution condition for the life of the aircraft, but design variability did not include such items as aircraft reconfigurations due to application of an STC to a given aircraft. As stated earlier, an STC aircraft is considered to be a new baseline. Active failure modes were separated from operating modes by recognizing the difference of operating the aircraft under emergency or abnormal operating procedures of the Aircraft Flight Manual (AFM) vs. the normal operating procedures. The distinction between the two is that one mode is entered because of an equipment malfunction while the other is selected by the pilot.

These conditions were then categorized as "Actual" or "Potential". The "Actual Conditions" were defined as those conditions that are identifiable for a specific airplane or flight prior to the initiation of the flight. The "Potential Conditions" were defined as those conditions that are not known to exist for a specific airplane or flight but may be expected to exist prior to the initiation of some flights during the fleet life.

6.1.3.2 Task 3 Relevancy Logic

To determine if a particular condition was a specific risk of concern and was worthy to proceed to Task 3, the ASAWG membership developed a series of decision points to go through. A simple logic diagram is provided in Figure 6-2 that illustrates the decisions that should be passed through to determine if the particular condition is considered Task 3 relevant or not. Only one particular condition at a time goes through the decision points.

The first decision point is simply a determination if the particular condition is considered inside or outside of the design envelope (i.e. design specification) and certification basis of the aircraft. If the condition is outside the design conditions of the aircraft then it is not considered within the boundaries as established for the ARAC Specific Risk tasking.

The remaining decision points in the diagram are an attempt to determine the level of increased risk introduced by each particular condition, with its specific assumptions made for these conditions as identified in 6.1.3.3. This assumption was only applied during Task 1 for the identification of particular conditions to be considered relevant for Task 3.

At this point in the flow diagram, the aircraft configuration does not change from one decision to the next, nor can the particular condition under review be changed. The first decision, determines if the particular condition can leave the aircraft one failure away from a catastrophe. If the answer is no then the next decision point, must be passed for

determination if the assumed particular condition has a remaining risk greater than the average probability criteria (i.e. 1.0E-7/1.0E-9 per flight hour) of AC/AMJ 25.1309 Arsenal.

To better understand the intent of the third decision point, Figure 6-1 above can be reviewed. When the airplane operates in the full-up configuration (i.e. no failures) the risk of a failure condition is by regulation below the design criteria called out in AC/AMJ 25.1309 Arsenal. The criterion of the third decision looks at what configuration the aircraft may be in when a particular condition is evaluated.

At this point, the particular condition becomes the variable and it is the only variable that changes when it is applied to the aircraft design characteristics to see if the minimum probability criterion of AC/AMJ 25.1309 Arsenal has been exceeded. If the answer is no then this is not a specific risk of concern otherwise the condition is to proceed for review in Task 3. Though the particular condition may satisfy the no decision criteria the applicable requirements and/or guidance could still be reviewed in Task 3. The results of these assessments are to be reported to TAEIG Issues Group prior to initiation of Task 4.

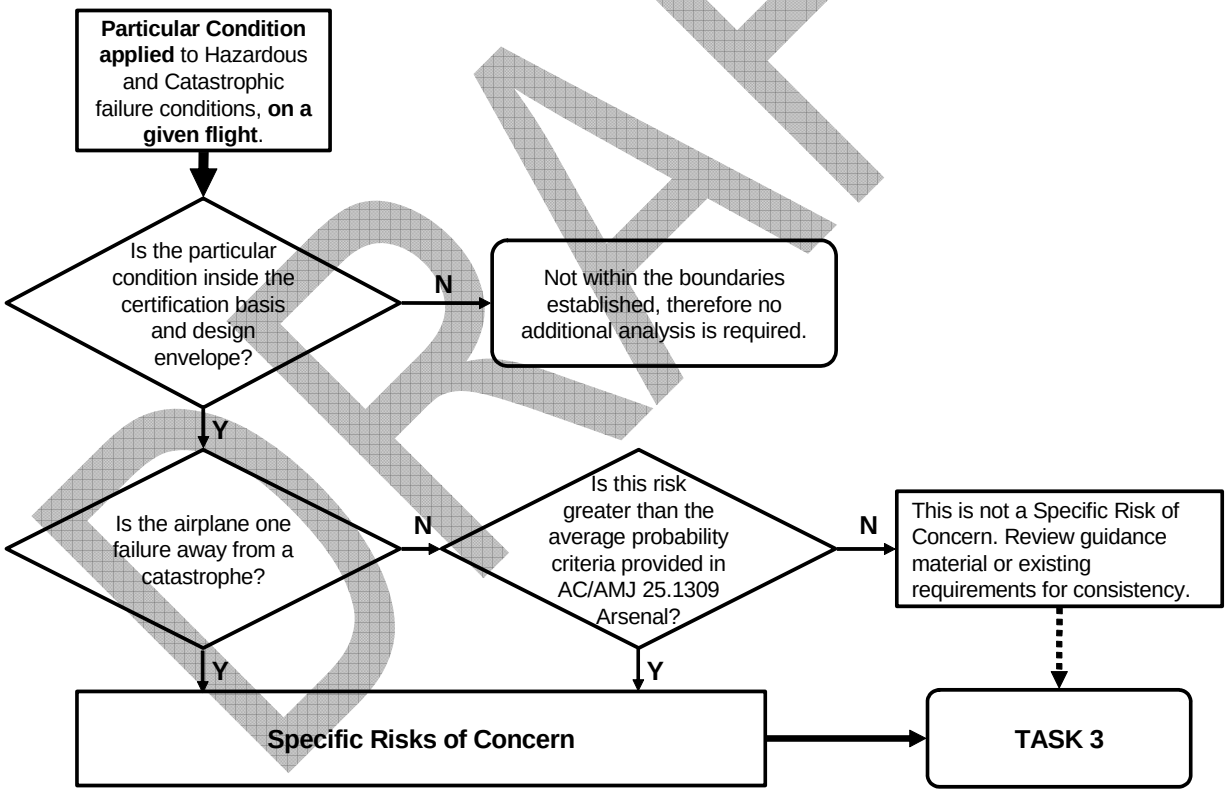


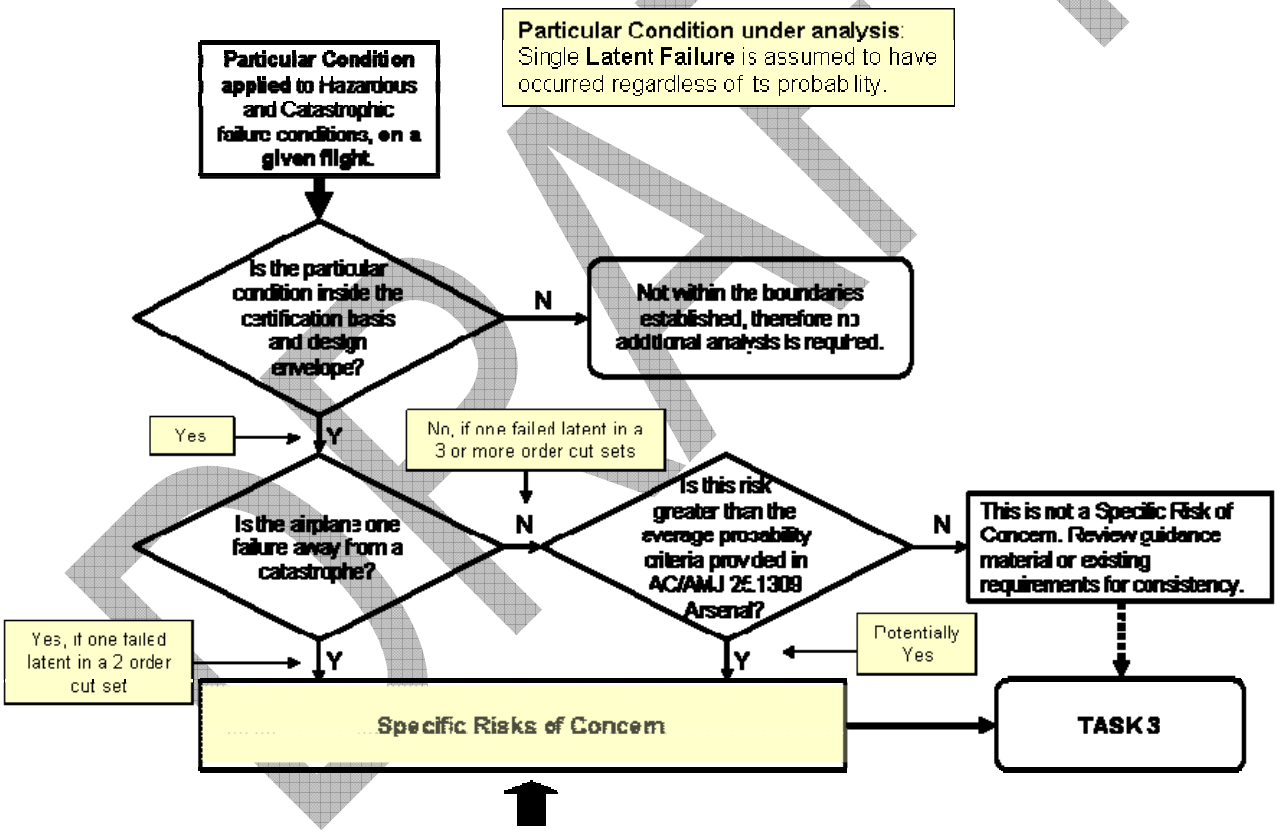
Figure 6-2: Task 3 Entry Flow Diagram

6.1.3.3 Decision (SRC, non SRC)

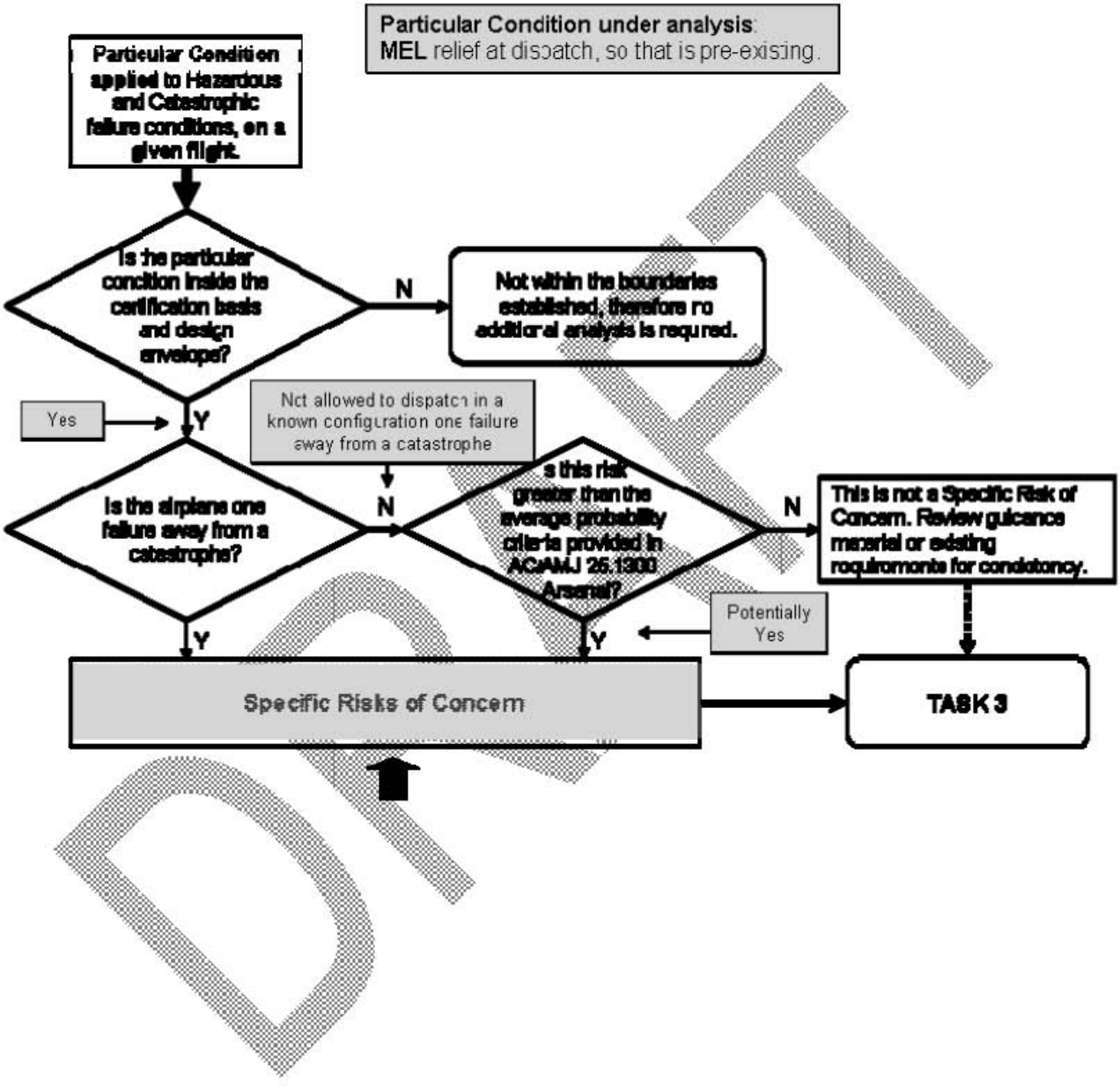
To apply the definition for specific risk developed by the ASAWG to a particular condition, the logic diagram described above was used for various conditions that historically had been agreed to be specific risk conditions. These two were latent failures and MMEL dispatch conditions. Additional conditions as defined in 6.1.3.1 were also tested. The following Table 6-1 provides the results of this testing process while the figures provide a graphic step by step view of the logic taken when progressing through the flow chart in Figure 6-2.

Examples from each sub-task are provided using the flow diagram of Figure 6-2 and applying to some particular conditions:

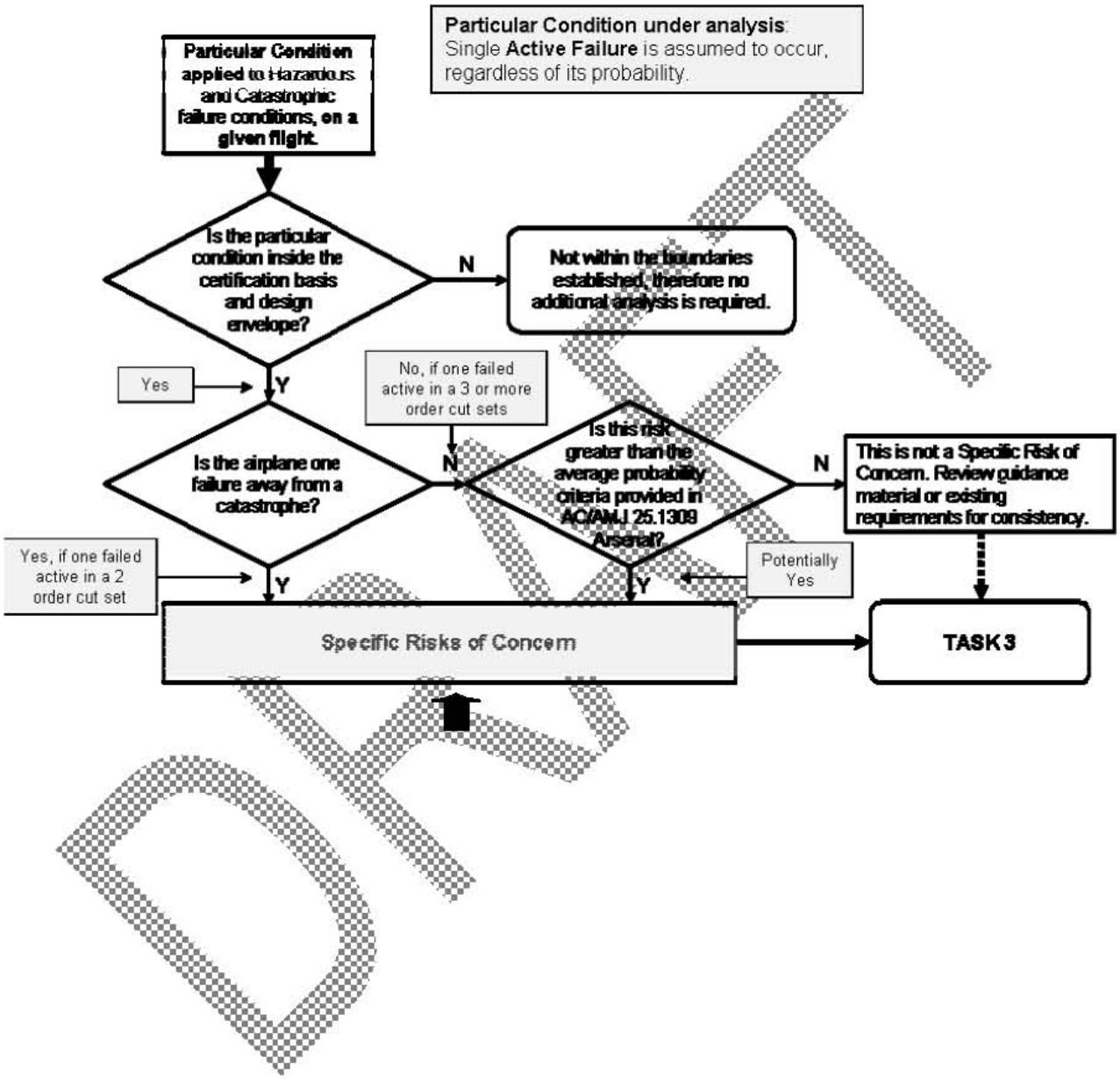
- Latent Failure



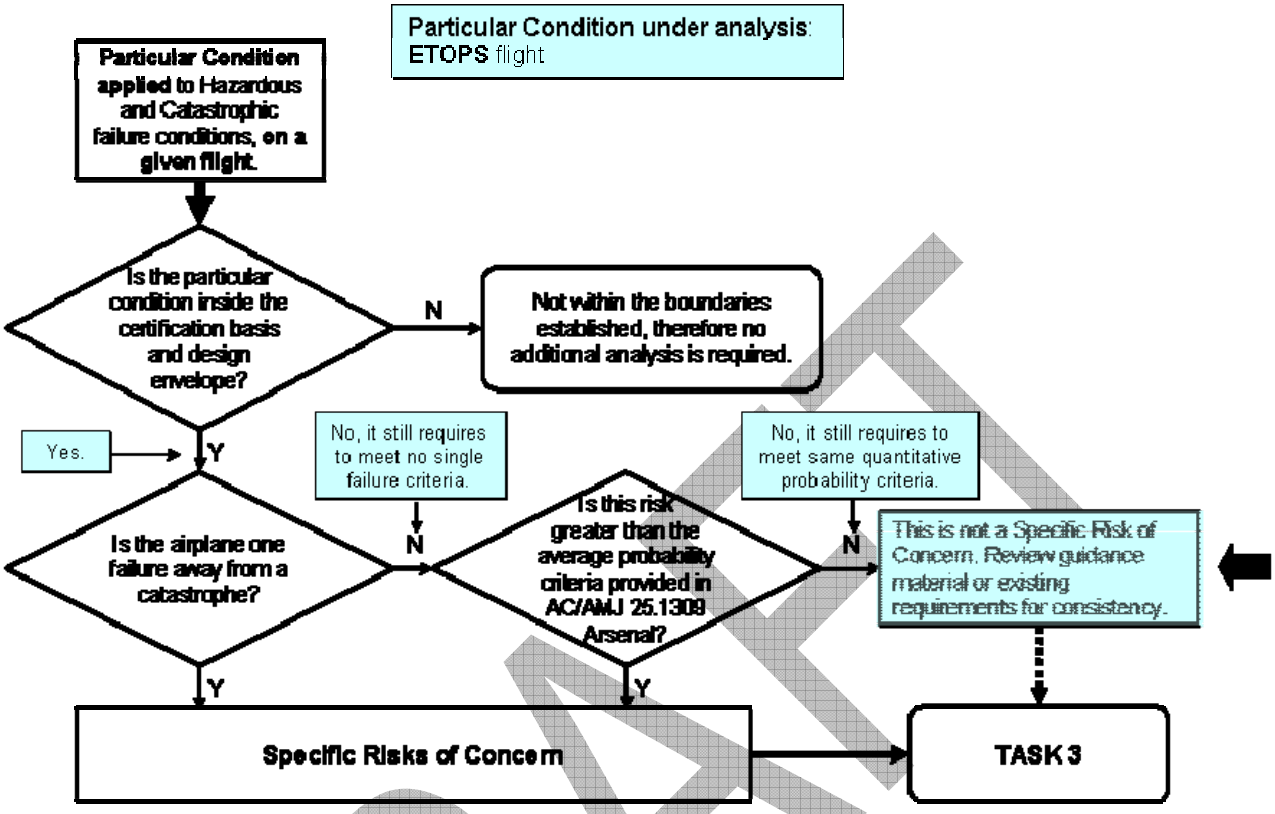
- MMEL


Particular Condition under analysis:
MEL relief at dispatch, so that is pre-existing.
Particular Condition applied to Hazardous and Catastrophic failure conditions, on a given flight.
Is the particular conction inside the certification basis and design envelope?
N
Not within the boundaries established, therefore no additional analysis is required.
Yes
Y
Not allowed to dispatch in a known configuration one failure away from a catastrophe
Is the airplane one failure away from a catastrophe?
N
Is this risk greater than the average probability criteria provided in AC/AMJ 26.1309 Arsenal?
N
This is not a Specific Risk of Concern. Review guidance material or existing requirements for consistency.
Y
Y
Potentially Yes
Specific Risks of Concern
TASK 3

- Active Failure



- Flight Time



The particular conditions tested and a brief description or examples of the type of conditions were:

- **Latent Failure** – A failure is latent until it is made known to the flight crew or maintenance personnel.
- **MMEL** – Recognized or approved under FAR 91 configurations of the aircraft that are permitted at dispatch using operating rules, but may leave the aircraft in a configuration that is less than that evaluated for certification under FAR/JAR 25.
- **Operating Modes** – These are system or aircraft normal modes (abnormal modes are addressed in other particular conditions, e.g. active failures) such as auto pilot on/off, flaps up/down, etc…, that the pilot places the aircraft in.
- **Flight Condition** – This include most of the environmental conditions such as flight over water or high terrain, high altitude operations, operating into high cross winds or extreme cold environments, etc.
- **Design Variability** - Includes design characteristics such as aging, wear, cycle dependencies that may impact the assumption a component was operating under a random failure distribution condition for the life of the aircraft, but it did not include

such items as aircraft reconfigurations such as application of a specific STC on a given aircraft

- **Active Failure**– Equipment / system failure conditions which are identifiable during the flight for a specific airplane.
- **Flight Time** – Encompasses all the permitted flight that goes into the calculation of average flight time. It recognizes the potential for one aircraft to be operating in a very high cycle condition but low average flight time to the extreme of ultra long flights that include ETOPS operations.
- **Diversion / Return to Land Conditions** – The conditions associated with an in-flight emergency being that requires the crew to proceed to the closest landing site. This could be caused by a medical condition of a passenger or other external event such as a bird strike at takeoff or other.
- **Flight Phase** – Includes the classic conditions such as taxi, takeoff, climb, cruise, descent and landing. Each condition covers the entire average time associated with that condition.
- **At Risk Time** – The period of time at which an item must fail in order to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition.

The particular conditions were categorized as either potential risk conditions or actual risk conditions as defined in section 6.1.3.1 above.

The results of the testing identified ten potential condition categories that the ASAWG had to be investigating during Task 2 and 3. Some examples of these types of conditions and a more thorough explanation of the types of conditions included in these categories are provided in the follow on sections. The conditions identified for further considerations were:

- Latent Failure
- MMEL
- Active Failure
- Operating Mode
- Flight Condition
- Design Variability
- Flight Time
- Diversion / Return to Land
- Flight Phase
- At Risk Time

The Specific Risk is the risk on a given flight due to a particular condition.

*The **Specific Risks of Concern (SRC)** are when the airplane is one failure away from a catastrophe, or when the risk is greater than the average probability criteria provided in AC/AMJ 25.1309 Arsenal for hazardous and catastrophic failure conditions, on a given flight due to a particular condition.*

Particular Condition applied to Haz / Cat FC on a given flight.	Inside Envelope / Spec?	Actual or Potential risk condition?	Is the airplane one failure away from a catastrophe?	Is the risk greater than the average probability criteria provided in AC/AMJ 25.1309 Arsenal?	Comments
MMEL	Y	A	N	Y	- Acceptable level of safety to be defined (JAR MMEL). - Standardized approach to be developed. - Some OEMs satisfy average probability criteria of AC/AMJ 25.1309 Arsenal.
Operating mode	Y	A	N	Y	- Some operating modes inside the envelope are assumed to have a probability of 1 (average probability criteria of AC/AMJ 25.1309 Arsenal not exceeded). There may be other conditions that have probabilities less than 1 (average probability criteria of AC/AMJ 25.1309 Arsenal potentially exceeded, if probability of 1 would be assumed). - Operating modes related to failures are addressed separately. - This is not SRC in and of itself.
Flight condition	Y	A	Y	Y	- Some flight conditions inside the envelope are assumed to have a probability of 1 (average probability criteria of AC/AMJ 25.1309 Arsenal not exceeded). There may be other conditions that have probabilities less than 1 (average probability criteria of AC/AMJ 25.1309 Arsenal potentially exceeded, if probability of 1 would be assumed). Examples may be crosswind, gust and turbulence. - Not SRC in and of itself.
Design variability	Y/N	A	N	Y/N	- Variability affects a random failure distribution.
Flight phase	Y	A	N	Y	- Average probability criteria of AC/AMJ 25.1309 Arsenal potentially exceeded, if an occurrence probability especially for this flight phase calculated, i.e. without normalizing using the average flight time hour.
Flight time	Y	A	N	Y/N	- If flight time is always below average, than cycling effects are perhaps not properly covered. - 25.1309 compliance: ETOPS assessments to meet 25.1309 criteria per Part 25 Appendix K. Other SSAs use fleet average flight times which may not be conservative for all cases.

The Specific Risk is the risk on a given flight due to a particular condition.

*The **Specific Risks of Concern (SRC)** are when the airplane is one failure away from a catastrophe, or when the risk is greater than the average probability criteria provided in AC/AMJ 25.1309 Arsenal for hazardous and catastrophic failure conditions, on a given flight due to a particular condition.*

Particular Condition applied to Haz / Cat FC on a given flight.	Inside Envelope / Spec?	Actual or Potential risk condition?	Is the airplane one failure away from a catastrophe?	Is the risk greater than the average probability criteria provided in AC/AMJ 25.1309 Arsenal?	Comments
Diversion / Return to land	Y	P	N	Y	- Issue Paper available.
Latent failure	Y	P	Y	Y	The airplane may be one failure away from catastrophe assuming that one failed latent in a 2 order cut set.
Active failure	Y	P	Y	Y	- The airplane may be one failure away from catastrophe assuming that one failed active in a 2 order cut set,. - Regulations to be re-examined like 25.671, 25.981, 25.933.
At Risk Time	Y	A/P	Y	Y	- Average probability criteria of AC/AMJ 25.1309 Arsenal potentially exceeded, if an occurrence probability especially for this at risk time calculated, i.e. without normalizing using the average flight time hour. - Whether or not it is actual/apparent when a particular airplane is at risk depends upon the particular condition and associated risk under study.

Table 6-1: Specific Risk Analysis Table

6.1.4 SR examples

6.1.4.1 Latent Failure Task

The Latent Failure Task Group was assigned the task to identify and document the current approaches in order to assess in Task 3 the acceptance criteria for the "significant latent failures" highlighted in paragraph 9.c.6 of the proposed ARAC Advisory Circular (AC) 25.1309 - "Draft ARSENAL version," dated 6/10/2002.

In order to provide current examples of latent failure applications, the following items were identified. More details like the background, the intent of relevant existing requirements, the existing guidance material, industry practices, and the explanation of how specific risk is addressed should be reviewed and provided in Task 2.

- AC 33.28-1 (Engine over-speed criteria)
- 25.671
- ARAC 25.671
- Generic IP - 25.933
- ARAC 25.933
- AC 25-19
- AC 25.1309-1A
- AC/AMJ 25.1309 - Arsenal
- ARP 4761 (Maximum dormancy)
- SFAR88 & 25.981
- FAA Policy 25.901(c)
- IP to 25.901(c)

6.1.4.2 MMEL Task

6.1.4.2.1 Background

The FAA MMEL process is an operational process led in the field by Aircraft Evaluation Groups (AEG). FAA HQ Flight Standards division in Washington, DC controls the policy and overall standardization of the MMEL.

The development of standardization and policy guidance is performed by an MMEL FAA/Industry Group (MMEL IG). The MMEL IG is composed of representatives from the

FAA, operators and the industry. This group reviews items of equipment that are required by a new regulatory requirement or are MMEL items that are affected by FAA policy decisions. This process has led to the issuance of a set of FAA Policy Letters in which guidance is given to FOEB chairmen for drafting specific MMELs.

FOEB chairmen set up an initial aircraft MMEL based on the aircraft manufacturer's Proposed MMEL (P-MMEL). During a public FOEB meeting that gathers AEG staff and chairman, the respective aircraft manufacturer [OEM] and operators, the initial MMEL is reviewed, and amended as necessary. This updated MMEL is then posted on FAA Opspecs website [draft section] for public comments. After a specified period of time, public comments are reviewed by the FOEB chairman. Final revisions are then made and the MMEL posted in the "Valid" section of the FAA Opspecs website for public use.

This process is further described in Airworthiness Inspector's Handbook, Order 8300.10 - Volume 2 - Chapter 7. This process is also described in FAA Order 8400.10.

6.1.4.2.2 Developing MMEL

In developing their P-MMEL, manufacturers and operators seeking consideration for relief for operating with certain items of equipment inoperative, are requested to provide supporting documentation that sufficiently substantiates their request. In addition to including an evaluation of the potential outcome of operating with specific items inoperative, this documentation should consider the following topics: the subsequent failure of the next most critical component; the interrelationships between items that are inoperative; the specific conditions under which the equipment is to be allowed to be inoperative [provisos]; any necessary Operations and/or Maintenance procedure [M & O's]; the proposed repair interval; the impact on approved flight manual procedures; the reliability of critical components; and any/all potential impacts on crew workload that could adversely degrade safety margins.

The basic concept to be applied in accepting an item for inclusion into a Master Minimum Equipment List is that the subsequent failure of the next most critical component in flight must not lead to a catastrophic event. There are other essential considerations too, however such as qualitative requirements that prohibit the incorporation of items of equipment powered by essential buses, or items of equipment necessary to accomplish an emergency procedure[s]. Related to all of these, is guidance for electrical systems on two-engines airplanes. In addition, the MMEL may not conflict with other FAA-approved documents such as the approved aircraft flight manual limitations, emergency procedures, and/or Airworthiness Directives (AD). AD's always take precedence over any published MMEL relief.

Appropriate restrictions and/or procedures are established to ensure an acceptable level of safety is maintained during the MMEL/MEL deferral period.

Specific OEMs may apply different processes for establishing their Proposed MMEL. These processes range from a full safety analysis established for each item -assigning a probability of one or a conditional probability to the failed item- to a qualitative analysis that

is supported by quantitative analysis when requested. These company processes are designed and intended to be more conservative than that required by the FAA.

When an airplane is dispatched under MMEL/MEL relief (i.e. less than full up) it is an example of SRC, as the specific aircraft configuration may now have a risk higher than that established under an average full up configuration.

6.1.4.2.3 Non-US Practices

Transport Canada MMEL process is conducted along with Type certification activities, should end at TC date and involves certification specialist. It is based on safety analyses and it mainly looks at the impact of inoperative item coupled with the next failure and assesses whether the residual probability is still “on the order” of what it should be for the failure classification being assessed.

European process is still processed under JAA rules as EASA has not overtaken this activity. It is driven by JAR-MMEL/MEL, specifically by requirement .010(a) which request "to maintain an acceptable level of safety as intended in the applicable JAR or equivalent Requirement".

6.1.4.3 Airplane Configuration Task

The first task of the group, was to identify and discuss how different Operating Modes of Aircraft Systems, Flight Conditions (Environmental Conditions), Active failure and Design Variability where considered in showing compliance.

All the members that provided feedback on their methods of showing compliance used SAE ARP 4761 (published 1996-12), AMC 25.1309 (2006-5), the Arsenal (2002-6) or Diamond Draft (1998-4) of AC 25.1309. There were slight differences between the companies. This can be attributed to relative newness of the system safety process when compared to mature processes (i.e. structures or pressurization).

As outlined in 25.1309 compliance guidelines mentioned above, the applicant in their functional hazard assessments (FHA), evaluate the effect of the functional failure condition on the aircraft and crew based on the worst case within the certification approved standard, flight envelope and design specification. This sets the hazard classification and drives the qualitative and quantitative requirements, as well as requirements for HIRF/IEL, software and hardware design assurance. While this conservatively takes the severity aspect of the specific risk and treats it as the average, there is still the related issue of the conditional probability of being in the “worst case” condition. As credit for these conditional probabilities is increasingly being taken when showing compliance with the probability guidelines (example: AC25-7A, Appendix 7, HQRM), further consideration of these particular conditions in Task 3 was deemed appropriate, not only to assure the overall specific risk is adequately addressed, but also to assure that the probabilities guidelines associated with less severe outcomes are also met.

6.1.4.4 Flight & Diversion Time Task

The Flight Length and Diversion Time Task Group was assigned the task to identify and document the current approaches to exposure times where specific risk might be applied.

In order to provide current examples of possible Specific Risk application to flight length and diversion time the following examples were reviewed. More details like the background, the intent of relevant existing requirements, the existing guidance material, and the explanation of how specific risk is addressed had to be reviewed and provided in Task 2.

The first task of the group was to identify and discuss how At Risk Time, Flight Phase, Flight Time and Diversion Time were considered in showing compliance.

- "At Risk " Time
  - ARP 4761 Paragraph 2.2 and Appendix D paragraph D.11.1.3.2
  - AC/AMJ 25.1309 (Arsenal) Appendix 3 paragraph b2
- Flight Phase
  - ARP 4761 Appendix A paragraph A.1 and Appendix D paragraph D.11.1.3.2
  - AC/AMJ 25.1309 (Arsenal) Appendix 3 paragraph a and paragraph b2
  - AC 25.1309-1A
  - Draft AC 25.671
  - 25.901c exemption B717 docket no. FAA-2003-14201
  - Industry examples
- Flight Time
  - ARP 4761 paragraph 2.2
  - AC/AMJ 25.1309 (Arsenal) Appendix 3 paragraph c
  - Draft AC 25.671
  - Industry examples
- Diversion Time
  - FAR 121.161
  - ETOPS/JAR-OPS
  - FAA Part 25 Appendix K (new)
  - NPRM Docket No. FAA-2002-6717 Notice No. 03-11

- AC120-42A Extended Range Operation with Two Engine Airplanes
- JAR-OPS 1.246 Extended Range Operation with Two Engine Airplanes
- Return Landing Capability – Generic Issue Paper

The group concluded that At Risk Time, Flight Phase, Flight Time, and Diversion Time are examples of specific risk variables and they should be examined further in Tasks 2 and 3.

6.1.5 ASAWG Recommendation

The ASAWG recommends that "**Specific Risk**" be defined as the "**risk on a given flight due to a particular condition**". In addition, the categories of conditions that should be researched further during Task 2 and 3 should be the following:

- MMEL
- Design Variability
- Flight Time
- Diversion / Return to Land
- Latent Failure
- Active Failure
- Operating Mode
- Flight Condition
- Flight Phase
- At Risk Time

6.2 Task 2

The ASAWG reviewed during Task 2 the background and intent of relevant existing requirements, existing guidance material, and ARAC recommendations and explained how specific risk is addressed. In Task 2, the ASAWG had to document all current and proposed approaches to specific risk but should not establish how specific risk should be assessed. The outcome of this task was a description how specific risk is currently assessed and managed, by currently available regulatory guidance and by actual practice in recent certification programs. Task 2 also included the intended improvements and safety benefits of currently available regulatory guidance and actual practice.

The conditions associated to Specific Risk as recommended according to Task 1 result were categorized as followed:

- Latent Failure,
- MMEL,
- Active Failure / Design Variability / Flight Condition / Operating Mode.
- Flight Time / Diversion Time / Flight Phase / At Risk Time.

The task groups working at the above-mentioned categories were guided by the following questions:

- What is addressed (regulation or guidance)?
- Why is it addressed (regulation or guidance recommendation background / preamble)?
- How is it addressed?
    - Industry application / practices?
    - Acceptability of next most critical failure on safe operation?
    - Crew limitations and procedures?
    - Reliability of critical components?
    - Allowable exposure time?
    - Meet average risk criteria of 25.1309?
    - One failure away from catastrophe?

The following chapters give the results of Task 2. The results of each task group were detailed in tables addressing the above-mentioned questions.

6.2.1 Latent Failures Task

To meet the objectives of Task 2, the ASAWG established a task group to specifically address latent failures and to develop the table below.

The 6.2.1.1 table identifies Part 25 requirements, guidance, and other means that address latent failures, both directly and indirectly. The table also describes how latency is addressed by these criteria. The table identifies examples of application, including both FAA interpretation and industry practice.

In summary, the group found that there were a wide variety of approaches to addressing latency. Certain criteria apply to the latent side, or the active side, of failure combinations, or to the combined failure condition. Criteria also vary depending on whether the latent failure leaves the airplane one failure away from a catastrophic event. Different criteria are applied depending on the type of system being analyzed; for example, flight controls versus power plant installations. There may also be varying criteria for the same system depending on which rule is applied.

6.2.1.1 Latent Failures Task 2 table

→ Task 2 table.

Note: verify that you are on the "Latent" tab when opening the Task 2 table.

6.2.2 Active Failures & Design Variability Task

To meet the objectives of Task 2, the ASAWG established a task group to specifically address Active Failures, Design Variability, Flight Condition and Operating Mode and to develop the table below.

The table 6.2.2.1 identifies Part 25 and 33 requirements, guidance, and other means that address Active failures, Design Variability, Flight Condition and Operating Mode, both directly and indirectly. The table identifies examples of application, including both FAA interpretation and industry practice.

In summary, the group found that there were a wide variety of approaches to Active Failures. Certain criteria may apply to the active side or the latent side, of failure combinations, or to the combined failure condition.

The task of this group was to consider that the active failure occurred during a given flight. An active failure, which occurred before the flight, is addressed by the MEL or Aircraft Flight Manual.

In addition, the group realized that the airplane can be one failure away from a catastrophe. The group discussed several of these, but the easiest to grasp is the case on a two engine aircraft where one engine has failed. This, by itself, is minor or major, but now the aircraft is one failure away from a catastrophe, another failure that results in the loss of thrust from the other engine to maintain flight.

For design variability, quality escapes, as described in section 3 of this document, are outside the boundary of this document.

6.2.2.1 Active Failures & Design Variability Task 2 table

→ Task 2 table.

Note: verify that you are on the "Active & Design" tab when opening the Task 2 table.

6.2.3 MMEL Task

To meet the objectives of Task 2, the ASAWG established a Task Group to specifically address specific risk criteria related to the development of a Master Minimum Equipment List (MMEL). Table 6.2.3.1 was generated identifying; the regulations and/or guidance followed in developing an aircraft MMEL; the specific tailoring that an OEM may have utilized during the development of a MMEL; and just how the process addressed the specific risk issues related to the next most critical failure, crew limitations, reliability of critical components, allowable exposure times, quantitative dispatch times and being one failure from a potentially catastrophic condition.

In summary, all the OEMs are following the Flight Operations Evaluation Board (FOEB) process derived from FAA policy letters or a joint FOEB/JOEB process. Though the process that was followed was consistent across the industry, how the MMEL was actually derived and the data used to substantiate the recommended items in the MMEL varied. A common theme, however, did appear in that aircraft systems are becoming more and more functionally integrated using software and complex hardware logic devices to perform critical aircraft functions. Therefore qualitative design assurance processes, human factor aspects and common cause assessments are playing an increasingly important role with respect to MMEL relief.

6.2.3.1 MMEL Task 2 table

→ Task 2 table.

Note: verify that you are on the "MMEL" tab when opening the Task 2 table.

6.2.4 Flight & Diversion Time Task

To meet the objectives of Task 2, the ASAWG established a task group to specifically address Flight Time, Diversion Time, Flight Phase and At Risk Time. The task group documented what the primary issues were regarding the many regulations, guidance materials and industry examples, identified in Task 1.

The 6.2.4.1 table summarizes the associated regulations and background of each, along with industry application and practices. Also several questions were addressed regarding each of these examples. Some of these questions (written with MMEL in mind) are not applicable to flight time and diversion time and are so noted.

In summary, the flight time and diversion time team, notes that the ETOPS rule was recently revised and incorporates text that says it is necessary to meet 25.1309 under the ETOPS allowed configurations, so any changes that are made to 25.1309 is to cover ETOPS by default. Additionally, the item titled "Maximum flight time or maximum diversion time against mean flight time in Functional Hazard Assessments" is to address flight length (which may be driven by ETOPS flight times) assumptions in FHAs. The flight time and diversion time team recommends that all areas be further investigated in Task 3 and be considered within any specific risk discussion. Two items on the table, address basic assumptions made for a system or airplane in its functional hazard assessment with respect to flight length extremes. Assumptions made for shorter or longer than average flight lengths can in some cases result in severity of a failure condition being misclassified.

6.2.4.1 Flight & Diversion Time Task 2 table

→ Task 2 table.

Note: verify that you are on the "Flight" tab when opening the Task 2 table.

6.2.5 Task 2 Table – Excel Workbook

There are some incomplete fields with missing words in the tables from 6.2.1, 6.2.2, 6.2.3, and 6.2.4 due to the formatting issues, so that an MS Excel workbook is attached as follow:

ASAWG_Task 2 Table

[Click on the above link (icon) for opening the workbook]

6.3 Task 3

The ASAWG reviewed during Task 3 the results of Tasks 1 & 2 and determined the appropriateness, adequacy and consistency of the relevant existing regulations, existing guidance material, ARAC recommendations, and industry practices for airplane-level safety analysis. Task 3 demonstrated that a more consistent approach across systems is necessary.

The task groups (latent failure, active failure, MMEL, flight time) were guided by questions designed to help team members assess whether the existing regulations / guidance material / ARAC recommendations / industry practices are:

- Adequate?
- Appropriate?
- Applicable across systems?

The assessment was further guided by the following sub questions

- For adequacy:
  - Is the reason for the regulation/guidance given (why, preamble)?
  - Are all the relevant Hazardous and Catastrophic failure conditions covered?

- For appropriateness:
  - Is it commensurate with the potential level of risk?
  - Is it clear (unique interpretation)?
  - Is it a current requirement?
  - Is it practicable, i.e. achievable in itself and achievement verifiable?
  - Is it redundant with AC 25.1309 Arsenal Version?
  - Is it consistent with other rules and guidance related to the particular condition being reviewed?

- For applicability
  - Is it possible to be applied across all systems for this particular condition?
  - Is it possible to be applied across all systems for other particular conditions?

The task groups then identified the "fundamental issues" of the existing regulations / guidance material / ARAC recommendations / industry practices. "Fundamental issues" are the key approaches addressing Specific Risk.

For each "fundamental issue":

- The current practice was summarized in Task 2 results.
- The pros and cons of the fundamental issues & current practices were identified, and supported by Task 3 questions / answers with regard to adequacy, appropriateness and applicability across systems.
- One or more recommendations were provided.

For each fundamental issue recommendations for Task 4 were developed and reviewed by stakeholders (industry & regulators). This review generated comments, the disposition of which is documented in this report.

The following chapters give the results of Task 3. The results of each task group were detailed in tables addressing the above-mentioned questions (adequacy, appropriateness and applicability across systems) and the fundamental issues.

6.3.1 Latent Failures Task

6.3.1.1 Introduction

The latent task group reviewed the various system safety processes for different systems like flight controls, thrust reversers, etc. to determine if specific risk (the risk on an individual flight or flights) is addressed and how. Further consideration was given to whether the methodologies were adequate, appropriate and applied consistently across systems.

From this review, the group identified common concepts / ideas relating to methodologies that addressed specific risk. These were then condensed into fundamental issues. The pro and cons of each fundamental issue were documented and reviewed. From this sub-team review and a subsequent review by stakeholders, general recommendations and additional guidance were identified for Task 4.

6.3.1.2 Task 3 Table

As directed by the tasking, the latent task group determined if the regulations and practices were adequate, appropriate and applicable across systems. The results are

documented in the attached Task 3 table. This table was then used to perform the review described in section 6.3.1.3.

ASAWG_Task3 Table_Latent

6.3.1.3 Fundamental Issues

The latent task group reviewed current regulations and industry practices to determine common approaches that were used to address Specific Risk Concerns related to latency. After completing this review the task group took a brainstorming approach for allowing each member to voice his / her issues. Once everyone's issues were collected, they were condensed to the following four fundamental issues.

1 Limit Residual Probability (where "residual" is associated with the remaining risk following an assumed latent failure condition).

2 SRC Latent + 1 (addressing the question "What do you do" when a SRC latent failure condition leaves you one failure away from a catastrophe).

3 Definition of an SRC does not consider probability, leaving applicability too broad for Task 4 (need further criteria for when possible latency is not an SRC so that residual risk is not a concern).

4 Limit Latency.

6.3.1.4 Pros and Cons of Fundamental Issues

The pros and cons of each fundamental issue were discussed and documented in the attached Pros & Cons table. The table addresses each issue at a high level (is it worth implementing), and also focuses on the pros and cons of specific methodologies that incorporate this concept/issue. Based on these pros and cons, the information contained within the recommendation column resulted in the basic recommendations and additional guidance as discussed in 6.3.1.6 and 6.3.1.7, respectively.

ASAWG_ Pros and Cons Table_Latent

6.3.1.5 Stakeholder Review

The general recommendations and additional guidance (sections 6.3.1.6 and 6.3.1.7) were reviewed by stakeholders. This review generated comments, the disposition of which is documented in the attached Stakeholder Review table. Note that some of the stakeholder comments were marked as being applicable for consideration within Task 4 only.

ASAWG_Stakeholder Review_Latent

6.3.1.6 Recommendations for Task 4

Based on these pros & cons and recommendations from previous attached tables, general recommendations were made for each fundamental issue as follows:

6.3.1.6.1 First Fundamental Issue – Limit Residual Probability

- Establish a single consistent objective criteria and methodologies to limit the worst anticipated residual risk for catastrophic failure conditions.
- Determine whether limiting residual probability for any hazardous failure condition is warranted.

6.3.1.6.2 Second Fundamental Issue - SRC Latent + 1

- Give special consideration to this issue when addressing residual probability.

6.3.1.6.3 Third Fundamental Issue - Definition of an SRC

- Establish screening criteria (or filters) to determine which failure conditions will have additional specific risk criteria applied.

6.3.1.6.4 Fourth Fundamental Issue - Limit Latency

- Establish acceptable criteria to limit the exposure to latent failures which are not practical to eliminate.

  For example, limit the exposure to a latent failure in an inverse relationship to the failure rate such that maximum total probability of the latent failure is less than some TBD fixed value (e.g., some of the current practices use 1E-03).

  We recommend that this issue be carried forward as an and/or consideration with Fundamental Issue 1.

6.3.1.7 Additional Considerations for Task 4

The following additional considerations for Task 4 were derived from a review of the pros and cons associated with each fundamental issue. These additional considerations convey guidance for interpreting the intent of the general recommendations.

1 Limit the application of both residual risk and latency criteria chosen in Task 4 to Catastrophic failure conditions. Limiting residual probability for hazardous failure conditions may not be warranted and will need to be further addressed. [Note: Part 33 Engines worst case failure condition is "Hazardous" by definition of 33.75; there are some concerns with hazardous failure conditions which (a) border on being catastrophic (e.g. 1 in 50) or (b) result in 1 or 2 fatalities].

2 Limit the application of both residual risk and latency criteria (e.g., Fundamental Issue 3, see 6.3.1.6.3) chosen in Task 4 by probability and/or cutset order. Only a subset of possible configurations needs to be reviewed and will be determined in Task 4.

3 Establish both the residual risk and latency criteria chosen in Task 4 to set-up a control or acceptable level of risk for the subset population or fleet consistent with the current average risk criteria (e.g., do not drive 1E-09 failure combinations to 1E-12, etc.).

4 Limit the application of both residual risk and latency criteria so that they do not result in excessive analytical workload. Keep the criteria and process as simple as possible.

5 Minimize the architectural impact of both the residual risk and latency criteria chosen in Task 4 by considering the industry standard of reliability range (e.g. MIL-HDBK-217F, TELCORDIA, FIDES, NPRD and EPRD) for components. For example, take a dual failure cutset scenario -- neither the residual risk nor latency criteria should be outside the predicted reliability range of electronic components within that cutset.

6 Limit the application of both the residual risk and latency criteria chosen in Task 4 so that they do not routinely force significant increased model resolution (e.g., the use of LRU level basic events and associated MTBFs should be acceptable in fault tree models if justified by either a FMEA or a common cause analysis). Criteria should account for the existing conservatism in prediction methods like part count or part stress analysis used to calculate MTBFs when applied at the LRU level.

7 Limit the application of both the residual risk and latency criteria and policy chosen in Task 4 so that they do not adversely impact the risk of maintenance errors [e.g., increase the frequency such that traditional shop maintenance is moved to the flight line, increase the frequency of RII tasks (Required Inspection Items), etc.].

8 Establish in a clear, concise manner that both the residual risk and latency criteria chosen in Task 4 will recognize that exposure times are dependent upon when the failure occurs within a specific failure sequence (i.e., exposure times will change based on failure sequence).

9 Establish in Task 4 that “SRC Latent + 1” failure conditions that are catastrophic may be allowed, but should be limited via criteria which are as deterministic and objective as possible. If objective criteria are not attainable, resorting to more subjective case by case engineering judgments may be needed. Deterministic criteria examples are (1) reliance on the one remaining failure that has a failure distribution to some known confidence level, or (2) reliance on the integrity of a single component to those meeting standardized “critical parts” acceptance criteria (examples: special process controls on design, production, operation, and/or maintenance to limit failures of critical parts such as turbine disks or wiring), etc.

10 Establish in Task 4 criteria for addressing “SRC Latent +1” failure combinations that are consistent across systems, that do not drive unnecessary redundancy; and that do not drive unnecessary maintenance. Any SRC latent + 1 criteria is not to be defined so broadly that for example 90% of the time the cutset under evaluation could not meet the criteria and thus required additional redundancy.

11 Only allow latency which (a) cannot be eliminated or further reduced through practical means (i.e., like AC 25.1309-1A does now, indicate that relying on maintenance to detect latent failures is undesirable and should not be used in lieu of practical monitoring, etc.), [Note: may need to add more clarifying words in AC 25.1309 to define "practical" (e.g.. bring in technical and economic feasibility, design complexity, maintenance costs, regulatory burden and reliability)] and (b) meets an acceptable total probability criteria (e.g. less than 1E-3).

12 Establish in a clear, concise manner in Task 4 that exposure times equal to the life of the airplane in 3rd order cutsets (or 4th order cutsets, or 5th order cutsets, etc.) will not be prohibited.

6.3.2 Active Failures Task

6.3.2.1 Introduction

The active task group examined the current regulations and guidance material identified in Task 2.

6.3.2.2 Task 3 Table

As directed by the tasking, the sub-team determined if the regulations and practices were adequate, appropriate and applicable across systems. The results are documented in the attached Task 3 table. This table was then used to perform the review described in section 6.3.2.3.

ASAWG_Task 3 Table_Active

6.3.2.3 Fundamental Issues

To meet the objectives of Task 3, the Active task group identified the following fundamental issues:

- After the first failure, you are still more than one more failure away from a catastrophe (not universal for all situations, e.g. dual channel system),
- After the first active failure, there are ways to control (identify, quantify) the residual risk,
- Assure compliance when considering the effects of aging and wear.

6.3.2.4 Pros and Cons of Fundamental Issues

Upon review of the fundamental issues, the group concluded that the first fundamental issue was a subset of the second, and only carried the second and third fundamental issues forward. Pros and cons of current practices for the fundamental issues were then discussed, and those results are presented below:

6.3.2.4.1 "After the first active failure, there are ways to control (identify, quantify) the residual risk"

"Pros" Attributes:

- Regulations/guidance control (identify, quantify) the residual risk after an active failure

"Cons" Attributes:

- Current practices for limiting residual risk are inconsistent across systems.
- Inconsistent quantitative requirements for residual risk may:
  - lead to unbalanced system architectures (e.g. in case of extremely remote required by 25.981)
  - result in the average risk being significantly below the 1e-9/1e-7 criterion (i.e. unnecessary additional redundancy),
  - lead to unnecessary additional maintenance,
  - drive reductions in maintenance intervals that would have a net adverse impact on safety (e.g. cause critical maintenance to be moved from the hanger to the flight line)

6.3.2.4.2 “Assure compliance when considering the effects of aging and wear”

“Pros” Attributes:

- 25.1309 was identified as the place where aging and wear are currently addressed. 25.1309 considers aging, wear by assuming a constant failure rate based on service history that includes aging and wear.
- The analysis should establish life limits or other restrictions to ensure that the failure rate used in the analysis is constant.
- Doing an analysis using a time dependent failure rate is not required if the applicant has established life limits or other restrictions to ensure the failure rate is constant.
- 25.1309 and 25.981 are consistent with regard to aging and wear aspects.

“Cons” Attribute:

- System component life limits established to protect against aging and wear out are not documented consistently.

6.3.2.5 Stakeholder Review

The general recommendations were reviewed by stakeholders. This review generated comments, the disposition of which is documented in the attached Stakeholder Review table.

ASAWG_Stakeholder Review_Active

6.3.2.6 Recommendation for Task 4

6.3.2.6.1 Recommendation for the first fundamental issue

The regulations address this fundamental issue by using different quantitative values for different systems. Today's regulations / guidances are inconsistent and a more standardized approach is recommended.

This approach should:

- allow for different residual risk criteria for two channel systems and for more than two channel systems,
- not result in the average risk being significantly below the 1e-9/1e-7 criterion (i.e. unnecessary additional redundancy),
- not lead to negative consequences for maintenance,
- continue to allow qualitative analysis for simple and conventional systems,
- be consistent with the latent failure sub team recommendation(s).

6.3.2.6.2 Recommendation for the second fundamental issue

For aging and wear, the current regulations / guidance require further review. AC 25.1309 Arsenal currently states, "Average Probability per Flight Hour should be estimates of the mature constant failure rates after infant mortality and prior to wear-out …" For mechanical components whose probability of failure may be associated with non constant failure rates, reliability analysis may be used to determine component life limits.

In Task 4, develop recommendation for consistently documenting system component life limits that are necessary to protect against aging and wear out.

6.3.3 MMEL Task

6.3.3.1 Introduction

A review of FAA, TCCA and JAA/EASA guidelines and policy material on the development and approval of the MMEL was conducted in Task 2. Task 3 reviewed the results of Task 2 to determine the appropriateness, adequacy and consistency of the existing guidance and policy material relating to the development and approval of the MMEL. This task was also intended to determine if a consistent approach to MMEL development is needed with regard to Specific Risk.

The MMEL/MEL is the authority approved document that allows dispatch of the airplane with inoperative equipment. The SR tasking is concerned with the conditions where the airplane does not meet the average reliability requirements of 25.1309 when dispatched with inoperative equipment.

The current processes employed by OEMs and Authorities are:

- The OEMs currently provide SR assessments on selected systems based on experience and technical knowledge

  (a) All the OEMs represented in the ASAWG performed quantitative analysis on all or selected systems to support entry on a proposed MMEL.

  (b) The analysis methodology is consistent with current accepted arsenal AC25.1309 recommendations for reliability analysis with only the selection and approval criterion differing
- Selected MMEL items may be assessed during Function and Reliability (F&R) flight testing conducted as part of the operational evaluation process.
- The flight standards process is independent of the certification process.
- Selected (proposed) MMEL items are reviewed by the FOEB/JOEBs using engineering cab simulation.
- Selected (proposed) MMEL items are reviewed by engineering analysis using both certification data and requested analyses.
- In service events are constantly monitored by the FOEB/JOEB chairman to ensure continued acceptability of individual MMEL items.

The MMEL group finding in this task is that SR is not the main concern during MMEL dispatches. Far more important are the airplane's operational characteristics in its dispatch condition as well as its operational characteristics after the next worst case failure.

After consideration of these current processes, the MMEL group conclusion is that the current policies and practices concerning the development and approval of the MMEL over the past several decades, has consistently demonstrated a high level of reliability and comprehensiveness in maintaining the necessary safety margins that both the engineering and operations communities have come to expect and require.

6.3.3.2 Task 3 Table

The Task 3 tables associated to the MMEL Task Group can be found at the link below. These include responses from the stake holders to the questions of Adequate, Appropriate and Applicable across Systems. In the case of the latter of these questions "Applicable across Systems", this question and some of the questions used to determine if it was "Appropriate" were considered not to be applicable to the MMEL case. The responses were used to help derive the task group's fundamental issues.

ASAWG_Task 3 Table_MMEL

6.3.3.3 Fundamental Issues

The MMEL Task Group identified two "fundamental issues" from the application of the existing regulations/guidance material and various industry practices used in the development and supporting rationale of a MMEL as defined in the Table above. The fundamental issues identified are:

1. There is no explicit guidance on methodology for conducting specific risk evaluation for dispatch under a MEL ("Limiting Residual Risk").

2. The explicit guidance / methodology on the application of the next worst failure criteria when developing a MMEL ("One Failure Away").

6.3.3.4 Pros and Cons of Fundamental Issues

During the consolidation of the fundamental issues at the ASAWG level the two MMEL issues were placed under the headers of "Limiting Residual Risk" and "One Failure Away". Each fundamental issue was then reviewed with the "Pros" and "Cons" identified. These attributes for each review are:

6.3.3.4.1 Limiting Residual Risk

"Pros" Attributes:

- In general, the application used by the various OEMs relates back to the 25.1309 criteria, and then relies on a qualitative review to accept variances. This permits adaptability while still providing regulatory review in the loop.
- The criterion used by large transports appears to align well with some of the quantitative criteria by the other task groups. As an example if 1.0E-7 criteria is acceptable provided you are not one random system failure away then you potentially have a balanced system that would require two random failures (less than 1.0E-3 each) which should be acceptable depending on the outcome from the Latent and Active groups.

"Cons" Attributes:

- There currently is no design guidance, therefore, it lets the various OEMs and authorities determine what is appropriate.
- The application by the various OEMs to require full compliance to 25.1309 criteria with P=1 is conservative. There currently is no design regulatory guidance so it lets the various OEMs and Certification Offices to determine what is appropriate, this provides a disparity across OEMs.
- The application by the various OEMs to require full compliance to 25.1309 criteria with P=1 is conservative but may not be consistent with other conditions such as latent failures.

6.3.3.4.2 One Failure Away

"Pros" Attributes:

- For systems the practice makes sense irrespective of the probability of the next single failure. This is typical because the best failure rates you see systems exhibit is between 1.0E-4 and 1.0E-5.
- Prior to dispatch (while on the ground) the discrepancy is known and if deemed necessary, repair can be made.

"Cons" Attributes:

- The specific conditions related to interaction of systems and structure may be a peculiarity but one that this black and white philosophy does not cover well. In structural conditions where the next failure may be on the order of 10-7 it may make

sense to permit a short term dispatch criteria with one failure away if you know the failure is not random in nature but exhibits wear out or fatigue characteristics that are very much controlled, and/or the exposure window is quite limited.

6.3.3.5 Stakeholder Review

Preliminary recommendations that were developed from the above "Pros" and "Cons" were reviewed by stakeholders. This review generated comments, the disposition of which is documented in the attached table.

ASAWG_Stakeholder Review_MMEL

The following recommendations account for the comments provided in the above Table.

6.3.3.6 Recommendation for Task 4

The final evaluation of the current policies and practices implemented by OEMs and the various regulatory organizations concerning the development and approval of the MMEL over the past several decades, has consistently demonstrated a high level of reliability and comprehensiveness in maintaining the necessary safety margins that both the engineering and operations communities have come to expect and require. However, if a numerical analysis is used to support a MMEL proposed item some MMEL policy guidance would be beneficial to ensure consistency in approaches and methodologies.

During Task 4, it is recommended that a standardized methodology be prepared for Flight Standards to review and consider in their guidance and policies on MMEL development. As a minimum, the following attributes should be considered when developing this MMEL methodology:

- When specific risk should be used to support an individual MMEL item proposal.
- Consideration of MMEL dispatches when the next worst case failure could lead to a hazardous / catastrophic conditions.
- Architectural considerations of complex systems.

6.3.4 Flight & Diversion Time Task

6.3.4.1 Introduction

The Flight Time Team reviewed during Task 3 the results of Tasks 1 & 2 to determine the appropriateness and adequacy of the relevant existing regulations, existing guidance material, ARAC recommendations, and industry practices for airplane-level safety analysis. The intent of this review was to determine if a more consistent approach across systems is necessary.

The flight time task group was guided by questions designed to help team members assess whether the existing regulations/guidance material/ARAC recommendations/ industry practices are adequate, appropriate and applicable across systems.

As described above the flight time task team evaluated whether the available regulations and guidance material were adequate to be applied across systems. This included an assessment of whether the regulation or guidance was clearly written, current, practical and verifiable. The regulations, guidance and practices were also reviewed to evaluate whether it would be appropriate to apply a regulation that may have been written for a specific issue, across systems. This included a review of preamble material that describes why the regulatory material was written. Applicability of the regulations included an assessment of whether it makes sense to broadly apply the existing regulations across systems.

The flight time team assessed eight areas of regulation and guidance using the attached Task 3 table. Ultimately, we used this spreadsheet to look for common themes across the rows and columns for the eight areas to distill into the fundamental issues outlined below. We also reviewed the spreadsheets of the other teams to assure that the fundamental issues identified by the flight time team were not redundant.

ASAWG_Task 3 Table_Flight

Based on this assessment, it was concluded that a more consistent approach is necessary to avoid undue burden on the applicant and regulatory authorities. Regulations which have varied approaches to specific risk can lead to confusion and misapplication of rules across OEMs, Regulatory agencies, and suppliers. A more consistent approach will also assure that the level to which specific risk is regulated is warranted.

6.3.4.2 Fundamental Issues

The following three fundamental issues are recommended to be moved forward to Task 4.

1. The first fundamental issue is that the FHA needs to consider flight length and flight phase as relevant to the intensifying hazard class severity.

2. The second fundamental issue is to assess risk based on maximum flight time and maximum diversion time instead of average flight time.

3. The third fundamental issue is to assess risk during actual at-risk time versus normalizing by flight length (AC 25.1309-1A vs. AC 25.1309 Arsenal Version).

6.3.4.3 Pros and Cons of Fundamental Issues

6.3.4.3.1 Intensifying factors for hazard class severity.

In the current practice for 25.1309, the FHA considers intensifying factors in assigning hazard classification.

“Pros” Attributes:

> The hazard classification of a failure condition is complete (and correct) when both operational and environmental factors are considered along with the failure(s). The definition of "failure condition" in AC25.1309-1A and Arsenal clearly includes consideration for these factors. More importantly, service history clearly shows the need to take these factors into account and the current practice allows engineering judgment when considering intensifying factors and hazard classification.

“Cons” Attributes:

> The FHA guidance is not clear on how many intensifying factors, of which flight length may be one, must be considered in combination. With enough "intensifying factors" combined, FHA hazard classifications could be unnecessarily raised, resulting in unreasonably high development assurance levels and increased complexity if added redundancy is required to comply with unrealistic hazard stack-ups. In addition, the distinction between hazardous and catastrophic is difficult to achieve, given existing guidance due to numerous possibilities of intensifying factors.

6.3.4.3.2 Risk based on maximum flight time and maximum diversion time instead of average flight time.

In the current process for 14 CFR 25 Appendix K the exposure times must consider maximum mission time and maximum diversion time for both group 1 and 2 systems and they must meet 25.1309 criteria per Appendix K25.1.1. In addition, in 25.1309, only average times are considered in numerical analysis.

“Pros” Attributes:

Using the maximum flight time is usually, but not always, conservative for all cases, so current practice results in most conservative approach.

“Cons” Attributes:

The 25.1309 probability criteria is based on the average flight, using maximum flight length for all cases which results in unnecessarily conservative designs. Also, the available guidance is unclear on how “ETOPS significant systems” should be analyzed.

6.3.4.3.3 Risk during actual at-risk time versus normalizing by flight length (AC 25.1309-1A vs. AC 25.1309 Arsenal Version).

The current process in AC 25.1309-1A 10.b.2 states that for a function which is used only during a specific flight operation; e.g., takeoff, landing, etc., the acceptable probability should be based on, and expressed in terms of, the flight operation's actual duration.

AC 25.1309 Arsenal Appendix 3.b.2 states that if the failure is only relevant during certain flight phases, the calculation should be based on the probability of failure during the relevant "at risk" time for the "Average Flight". The "at risk time" probability is then normalized by dividing by the average flight time.

“Pros” Attributes:

No pros were identified for having two different sets of guidance.

“Cons” Attributes:

The currently approved EASA and FAA guidance is in conflict with each other and requires harmonization. If only the Arsenal criteria were used per flight hour calculations under estimate the risk for those items where the exposure is concentrated in a segment of the flight, for instance takeoff and landing (where most accidents occur). If only the AC25.1309-1A criteria were used, by requiring short flight phase exposure times to have to meet the same criteria, it unfairly penalizes systems critical during short phases and is more conservative than average risk

criteria based on per flight hour. It could also result in increased complexity if added redundancy is required.

6.3.4.4 Stakeholder Review

6.3.4.4.1 Intensifying factors for hazard class severity.

During stakeholder review, there were several comments on each fundamental issue. A comment was made that extreme care should be taken in any clarifying language not to change the definition of the hazard classifications. This was noted in the Task 4 issues to consider for this item. Other comments to this fundamental issue were discussed and dispositioned without change to the recommendation.

6.3.4.4.2 Risk based on maximum flight time and maximum diversion time instead of average flight time.

During stakeholder review, there were three comments on this fundamental issue. One comment was that the working group should consider the definitions as per draft AC25.1535-1X (i.e. max. flight time, max ETOPS mission time, average ETOPS mission time, max diversion time) and using them consistently in the recommendation. This comment was incorporated into the recommendation. The other comments were to remember to consider impact on various operational rules in Task 4. This was incorporated into the recommendation as well. The other comment to this fundamental issue was discussed and dispositioned without change to the recommendation.

6.3.4.4.3 Risk during actual at-risk time versus normalizing by flight length (AC 25.1309-1A vs. AC 25.1309 Arsenal Version)

During stakeholder review, there were two comments on this fundamental issue. The comments lead to a clarification of the original recommendation to delineate that the AC 25.1309 Arsenal Version remained acceptable for average risk calculation, and Task 4 will only look at those conditions where specific risk criteria need to be developed. The recommendation was revised to reflect this change.

ASAWG_Stakeholder Review_Flight

6.3.4.5 Recommendation for Task 4

6.3.4.5.1 Intensifying factors for hazard class severity

The recommendation to resolve this first fundamental issue is to add text to AC 25.1309 Arsenal Version to clearly lead to the conclusion that FHA needs to consider intensifying factors expected in the approved envelope, including flight length, flight phase, and diversion time. The AC should provide qualitative guidance on when combinations of intensifying factors should be considered, and when combinations of factors can be considered to not be reasonable (e.g. icing+130 deg ambient temp). In addition, additional guidance should be added to clarify distinction between hazardous and catastrophic failure conditions without changing the hazard classification definitions.

6.3.4.5.2 Risk based on maximum flight time and maximum diversion time instead of average flight time

The recommendation for the second fundamental issue is that the maximum mission time and maximum diversion time should be used for hazard classification in functional hazard assessments. System capability, capacity and performance should be sized for maximum mission time and maximum diversion time as appropriate. Numerical analysis should use average flight time for the fleet under consideration. For ETOPS specific risk, this means Group 1 and 2 systems both use the average ETOPS mission time in their probability calculations. Diversion times should use the maximum diversion time of all flights in the probability calculations. Both ETOPS and non-ETOPS calculations should meet current 25.1309 criteria.

Various operational rules will be considered in development of the final recommendation in Task 4. Recommendation will be coordinated for consistency with ETOPS EASA NPA and Draft FAA AC (this clarifies the MOC, no rule changes proposed).

6.3.4.5.3 Risk during actual at-risk time versus normalizing by flight length (AC 25.1309-1A vs. AC 25.1309 Arsenal Version)

The recommendation to resolve the third fundamental issue is to use AC 25.1309 Arsenal Version paragraph 11.e(1) for average risk. For specific risk, determine if AC 25.1309-1A criteria should be used or other criteria developed for latent and active failures.

6.4 Task 4

TBD – Preliminary