



AEROSPACE RECOMMENDED PRACTICE

ARP5150™

REV. A

Issued 2003-11
Reaffirmed 2013-05
Revised 2019-01

Superseding ARP5150

(R) Safety Assessment of Transport Airplanes in Commercial Service

RATIONALE

Some information was not included in the first version that we now have material to include, plus some corrections and clarifications to existing text. The addition of sources of information publicly available on the internet was added. Also, all aviation companies need to include the Safety Management System process in their safety process and therefore some of that material needs to be added.

TABLE OF CONTENTS

1.	SCOPE.....	3
1.1	Purpose.....	3
1.2	How to Use This Document.....	3
1.3	Intended Users.....	4
2.	REFERENCE DOCUMENTS, DEFINITIONS, AND ACRONYMS.....	4
2.1	Applicable Documents.....	4
2.1.1	Airworthiness Documents.....	4
2.1.2	Industry Documents.....	5
2.1.3	Military Publications.....	5
2.2	Definitions.....	5
2.3	Acronyms.....	8
3.	SAFETY PROCESSES IN THE OPERATING FLEET.....	10
3.1	Overview of the Ongoing Safety Assessment Process.....	10
3.2	The Ongoing Safety Assessment Process.....	11
3.2.1	Establish Monitor Parameters.....	13
3.2.2	Monitor for Events.....	15
3.2.3	Assess Event and Risk.....	16
3.2.4	Develop Action Plan.....	20
3.2.5	Disposition Action Plan.....	22
3.2.6	Lessons Learned.....	23
3.3	The Integrated Ongoing Safety Assessment.....	24
3.4	Related Topics.....	26
3.4.1	Review of Process and Organization Effectiveness.....	26
3.4.2	Alternative Dispatch Conditions.....	26
3.4.3	Design Changes.....	26

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2019 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: <http://www.sae.org>

SAE values your input. To provide feedback on this Technical Report, please visit <http://standards.sae.org/ARP5150A>

3.4.4	Alternative Parts	27
3.4.5	Safety Processes and Human Performance	28
3.4.6	Maintenance Program Development	28
3.4.7	Process to Appendix Cross Reference	29
4.	IN-SERVICE DATA	30
4.1	The Systemic View of Safety Information	30
4.2	Categories of Data	30
4.2.1	Accident Data	30
4.2.2	Incident Data	32
4.2.3	Safety Recommendation Data	32
4.2.4	Other Official Data	32
4.2.5	Data from Manufacturers	33
4.2.6	Operator-Level Data	33
5.	METHODS AND TOOLS	35
5.1	Root Cause (Event Tree) Analysis	35
5.2	Weibull Analysis	36
5.3	Monte Carlo Simulation Analysis	36
5.4	Corrective Action Scheduling	37
5.5	Sensitivity Analysis	37
5.6	Reliability Growth Modeling	37
5.7	Human Factors Methods and Tools	37
5.7.1	FOQA	38
5.7.2	MEDA Tool	38
5.8	Fleet Risk Exposure Analysis	38
6.	BEING INVOLVED IN THE AVIATION SAFETY COMMUNITY	38
7.	NOTES	43
7.1	Revision Indicator	43
APPENDIX A	SAFETY SIGNIFICANT EVENT REFERENCE LIST	44
APPENDIX B	QUALITATIVE RISK ASSESSMENT	68
APPENDIX C	QUANTITATIVE RISK ASSESSMENT	78
APPENDIX D	ROOT CAUSE (EVENT TREE) ANALYSIS	87
APPENDIX E	WEIBULL ANALYSIS	100
APPENDIX F	MONTE CARLO SIMULATION	118
APPENDIX G	RELIABILITY GROWTH MODELING	137
APPENDIX H	FLIGHT OPERATIONAL QUALITY ASSURANCE FOQA	145
APPENDIX I	MAINTENANCE ERROR DECISION AID (MEDA)	151
APPENDIX J	OPERATOR SERVICE BULLETIN PROCESS	188
APPENDIX K	MANUFACTURER SERVICE BULLETIN PROCESS FOR SAFETY RELATED SERVICE INFORMATION	193
APPENDIX L	AIRWORTHINESS DIRECTIVE DEVELOPMENT PROCESS	195
APPENDIX M	HAZARD TRACKING	199
APPENDIX N	LESSONS LEARNED	202
APPENDIX O	FAA AND EASA QUANTITATIVE RISK ANALYSIS METHODS AND GUIDELINES	209
Figure 1	Overview of the ongoing safety assessment process	11
Figure 2	Ongoing safety assessment process	12
Figure 3	Numerical risk assessment overview	19
Figure 4	Integrated ongoing safety assessment process	25
Table 1	Database access	31
Table 2	Safety related conferences	39
Table 3	Safety related websites	41

1. SCOPE

This document describes guidelines, methods, and tools used to perform the ongoing safety assessment process for transport airplanes in commercial service (hereafter, termed “airplane”). The process described herein is intended to support an overall safety management program. It is associated with showing compliance with the regulations, and also with assuring a company that it meets its own internal standards. The methods identify a systematic means, but not the only means, to assess ongoing safety.

While economic decision-making is an integral part of the safety management process, this document addresses only the ongoing safety assessment process. To put it succinctly, this document addresses the “Is it safe?” part of safety management; it does not address the “How much does it cost?” part of the safety management.

This document also does not address any specific organizational structures for accomplishing the safety assessment process. While the nature of the organizational structure is significant to the quality of a safety program, this document focuses on the functions to be accomplished and does not attempt to define what the structure should be. The intent is to leave the greatest amount of flexibility to the organizations that use this document.

1.1 Purpose

This document provides a systematic process to measure and monitor safety to help determine safety priorities and focus available resources in areas that offer the greatest potential to improve aviation safety. The current practice for ongoing safety assessment relies primarily on input from individual carriers or operators, with substantial involvement from the manufacturers, suppliers, airworthiness authorities, and other aviation service providers. There are variations in practices at all levels throughout the industry. Also, air transport carriers, air cargo carriers, and manufacturers each use their own methods for accomplishing safety assessment. It is felt that the creation of an industry practice will enhance consistency of approach in how airplane safety assessment is conducted and how airplanes are operated worldwide. This document is not a regulation. It is, rather, a compendium of best safety practices gathered together as a reference. It allows the users to compare their existing methods to those listed herein to seek improvements.

To improve safety during the complete airplane life cycle, it is not sufficient to assess the safety of the airplane only during its design phase. Ongoing airplane operations must be evaluated for safety (e.g., maintenance or operation procedures). The airplane is also evolving and changing during the “In-Service” phase (e.g., obsolescence, modifications). Differences exist or can develop between the assumptions made during the design phase and how the airplanes are actually operated and maintained. For these reasons, safety should be assessed also during the “In-Service” phase of the airplane life cycle. In order to do that, information must be collected, monitored and analyzed. A large portion of this needed information may already exist in an organization's maintenance or warranty information databases.

In addition to maintaining the safety of the airplane, there is also a need to enhance safety wherever possible. This means that the user must always be alert to the opportunity to advance safety where possible and feasible.

The transport airplane accident rate has improved since 1975; however, the number of airplanes has greatly increased and will continue to increase. The transport aviation industry provides the safest form of transportation in the world, but each accident generates tremendous negative effect. Thus, it is imperative to constantly improve. This can be accomplished by continuously improving what we do and what we accept as adequate.

This revision contains several new practices (e.g., the Transport Airplane Risk Analysis Method (TARAM), Safety Management System (SMS)) that did not exist at the time of the original publication.

1.2 How to Use This Document

The intent of this document is to identify typical activities, methods, and documentation that may be used to perform safety assessments for airplanes (including their associated systems and equipment) and user operations. The document describes a number of valid methods for resolution of safety issues, selection of actions, and their scheduling. The specific applicability and usefulness of the individual guidelines, methods, and tools will vary among organizations and from situation to situation. The user is not constrained to use all of the elements contained within this document. Each organization needs to establish which sections may prove helpful in improving or supplementing its existing safety-related practices. The guidelines, methods, and tools provided in this document are to be used in conjunction with other applicable guidance materials.

The appendices are not stand-alone documents, but rather are to be used in conjunction with the information contained in the basic document. The user is cautioned not to use the appendices independently of the basic document. Document users are also cautioned not to ascribe greater importance or validity to one method or tool presented in the appendices over another when addressing safety issues. No hierarchy is intended, either explicitly or implicitly, by the authors.

1.3 Intended Users

The intended users of this document include but are not limited to:

- a. Operators
- b. Manufacturers
- c. Equipment suppliers
- d. Modification or repair centers
- e. Airworthiness authorities

Anyone involved with the safety assessment and safety management of transport airplanes in commercial service may be a potential user.

2. REFERENCE DOCUMENTS, DEFINITIONS, AND ACRONYMS

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 Airworthiness Documents

AC 20-176A	Service Bulletins Related to Airworthiness Directives
AC 25.1309	System Design and Analysis, Advisory Circular
AC39-8	Continued Airworthiness Assessments of Powerplants
AC120-92B	Safety Management Systems for Aviation Service
AD FAA-IR-M-8040	Airworthiness Directives
AMC 25.1309	System Design and Analysis, Advisory Circular (was AMJ)
FAA Order 8110.107A	Monitor Safety/Analyze Data
ICAO Annex 8	Continuing Airworthiness of Aircraft
ICAO Annex 13	Accident Investigation
ICAO Annex 19	Safety Management
PS-ANM-25-05	Airworthiness Manual

2.1.2 Industry Documents

AIA Project Report High Bypass Ratio Turbine Engine Uncontained Rotor Events

ARP4754 Guidelines for Development of Civil Aircraft and Systems

ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

ATA Spec 100 Specification for Manufacturer's Technical Data

ATA Spec 111 Airworthiness Concern Coordination Process

CAAM 1 Technical Report on Propulsions System and Auxiliary Power Unit (APU) Related Safety Hazards

CAAM 2 2nd Technical Report on Propulsions System and Auxiliary Power Unit (APU) Related Safety Hazards

CAAM 3 3rd Technical report on Propulsions System and Auxiliary Power Unit (APU) Related Safety Hazards

MSG-3 Airline/Manufacturer Maintenance Program Development Document MSG-3

2.1.3 Military Publications

MIL-STD-882E Standard Practice for System Safety

2.2 Definitions

This section provides definitions for terms uniquely used in this document.

Note: Terms with an * are intentionally defined differently versus ARP4761 and ARP4754, as those documents apply to aircraft/system development.

ACCIDENT: An occurrence associated with the operation of an airplane, that takes place between the time any person boards the airplane with the intention of flight, until such time as those persons have disembarked, in which: Any person suffers death or serious injury as a result of being in or upon the airplane, or by direct contact with the airplane or anything attached thereto; the airplane received substantial damage; any damage is caused to the property of a third party. (NTSB)

ACCIDENT PREVENTION STRATEGIES: An ongoing process of developing lessons learned from past prevention events to identify strategies for preventing future accidents. Use of a prevention strategy approach has the potential of preventing accidents by identifying and removing one or more links in the accident chain.

AIRWORTHINESS: The condition of an item (airplane, airplane system, or part) in which that item operates in a safe manner to accomplish its intended function.

ANALYSIS: A detailed examination based on decomposition into simple elements.

APPROVED: Accepted by the certification authority as suitable for a particular purpose. (ICAO)

ASSESSMENT: An evaluation process which may include one or more types of analysis and experience.

AUTHORITY: The organization or person responsible within the State (Country) concerned with the certification of compliance with applicable requirements.

CANCELLATION: Elimination of a scheduled flight because of a known or suspected malfunction and/or defect. Note: Cancellation of any or all of the flight legs of a multi-leg flight constitutes only one cancellation (WATOG).

CERTIFICATION MAINTENANCE REQUIREMENT (CMR): A Certification Maintenance Requirement is a required periodic maintenance task established through formal numerical analysis to show compliance with certification requirements.

COMPLEXITY: An attribute of systems or items that makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.

COMPLIANCE: A timetable for performing specified corrective actions (e.g., schedule maintenance, inspections, part replacements, alterations, etc.) to alleviate an identified safety related problem.

COMPONENT: Any self-contained part, combination of parts, subassemblies, or units, which perform a distinct function necessary to the operation of the system.

CONFIGURATION DEVIATION LIST (CDL): An approved list of items, such as access panels, caps, fairings, etc., normally forming part of the airplane exterior profile, the absence of which do not prevent dispatch (WATOG).

CONFORMITY: Agreement of physical realization of the item with the defining document.

CONTROL PROGRAM: The combination of compliance schedule and corrective actions needed to alleviate an identified problem.

CREW: Crew includes but is not limited to, the following participants in the aviation system; flight crew, cabin crews, maintenance personnel, dispatchers and crew schedulers, and air traffic controllers.

CRITICALITY: Indication of the hazard level associated with a function, hardware, software, etc., considering abnormal behavior (of this function, hardware, software, etc.) alone, in combination, or in combination with external events.

DEFECT: State of an item consisting of the non-performance of specified requirements by a characteristic of the item. A defect may, but need not, lead to a failure.

DISPATCH RELIABILITY: The percentage of scheduled revenue flights that depart without incurring a technical delay or cancellation.

ERROR: An omitted or incorrect action by a manufacturer, crew member, or maintenance person, or a mistake in requirements, design, or implementation.

EVENT: An occurrence that is of interest for airplane safety.

EXTERNAL EVENT*: An occurrence that has its origin distinct from the airplane, such as atmospheric conditions (e.g., wind gusts, temperature variations, icing, lightning strikes), runway conditions, and cabin or baggage fires. The term is not intended to cover sabotage.

FAILURE: A specific way in which a system, equipment, item, or piece-part may fail.

FAILURE CONDITION: A condition with an effect on the airplane and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operation or environmental conditions. A Failure Condition is classified in accordance to the severity of its effects as defined in regulatory advisory circulars.

FAILURE EFFECT: A description of the operation of an aircraft, system, equipment, or an item as the result of a failure; i.e., the consequence(s) a failure mode has on the operation, function or status of an aircraft, system, equipment, or an item.

FAILURE MODE: The way in which the failure of an item occurs.

FAILURE RATE*: The gradient of the failure distribution function divided by the reliability distribution function at time t . Failure Rate = $F'(t)/(1-F(t))$. If the failure distribution function is exponential, the failure rate is constant and the failure rate can be approximately calculated by dividing the number of failures within a hardware item population, by the total unit operating hours. Note: Failure rate may also be expressed in terms of failures per flight hour or per cycle.

FLIGHT CYCLE: A completed take-off and landing sequence.

HAZARD: A condition resulting from failures, external events, errors, or a combination thereof where safety is potentially affected.

HUMAN FACTORS: The optimization of the relationship between people and their activities by the systematic applications of the human sciences integrated within the framework of systems engineering.

INCIDENT: An occurrence other than an accident, associated with the operation of an airplane, which affects or could affect the safety of operation. (NTSB)

INFLIGHT SHUTDOWN: An engine shutdown which occurs at any time an airplane is airborne or has been committed to becoming airborne.

ITEM*: One or more hardware and/or software elements treated as a unit.

MALFUNCTION*: The occurrence of a condition whereby the operation is outside specified limits.

MASTER MINIMUM EQUIPMENT LIST (MMEL): A list of equipment and functions that need not be operative for safe flight and landing based on stated compensating precautions created during airplane type certification.

MEAN TIME BETWEEN FAILURES (MTBF)*: A performance figure calculated by dividing the total unit flying hours (airborne) accrued in a period by the number of unit failures that occurred during the same period.

MINIMUM EQUIPMENT LIST (MEL): An approved list of items that may be inoperative for flight under specified conditions cooperatively created by operators and regulatory authorities.

PARAMETER: A measurable or calculated quantity that varies over a set of values.

PILOT REPORT: Suspected or known malfunction or unsatisfactory condition entered by the flight crew into the airplane logbook and which requires maintenance action.

PROBABILITY: A measure of the likelihood of occurrence. When expressed qualitatively, words such as low, medium, high are frequently used. When expressed quantitatively, probability is the limiting value of the relative frequency of occurrence of events of interest, when the limit exists. Its value lies between 0 and 1.

QUALITATIVE: Those analytical processes that assess airplane safety in a subjective and non-numerical manner.

QUANTITATIVE: Those analytical processes that apply statistical and data based methods to assess airplane safety.

REDUNDANCY: Multiple independent means incorporated to accomplish a given function.

RELIABILITY: The probability that a system, equipment, or hardware item will perform a required function under specified conditions, without failure, for a specified period of time.

REVENUE FLIGHT: A flight intended to generate either passenger or freight revenue (or both).

RISK:* The frequency (probability) of occurrence and the associated level of hazard. Perceived risk is risk as seen intuitively by individuals. Predicted risk is predicted analytically from models structured from historical studies.

ROOT CAUSE: The initiator of a sequence.

SAFETY ASSESSMENT*: Safety Assessment is the monitoring, identification, assessment, and prioritization according to hazard/severity level and probability of occurrence of risks associated with operations in a company. A process dedicated to assuring that risk is identified and managed properly within established limits; a process of identifying, estimating, and prioritizing each risk; assessment of accident and injury, and determining if action should be considered.

SAFETY MANAGEMENT: Safety Management is the decision-making process involved with determining and implementing what level of risk and cost is acceptable in a company and controlling the risk to that level.

SERIOUS INCIDENT: Any event involving the operation of an airplane other than an accident where the event, or the event coupled with any other reasonably probable second event, has the direct potential to result in an accident. (ICAO)

SUBSTANTIAL DAMAGE: Damage or damage failure which adversely affects the structural strength performance, or the characteristics of the airplane, and which would normally require major repair or replacement of the affected component.

(Not considered substantial damage are engine failure or damage limited to an engine if only one engine fails or is damaged, bent fairings or cowlings, dented skin, small punctured holes in the skin or fabric, ground damage to rotor or propeller blade, and damage to landing gear, wheels, tires, flaps, engine accessories, brakes, or wing tips.) (NTSB)

SYSTEM: A defined combination of subsystems, equipment, or items that perform one or more specific functions.

VALIDATION: The determination that the requirements for a product are sufficiently correct and complete. For example; “Did I build the right house?” (with respect to my original expectations).

VERIFICATION*: The evaluation of an implementation to determine that applicable requirements are met. For example; “Did I build the house right?” (in accordance with the drawings).

2.3 Acronyms

A4A	Airlines for America
AC	Advisory Circular
AD	Airworthiness Directive
AIA	Aerospace Industry Association
AMOC	Alternative Means (Methods) of Compliance
AMSAA	Army Material Systems Analysis Agency
ARP	Aerospace Recommended Practice (SAE)
ASIAS	Aviation Safety Information Analysis and Sharing
ASRS	Aviation Safety Reporting System
ATSB	Australian Transport Safety Board
BASIS	British Airways Safety Information System
CAAC	Civil Aviation Administration of China
CAAM	Continued Airworthiness Assessment Methodologies
CDF	Cumulative Distribution (Density) Function
CDL	Configuration Deviation List
CFR	Code of Federal Regulations
CMR	Certification Maintenance Requirement
COS	Continued Operational Safety
DOE	Department of Energy
EAD	Emergency Airworthiness Directive
ECS	Electronic Control System
ETOPS	Extended Twin-Engine Operations
FAA	Federal Aviation Administration

FMEA	Failure Mode and Effect Analysis
FOQA	Flight Operational Quality Assurance
GAIN	Global Aviation Information Network
HCF	High-Cycle Fatigue
HF	High Frequency (VHF - Very HF)
IAR	Immediately Adopted Rule
ICAO	International Civil Aviation Organization
LCF	Low-Cycle Fatigue
LL	Lessons Learned
LRU	Line Replaceable Unit
MCAI	Mandatory Continuing Airworthiness Information
MEDA	Maintenance Error Decision Aid
MEL	Minimum Equipment List
MMEL	Master Minimum Equipment List
MRB	Maintenance Review Board
MSG-3	Maintenance Steering Group 3
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
NPRM	Notice of Proposed Rulemaking
NTSB	National Transportation Safety Board
OEM	Original Equipment Manufacturer
OHL	Operator Hazard Level
SB	Service Bulletin
SDR	Service Difficulty Report
SMS	Safety Management System
SRA	Safety Risk Analysis/Assessment
TARAM	Transport Airplane Risk Assessment Method
WATOG	World Airlines Technical Operations Glossary

3. SAFETY PROCESSES IN THE OPERATING FLEET

Ongoing safety management is an activity dedicated to assuring that risks are identified and unacceptable risks are eliminated or controlled. As such, the ongoing safety management process is a systematic and logical approach.

A robust Safety Management System (SMS) will help ensure that risks are identified and properly eliminated or controlled. There are many sections within ARP5150A that can help satisfy the requirements of SMS, including its Safety Risk Management (SRM) and Safety Assurance (SA) elements.

Removing the decision-making step from the safety management process leaves the safety assessment process, which this document describes. This process is accomplished by professionals whose job it is to handle the technical details of safety assessment. Results from the ongoing safety assessment process are provided for decision-making in safety management. This management decision-making is accomplished by those individuals responsible for choosing which projects are appropriate for the expenditure of company assets.

Safety is not self-sustaining. When an airplane is delivered and is in its pristine condition, it has an initial level of safety. As airplanes are operated, the level of safety is maintained through a continuing process of monitoring service experience, identifying safety-related issues and opportunities, and addressing these issues or opportunities through appropriate product or procedural changes.

3.1 Overview of the Ongoing Safety Assessment Process

The Ongoing Safety Assessment Process continues the effort started during the airplane design phase. It begins with the introduction of the new airplane and continues until the airplane is retired from service.

The Ongoing Safety Assessment Process includes three objectives:

1. Maintain the airworthiness (certification) of the airplane:

In-service events are assessed based on effects on the level of safety intended in the certification process.

2. Maintain the safety of the airplane:

In-service events are assessed against the internal safety objectives of the organization.

3. Improve the safety of the airplane:

In-service events are assessed to identify opportunities to decrease their number or to surpass the safety objectives of the organization.

The safety assessment process is expected to be continuous, iterative, and closed-loop. When an event is identified, assessed and action implemented, the monitoring continues, to validate the effectiveness of the action.

The safety of the airplane depends on numerous factors, including the original design, manufacturing, flight crew and maintenance actions, operation effects, quality of parts, modifications, environment, and airplane aging.

Each user of this document is encouraged to develop their own Ongoing Safety Assessment process and continuously adapt it to their specific operating needs and criteria. Communication with other operators, suppliers, and manufacturers is advantageous throughout the process.

Figure 1 identifies a recommended high-level process for ongoing safety assessment. This generic process consists of five high level steps:

1. Establish Monitor Parameters
2. Monitor for Events
3. Assess Event and Risk
4. Develop Action Plan
5. Disposition Action Plan

“ESTABLISH MONITOR PARAMETERS” starts with determining the company specific safety structure, objectives, and goals. This process also establishes the monitoring parameters and their values.

“MONITOR FOR EVENTS” is the continuous process of looking for events of concern. This monitoring is based on the parameters established in the previous step.

“ASSESS EVENT & RISK” is the process initiated when an event is detected. This includes assessment of the event sufficient to determine if the event is really of concern. It also includes a preliminary determination of risk for use in prioritizing initial expanded evaluation and action plan development. Based on the seriousness of the event and the initial risk evaluation, a more detailed and complete risk assessment may be performed.

“DEVELOP ACTION PLAN” is the process that establishes the correction or improvement, such as a design change, or a change to operations, maintenance, or training procedures for the event identified. The action plan may not be needed if the event is determined to be sufficiently benign.

“DISPOSITION ACTION PLAN” is the evaluation and/or implementation of the action plan. This may include determination of whether or not the action will be implemented and the prioritization, scheduling, and implementation of that action. Once the action is completed, or when the determination is made not to implement the action, the process returns to the normal state of monitoring for events. In some cases, revision or update of the parameters monitored may occur as a result of the event or the action implemented.

3.2 The Ongoing Safety Assessment Process

A further decomposition of the high-level process (Figure 1) is shown in Figure 2. The process shown in Figure 2 represents a recommended iterative process within each organization. Each user of this document is encouraged to tailor this process to meet their specific operations. The following sections describe each ongoing iterative safety assessment process steps shown in Figure 2.



Figure 1 - Overview of the ongoing safety assessment process

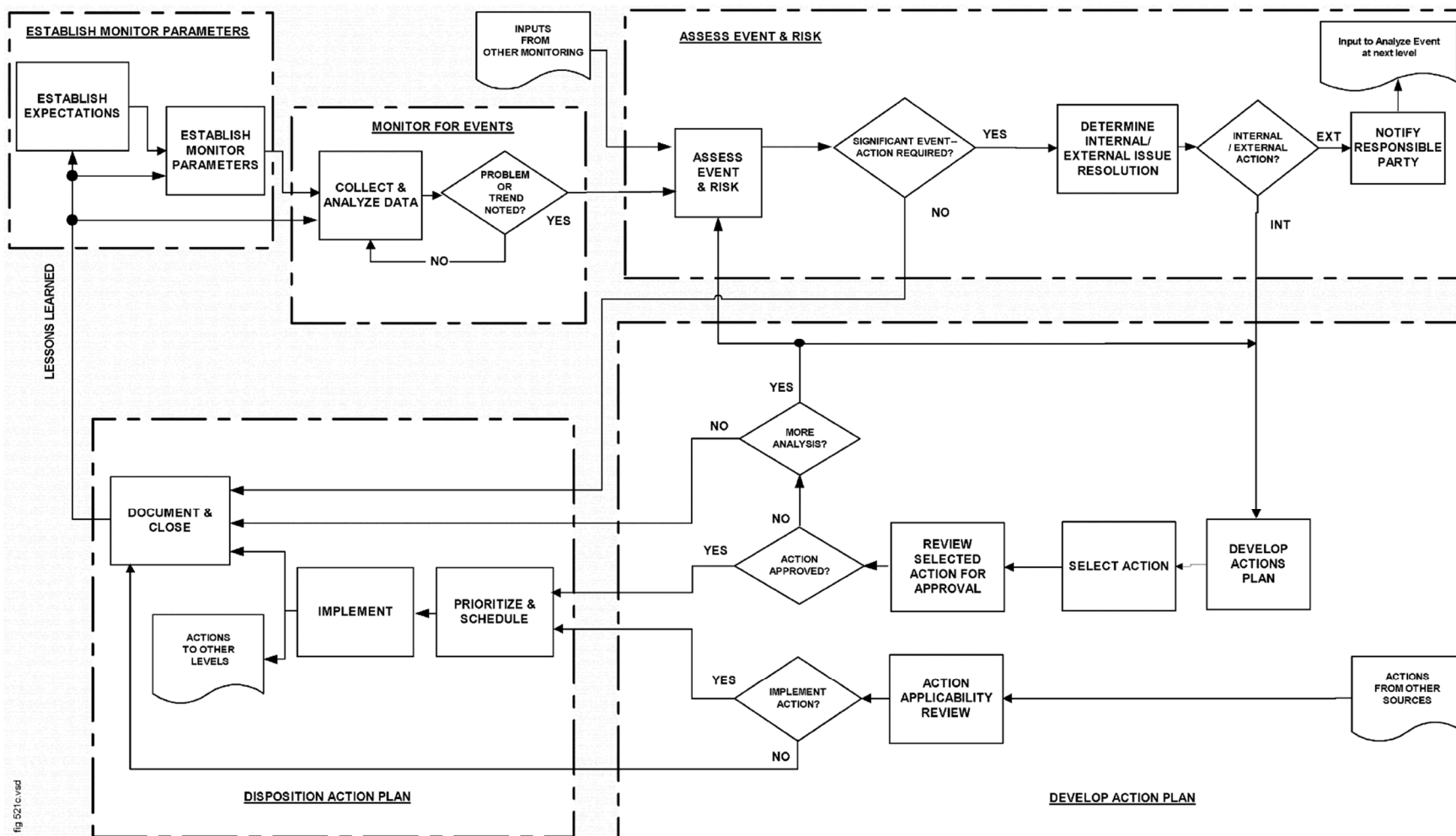


Figure 2 - Ongoing safety assessment process

3.2.1 Establish Monitor Parameters

The “ESTABLISH MONITOR PARAMETERS” phase shown in Figure 1 is expanded to “Establish Expectations” and “Establish Monitor Parameters” activities.

3.2.1.1 Establish Expectations

There are two basic aspects of the “Establish Expectations” step. The first of these is developing organizational structures and philosophies when initiating this process. This should include establishing the safety objectives and guidelines for the organization. The second is developing operational expectations for each specific fleet. This activity consists of determining what the day-to-day expectations of operation are, and what types of operations and performance will or will not be accepted within the fleet.

“Establish Expectations” encompasses the establishment of the company safety philosophy, assessment of the role of safety within the company structure, and the company’s definition of acceptable risk and performance levels. This company structure may vary from a structured formal safety organization to an informal structure. The safety organization should be sufficiently autonomous to ensure that it can influence the established safety philosophy.

There are at least two levels of expectations. The first are requirements imposed by the regulatory agency, which establish a minimum level of safety for operation. The second is the user’s own expectations, which may go beyond the requirements of the regulatory agencies. These internally imposed expectations may include parameters or criteria not covered by regulations, or levels of risk lower than required by regulations. The requirements and expectations may be based on a number of factors, including the following:

- a. Basic airplane requirements
- b. Safety analyses
- c. Regulatory reporting requirements
- d. Operational characteristics (e.g., cargo carriers versus passenger carriers or Cat I versus Cat IIIb)
- e. Airplane maintenance programs
- f. Environmental conditions of operation (e.g., tropical versus arctic operations)
- g. Experiences identified through previous use of the process (i.e., continuous improvement)
- h. Related industry accidents and incidents (where data is available)
- i. Lessons learned

The fleet specific expectations are passed on to the “Establish Monitor Parameters” phase of the process.

Once established, these expectations should be reviewed and adjusted whenever the user’s operation changes significantly or when external circumstances indicate the need for revision. Lessons learned from service experience, relevant certification assessments, post certification testing, product evaluations, and new technologies may also lead to the need for revisions of these expectations.

3.2.1.2 Establish Monitor Parameter Activities

The “Establish Monitor Parameters” step builds upon the expectations previously established. This step develops the information or data that should be collected, how it will be collected, and how it will be compared to expectations. This may vary from a minimum of existing regulatory-reportable issues to extensive data gathering and analysis programs. The exact parameters to be selected should be based on the level of the ongoing safety assessment process desired by management. The selection of specific parameters will be influenced by (among other things) the availability of data. Communication among the various organizations is beneficial in establishing appropriate parameters.

Appendix A provides an example list of airplane safety-related parameters and events that may be used as a starting point in the establishment of these parameters. In order to perform an effective ongoing safety assessment, many different types of data will have to be collected and analyzed. Section 4 provides more information on the types of data available to an organization and the sources from which the data may be obtained.

There are typically two types of parameters that are monitored. One type is the monitoring requirements generated as part of certification and identified in the Maintenance Review Board (MRB) document and subsequent Airworthiness Directives (AD). A second type is results from the user's own assessments (for example, an airline maintenance program may include a component functional check or removal at a specific interval).

Certain regulatory reporting requirements are called out in 14 CFR, 14 CFR Parts 121.703, 121.705, and 121.704. Parameters that may be required to be monitored include: engine overtemps, overweight landings, Service Difficulty Reports (SDRs), etc.

Based on the review of required reporting events described above, conditions may warrant the need for additional monitoring to help determine the event occurrence rate and the extent of the population at risk of the event.

The operator may also choose to monitor performance to assist in detecting problems before a serious event occurs. Monitoring the operation of specific systems can validate that their failure and availability rates are consistent with the supplier's or operator's expectations. While the occurrences of less-significant failures may be obvious to an operator because of their impact on reliability and the cost of operation, the operator may not be aware of more-significant failure conditions to which these failures contribute. Although it may be difficult for an original equipment manufacturer (OEM) or supplier to gather the data required to monitor the rate of occurrence of less-significant failures, this task should be accomplished whenever possible. Proactive monitoring of these lower events may identify potential problems early and allow for action to be taken to prevent more-serious events. This activity would be particularly effective at the OEM and supplier levels, as the action can be taken across on the affected worldwide fleet and not just within one operator's organization. It is therefore important that, where applicable, monitoring parameters for these lower-severity events be established at this stage.

As the Ongoing Safety Assessment process matures within an organization, the data being monitored, collection methods, and comparison processes should be continuously reviewed for the opportunity to make safety improvements. Continued service experience, new assessments, or post design evaluations are sources for lessons learned material. Lessons learned effects on the monitoring process are contained in 3.2.6 and Appendix N.

3.2.1.3 Monitoring Effectiveness of Previous Actions

After establishing the initial maintenance program for a given airplane, the operator, through its reliability program, continues to monitor the effectiveness of the program for the desired purpose of maintaining the airplane in a safe condition. The following are several means by which this is achieved.

Once actions are initiated to correct a problem, a follow-up validation process should be set up to monitor the implementation and determine effectiveness of the actions. This follow-up process may be accomplished by comparing pre- and post-action conditions of the systems affected by the correction. The frequency of comparison should be based upon probability and severity. During this post implementation review, a re-examination of the preliminary findings (e.g., teardown reports) may be accomplished. This verifies the implemented action eliminates the problem and that the assumptions used during the analysis are valid.

Adverse experience that deviates significantly from expectations or assumptions is grounds to revisit the safety assessment to determine which of the underlying assumptions are faulty, and whether additional actions are necessary. Since the immediate, short-term action is rarely expected to be the complete reaction to the problem, a complete validation of the effectiveness of any immediate action is likely not feasible prior to additional action being taken. Field experience and inspection results should continue to be monitored so that the new data acquired by interim action can be used to verify the effectiveness of the corrective action program. Final action carries with it an assumption that the failure mode has been effectively eliminated or mitigated; field experience should be tracked to validate this assumption. Care must also be taken to ensure that any unforeseen adverse impacts of actions are identified and evaluated.

Review of inspection findings allows for monitoring the effectiveness of the maintenance program. By reviewing the discrepancies generated by the performance of a regular task, the operator is able to get a good idea if the task itself and the interval at which it is performed are appropriate. For example, if too many discrepancies are reported against a specific task, the interval may need adjusting to a lower level check or the scope of the task may need to be broadened, so that any deterioration may be identified prior to a component or structural member needing replacement.

The reliability function also looks at the discrepancies discovered through unscheduled maintenance. By analyzing these discrepancies, recommended additions or changes to the existing maintenance program may be identified. Unexpected component removals for cause are indications that an adjustment to the maintenance task or interval is likely required.

The various engineering groups within an operator's organization may also play an important role in how effective a maintenance program is by continuously reviewing the various Service Bulletins (SBs) and Service Information Letters (SILs) issued by the manufacturer and the component vendors. These reviews establish the benefit of the SB recommendations to the operator's operational and maintenance procedures.

Once the expectations and monitoring parameters have been established, they are then used during the succeeding "MONITOR FOR EVENTS" step.

3.2.2 Monitor for Events

The "MONITOR FOR EVENTS" step consists primarily of the "Collect & Analyze Data" process.

An event is an occurrence. An event may be of interest by itself; e.g., an engine shut-down, or it may be of interest only in combination with other events that may or may not have happened at the same time; e.g., failure of one navigation receiver. An event may also be an operations or maintenance error. An event may or may not be significant for airplane safety. An event may be a single occurrence or a set or collection of separately identifiable occurrences that, for convenience of discussion and analysis, are thought of as a single event.

Monitoring for events encompasses two related, but distinct, elements: collecting and analyzing data, which monitors for previously unidentified or analyzed events of concern, and monitoring the effectiveness of previous actions, which monitors for events that have been already been evaluated through the process.

3.2.2.1 Collect & Analyze Data

The intent of the "Collect & Analyze Data" element of Figure 2 provides continuous monitoring of the actual operations to assess compliance with expectations. In this step, the data available to monitor any parameters defined in the "Establish Monitor Parameters" step should be obtained and analyzed. It is during the collection and analysis of this data that potential problems and trends will be identified. The cost of data collection and analysis is relatively low when compared to the potential cost of lost assets and equipment.

The following bullets highlight some example conditions that may be observed:

- Analysis of expected events occurring more frequently than anticipated provides for a comparison of performance data versus expected or acceptable frequency of occurrence for each event defined in the "ESTABLISH MONITOR PARAMETERS" phase. Any levels of occurrence closely approaching or exceeding the expected event's level of frequency indicate increasing potential for problems. These types of events may be monitored by reviewing the data results from scheduled airplane checks (sometimes called check reviews), and data from unscheduled maintenance (called reliability reports).

- If an unexpected or previously unknown event is detected, new parameters for this event should be established and added to the monitoring list. This event is then carried forward to “Assess Event & Risk.”
- The occurrence of minor events that could lead to increased risk should also be tracked to note any adverse trends. Minor events are not by themselves of concern, but may have more serious effects when combined with other events. When an adverse trend is detected, it should be investigated to determine if the trend indicates a safety concern. These types of events may be monitored using airplane reliability reports, employee suggestions, customer issues or Flight Operational Quality Assurance (FOQA) reports (see Appendix H).

It is recommended that each organization establish a formal means of collecting, summarizing and distributing the results of the “Collect & Analyze Data” element. The importance of accurate data should be emphasized. (Existing reliability programs may be extendible to encompass data collection for safety monitoring.)

Where no problem or trend is identified, the process continues in the “Collect & Analyze Data” element. When the analysis identifies a potential problem or trend, the data is summarized for use of the “ASSESS EVENT & RISK” phase of the process.

3.2.3 Assess Event & Risk

Once a potential problem or trend has been identified, either as a result of internal data collection and analysis or from an analysis performed by an external source, the “ASSESS EVENT & RISK” is initiated. This process develops a sufficient level of understanding of the event and its cause(s) to determine the possible consequences and assess the associated risk. Once these are known, a decision can be made as to whether or not the event warrants further action. If it is decided that the event does not warrant further action, the process should be recorded in the “Document & Close” step. If an event warrants further action, the appropriate organization(s) required to develop the action should be determined. If it is discovered that the problem requires external action, the responsible party should be notified of such action in a timely manner. If internal action is determined, then proceed to “DEVELOP ACTION PLAN.”

The “ASSESS EVENT & RISK” phase shown in Figure 2 is expanded to “Assess Event & Risk,” “Determine Internal or External Issue Resolution,” and “Notify Responsible Party.”

3.2.3.1 Assess Event & Risk

The assessment of the event and subsequent risk provides information that defines the magnitude of a specific safety issue. It also provides risk mitigation and optimization of inspection and modification programs designed to control in-service safety related problems. This assessment is performed to decide if an issue is a safety problem or to provide visibility of major risk issues. Risk assessments may be qualitative or quantitative and should always include a determination of severity and the probability of occurrence.

As a general principle, there should be an inverse relationship between severity and probability. Thus, safety issues of higher severity should be lower in probability.

In order for an organization's ongoing safety assessment process to be successful, it is essential that the “Assess Event & Risk” step effectively prioritizes the problems that occur so that the more critical problems are dealt with first. Although there are many prioritization schemes in use throughout the aviation industry, these schemes generally fall into three broad groups. These three groups differ based on what information is used as prioritization criteria.

Level 1 (Hazard Level): Severity (how bad is it?)

Level 2 (Risk): Severity + Probability (how bad is it, and how likely is it to happen?)

Level 3 (Fleet Risk): Severity + Probability + Exposure (how bad is it, how likely is it to happen, and what is the size and utilization of the affected fleet?)

An effective prioritization scheme evolves as the risk assessment task progresses. At each step in the review of a problem, it is important that priorities be established based on all relevant information available at the time. This evolution can be accomplished by moving from a Level 1 prioritization scheme to a Level 2 prioritization scheme, and then to a Level 3 prioritization scheme as probability and exposure information is collected.

3.2.3.1.1 Assess Event

The first step is to assess the observed event. Understanding the event obviously includes a review of the data obtained from the observed event, but also may entail searching accident and incident databases for similar occurrences of the event and potential problems resulting from it. These databases may be the user's own data sources, data shared with other operators on a limited basis, or industry, regulatory authority, government, or insurance company data. The search should be broad enough to detect similar problems in similar products or functions and should cover other airplane types to determine if the concern is an airplane or fleet specific issue, or a more general issue. Communication with other users of the equipment, the equipment manufacturer or airplane manufacturer may assist in this analysis.

In judging the severity of the event, it is important to understand the actual consequences that the observed event had on airplane operation. It is even more important, however, to understand potential airplane consequences if the event had occurred during more vulnerable circumstances. The event may be considered more severe if the consequences would be worse under different operating conditions (e.g., flight phase, environment).

A Level 1 problem prioritization scheme is most useful during the early stages of the safety assessment process, when little is known other than the observed or potential consequences to the airplane and passengers. The problem is assigned a severity category based solely on the seriousness of those consequences. Many different schemes for classification of safety events are used successfully within the aviation industry. The success of a particular classification method depends not so much on its specific details as on it being a formal and consistent part of an organization's safety process. Appendix B provides more details on the various event severity categorization schemes in use within the aviation industry.

It is also important at this stage to identify if the event would have been more severe had it occurred in combination with other failures. Time should be taken to identify all more severe failure conditions to which the observed event contributes. During the risk assessment phase, it is important to consider how the probability of the observed event influences the probability of these more severe failure conditions.

Research of the root cause should consider all known occurrences and initiators of the potential problem. Analysis of the causes of an event should consider:

- a. Aspects of the original design and design intent
- b. How the product or function's usage may have changed beyond initial design objectives
- c. Manufacturing aspects
- d. Specific utilization of the product or function relative to its intended usage instructions
- e. Maintenance of the product or function
- f. Complexity of the system
- g. Associated procedures and training
- h. Clarity/accuracy of the manuals and procedures
- i. Other applicable considerations

During the analysis of root causes, it may be necessary to define and gather additional data regarding sub-level events or failures leading to the condition. These issues could be failures or failure rates of other equipment or functions contributing to the event of concern. Where product manufacturer's installation, usage guidance instructions, and/or operational and operating environment assumptions are available, analysis of the actual installation and usage against those assumptions may aid in detecting and identifying characteristics leading to the unexpected operation or function. This review may identify discrepancies in modification or expected functionality.

A variety of tools may be used in determining the event extent, event causes, consequences of events, and event severity category. Section 5 presents a detailed description of some selected tools and their usage.

The assessment of the root cause should not be limited to the use of the analytical tools referenced above. Where possible, information should be obtained from computer fault logs, lab testing of suspected components, etc. A Line-Replaceable Unit (LRU) with a hard failure or a failure that can be duplicated either on the airplane or on the bench can provide a wealth of information to OEM or airplane manufacturer during the investigation. The ideal investigation may have these activities occurring in conjunction with the analytical process.

Again, the objective of this step is to gather information on the scope, causes, and severity of the event, not to produce an action for the event. The output of this phase is an overall understanding of the event suitable to form the basis of the Risk Assessment.

3.2.3.1.2 Assess Risk

The Risk Assessment begins once a potential problem has been identified from the event and should be refined as its scope, causes and severity are known. As the investigation progresses, the next step is usually to assess the probability of the problem. This assessment typically describes the probability of occurrence of the problem on per flight hour, although it can also be expressed on per flight cycle or other relevant time interval. The assessment can be either qualitative or quantitative. A Level 2 prioritization assigns a risk category based on both the severity category and this probability. One usage of this level is evidenced when two problems may have consequences of equal seriousness; using a Level 2 categorization, the problem with higher probability can appropriately be given higher priority.

Risk assessment factors may include failure modes, failure classifications, failure probability distributions, conditional probabilities, probability of detection at inspection, size of the "at risk" population, operational/maintenance constraints, and candidate actions.

The risk assessment should be verified by comparison with experience to date wherever possible. A team of experts from appropriate disciplines should review critical elements of the risk assessment.

Operators tend to use qualitative estimates of the probability of occurrence of a problem. Information provided by operators can be critical to the manufacturer's analysis of an event. The OEMs generally perform quantitative analyses since they have detailed knowledge of the equipment design. The OEMs may also have access to data on their worldwide fleet, which allows for a more accurate calculation of the event probability. Appendix B describes qualitative risk assessment methods, while Appendix C describes quantitative risk assessment methods, and 3.2.3.1.2.1 provides general guidance on possible processes in creating a quantitative risk assessment.

3.2.3.1.2.1 Developing a Risk Model

One of the first steps in creating a risk model is to determine what analytic method you should use, based on available data. Figure 3 (below) provides a sample procedure.

Step 1: Define the Failure. The failure criteria must be clearly and unambiguously defined. This definition must determine a clearly identifiable point in the propagation of the failure sequence; e.g., the first detectable crack, or cracking sufficient to cause detachment of blade airfoil. A clear engineering understanding of the problem to be modelled is required, and whether the failure is dependent on operating time or cycles.

Step 2: Determine the conditional probabilities and severity factors to relate the event to the possible consequences. This can be done various methods, such as a Markov Chain, historical rates, CAAM data, Event Tree, Engineering judgement, etc.

Step 3: Determine how many failures there have been to date.

Step 4: Determine if failure time (hours/cycles, etc.) for the individual components is available.

Step 5: Determine if failure calendar time is available. This will determine whether there is sufficient information to create a Weibull with estimated failure/suspension times/cycles, or if a Crow-AMSAA would be preferred.

Step 6: Determine if suspension time/cycles for the individual components is available or can be estimated. This will determine the recommended method.

Step 7: Once the current failure rate is modeled, determine if the failure rate is mitigated via some type of inspection/replacement process. A Monte Carlo simulation may be used to model the replacement/inspection risk.

Step 8: Evaluate the current risk versus the appropriate risk criteria to determine whether or not it is acceptable.

Step 9: If the current risk is not within limits, calculate the Risk Reaction Time and determine what method will be used to mitigate risk to acceptable levels (for example part replacement, inspection, redesign, etc.).

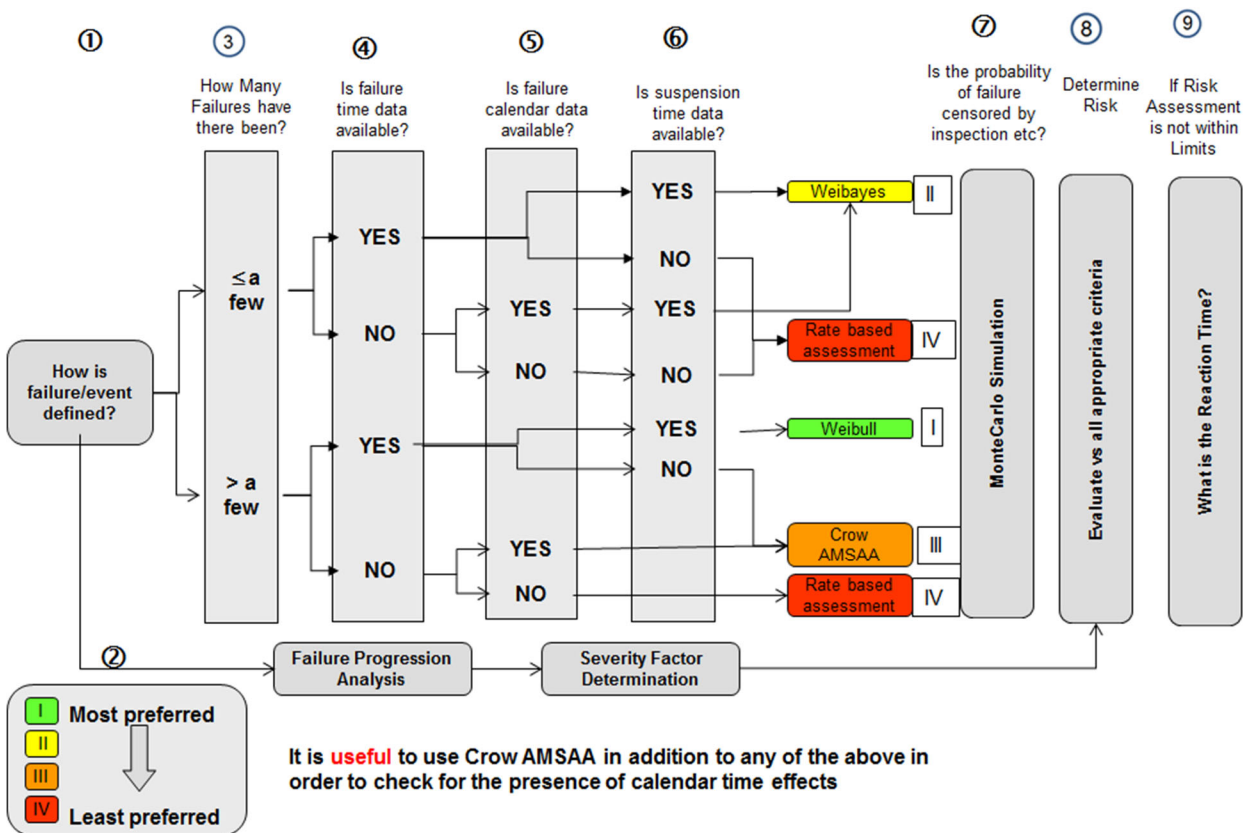


Figure 3 - Numerical risk assessment overview

With the initial risk assessment completed, the problem may be evaluated to determine if action is required, and, if so, to assign a priority to the resolution. Paragraph 5.4 describes two processes that may be used in scheduling implementation of corrective actions. It may be beneficial to establish a means of tracking the investigation or issue in order to ensure that the problem is resolved in a timely manner. One method of accomplishing this is to generate Hazard Summary and Hazard Tracking sheets. The Hazard Tracking Sheet and the Hazard Summary List are further discussed in Appendix M. A variety of tools may be used in assessing the risk of potential problems. Some of these tools and locations of information on these tools is provided in Section 5. As the study progresses further, information on the size of the affected fleet typically becomes available. Based on the fleet size and utilization, the future exposure can be determined. A Level 3 problem categorization can then be done, which assigns a fleet risk category based on severity, the per flight hour probability, and the future exposure. In effect, the Level 2 evaluation done earlier is extended to provide a “per fleet” probability. One usage of this level is evidenced when two problems may have equal severity and equal probability per flight hour; using a Level 3 categorization, the problem with the largest affected fleet (i.e., exposure) can appropriately be given higher priority.

The problem may apply to other airplane types/models as well. An assessment should be made to determine if other types may have the same problem. If so, the other types should be included in the “fleet” being considered.

The initial use of a risk assessment is to help provide an understanding of the magnitude of a specific problem. However, it will be necessary to revisit the risk assessment later to help judge the adequacy of proposed action plans. A specific proposed action plan will reduce the risk by reducing the probability or, alternatively, by lessening the severity (or possibly both). When there are alternative action plans proposed, risk assessment can be used to rank the plans, based on how much each plan reduces the probability or severity of failure.

An action plan, which provides adequate risk reduction for an individual “corrected” airplane, may still be inadequate if the action is implemented into the fleet too slowly. This can be judged via a “fleet risk” assessment, which expands the probability assessment to consider fleet size and the implementation schedule. When alternative implementation schedules are proposed, risk assessment can be used to rank the proposed schedules, based on how much and how quickly each proposed schedule reduces future exposure and risk.

Once the initial assessment of the event and risk has been completed, a determination of whether to accept the risk or initiate an action must be made. This determination should be accomplished by presenting the results of the event and risk assessment to the organization’s management and technical experts. As a practical matter in making decisions, economic impacts should also be considered by the organization’s management. These impacts are outside the scope of this document. The determination may include identification of additional monitor parameters as input to the “Establish Monitor Parameters” step.

If it is determined not to produce a corrective action for the event, the process proceeds to “Document & Close.” If the decision made is that the situation does warrant continued investigation, a determination must be made whether the responsibility to provide the action is internal to the organization or external.

3.2.3.2 Determine Internal/External Issue Resolution

If the organization identifying the event has the capability and responsibility to pursue the action, it does so, continuing through the process to the “DEVELOP ACTION PLAN” phase. If not, the responsible, external organization is determined.

3.2.3.3 Notify Responsible Party

Once the responsible organization has been identified, they are contacted and they begin evaluation with the “ASSESS EVENT & RISK” step within their process. Quite often the investigation continues with participation by more than one organization. For example, consider that an incident occurs in the field. The operator will assess the event and risk and may contact the OEM. It is important to understand that the processes between originator and actioned organizations are now interlinked. The originator may wish to coordinate and track the actioned organization's progress toward a timely action resolution. Good communication between all involved organizations is essential. Actions formulated by the external organization will reenter the originators safety assessment process at the “Action Applicability Review” step.

3.2.4 Develop Action Plan

The process continues with the responsible organization addressing the event in their respective “Develop Actions Plan,” “Select Action,” and “Review Selected Action for Approval” processes.

3.2.4.1 Develop Actions Plan

The “Develop Actions Plan” step encompasses any further research into event causes and the development of one or more potential actions. This should include risk assessment of the potential actions.

It may not be practical to develop actions for all problems simultaneously due to limited resources. Therefore, the organization must assign priorities based on their internal problem tolerance and possible regulatory oversight. These priorities allow an allocation of resources that focuses on safety-critical items first and the acknowledgment and tracking of operator-sensitive issues for review at a later time.

When developing an action, it is important to understand the root cause of the problem. This root cause may identify multiple failures that occurred over time or simultaneously and the sequence of these failures that led to the ultimate problem. By understanding these issues the responsible department can take each one of the failures and break it into two basic groups: hardware/software and human factors. Using these basic groups the action can be identified that best fits the needs of the user. Generic resolutions for these groups can be: replacement or redesign of an item, increase inspection frequency, retraining the operators, changing of a maintenance practice or addition of a system. It is desirable to focus on resolutions that reduce the probability of human error.

These resolutions should take into account the risk severity, the acceptable level of process or design change and the speed of risk reduction. In each case, the incremental risk associated with the interim solution should be reviewed, such as those associated with higher flight crew workload.

When the resolution is identified, it should be developed in detail, tested to verify the action and validate its effectiveness. The documentation should include the rationale and benefits of the proposed recommended actions (e.g., power the airplane down every “n” hours to force a power-up test to activate and verify absence of latent faults, thus maintaining the validity of the safety analysis).

3.2.4.2 Select Action

“Select Action” consists of evaluating the action options and identifying those with acceptable levels of safety. This step will usually involve presenting the action(s) for organizational approval. Typically, presentations are made by technical expert(s) to a review board or management position and should include a statement of the issue or concern, historical background, risk analysis results and assumptions, actions already taken and recommended future actions.

3.2.4.3 Review Selected Action for Approval

Based on the presentations made by the technical experts, the organization’s management or review board approves or rejects the proposed action. As a practical matter in making decisions, economic impacts would also be considered by the organization’s management. These impacts are outside the scope of this document.

For those actions approved by the organization’s review board or management, the implementation method depends upon the type of organization (e.g., Engineering Order (EO) for operators, Service Bulletin (SB) for manufacturers, Airworthiness Directive (AD) for regulatory authorities). Use of a consistent set of safety guidelines, ground rules, and objective safety analysis assists in ensuring that consistent decisions are made between product models and programs. Appendices K and L describe elements of manufacturer SB and AD processes, respectively.

If the decision made is to approve the proposed action(s), the process continues into the “DISPOSITION ACTION PLAN” phase and the “Prioritize & Schedule” and “Implement” steps begin.

If the recommended action is not approved by the organization, they must determine how to proceed. If more analysis is needed, then the process may return to either the “ASSESS EVENT AND RISK” step to reassess the significance of the recommended action, or to the “DEVELOP ACTIONS PLAN” step to refine potential action. If the recommended action is not organization approved and no further analysis is deemed necessary, the process moves to the “Document & Close” step. The decision and its justification are then documented and filed for future reference.

3.2.4.4 Action Applicability Review

The “Action Applicability Review” step is performed by the potentially impacted organization to determine if an externally created action (e.g., SB or AD) affects any airplane in their fleet.

Operators may receive externally developed actions in the form of service bulletins (SBs). Appendix J describes the operator process for handling SBs.

In the case of externally directed resolutions such as airworthiness directives (ADs), the basic action and implementation schedule will already be defined. For other resolutions, such as Alert Service Bulletins (ASBs), Service Bulletins (SBs), or Service Information Documents (SIDs), the basic action and implementation schedule will be suggested but will need to be factored into the operator’s overall implementation plan and prioritized. If the regulatory agency action or schedule cannot be met, the operator or manufacturer has the opportunity to request equivalent actions that provide the same level of safety. This forms the basis of the Alternative Means of Compliance (AMOC). The intent of the AMOC is to enable approval of options that were not necessarily conceived at the time of issuance of the original action, but that provide an equivalent level of safety to that afforded by the original action. The safety assessment process delineated in this document can be used to help determine if a proposed AMOC provides an equivalent level of safety. Appendix L discusses the regulatory AD process in more detail.

When the external action has been created to resolve an issue identified by the reviewing organization earlier, it should be carefully reviewed by the appropriate technical experts to ensure that it does in fact fully resolve that problem. Any concern with the proposed action should be communicated to the external party as soon as possible.

In cases other than ADs, a study to determine the costs and benefits may be performed. If the decision is to implement, the process continues to “DISPOSITION ACTION PLAN” phase and the “Prioritize & Schedule” and “Implement” steps begin. If the decision is to not implement the action, the process moves to the “Document & Close” step. The decision and its justification are then documented and filed for future reference.

3.2.5 Disposition Action Plan

The “DISPOSITION ACTION PLAN” phase is composed of the “Prioritize & Schedule,” “Implement,” “Actions to Other Levels,” and “Document & Close” steps.

3.2.5.1 Prioritize & Schedule

“Schedule” is unique to each organization and depicts their specific processes and approval cycles. The combined effects of hazard, probability of occurrence, risk exposure, and availability of parts and other resources assist in determining the priorities to implement the actions. During the normal execution of the process, several potential problems may be evaluated at the same time. This usually results in the need to prioritize the order in which problems will be corrected. The process encompasses determining relative priorities (e.g., risk reduction, cost, ease of implementation) of this and other actions and scheduling implementation.

This step may involve the scheduling of tasks and resources required to create and issue a service bulletin and to organize the availability of parts, etc., that will be required by the operators. If the affected airplane design is in production, the airplane manufacturer will also need to determine the production introduction of the corrected design. For an operator, this step may involve the scheduling required to incorporate an actual design change into airplanes in their fleet, or incorporate changes into their maintenance or operational programs.

The final aspect of this step is to establish a complete and coordinated implementation plan. Some simple action implementations may have very straightforward, simple, and non-time critical implementation plans. Other actions may require coordination of specific airplane changes combined with crew or maintenance procedure change requirements or training resulting in more complicated implementation plans.

Once an applicable implementation plan is developed and organizationally approved, actual implementation is initiated.

3.2.5.2 Implement

When the action plan is defined and verified to appropriately resolve the problem or concern, it can be implemented into the fleet or organization. Problem resolutions should be monitored for effectiveness to ensure that the action was effective in reducing or eliminating the problem. The monitor performance criteria and method of gathering and assessing the data should be defined within the “DISPOSITION ACTION PLAN” phase and forwarded to the “MONITOR FOR EVENTS” phase. If this monitoring determines the action is not effective, the problem reenters the ongoing safety assessment process, where additional data gathering and root cause analysis may be necessary. Re-addressing of the problem then continues through the normal safety assessment process, leading to revised action plans and implementations.

Verification and validation of the problem resolution should be an integral part of this step. Refer to ARP4754 for guidance in this area.

Unacceptable delays in the availability of the final action plan may necessitate development of an interim mitigating strategy such as an inspection program or modified operating procedures until the final action plan can be incorporated.

Although not always available in current practice, a closed-loop process is preferable; i.e., implementation should be carefully monitored to track completeness of the implementation process at any given time. This is particularly important in addressing ADs, manufacturer-required changes, or operator-driven changes, where knowledge of the status of percent of fleet addressed to date may be beneficial.

Throughout the process for any one potential problem, it is possible that new insight to “Establish Expectations” or “Establish Monitor Parameters” steps may arise. In these cases, the experience gained and lessons learned should be carried back into these steps and appropriate modifications put in place within the continuously operating portion of the assessment process. This iterative process improvement benefits effectiveness of the process for any specific user implementation.

3.2.5.3 Actions to Other Levels

Forward SBs, ADs, or proposed actions to other organizations that may also be affected for consideration of implementation. Some manufacturers have contractual agreements with operators for SB implementation tracking while others do not.

3.2.5.4 Document & Close

Normally, a problem resolution will be implemented through the issuance of an official technical document from the organization implementing the change. Examples of documents which may be changed include:

- a. Flight Operations Manual
- b. Engineering Orders
- c. Maintenance Alerts
- d. Maintenance Manuals
- e. Flight Operations Bulletins

For a manufacturer, the document issued may:

- a. Be focused toward the operator in the form of a Service Bulletin, Service Letter, All Operator Telex, Maintenance Tips, etc.
- b. Be directed toward its own organization, which may include new process instructions, production guidelines, new drawings, etc.

The regulatory agencies may issue an AD to ensure compliance with actions that are deemed mandatory.

In most cases, the document used to implement the change within the organization becomes the means for documenting closure of the project. In other cases, the organization may maintain a running log of all the problems in process and may update that log to show how the problem was resolved and which documents were used to close the issue, including those problems for which no action was taken.

In many cases, simply issuing a document will not resolve the problem. It is the response to the issued document by production, design, training, maintenance, or flight personnel that resolves the problems. Thus, the initial document used to implement the change may create a series of documents that must be acted upon. In many cases, new processes will be published, training programs will be developed, and, finally, personnel will be trained to act in a way that will resolve the problem. Continued monitoring may be required to ensure all processes, modifications, and training have been effective.

Assuming the series of documents, processes, and modifications have been accomplished and monitoring shows that they have successfully resolved the problem, the organization will then go back into a mode of monitoring parameters and perhaps evaluating lessons learned from the resolution process.

If no action was taken for the event, the decision and rationale are preserved in the Document & Close step.

3.2.6 Lessons Learned

The objective of a Lessons Learned process is to use in-service experience to improve all aspects of airplane operations and design. The introduction of a Lessons Learned process enables a systematic reuse of factual experience in an efficient way so that performance characteristics, such as the following, may be improved:

- a. Safety, reliability, availability, maintainability, cost
- b. Quality of products as well as quality of the company processes
- c. Number and cost of modifications of the products
- d. Compatibility of human/machine interface
- e. Satisfaction of users' needs

Appendix N presents a detailed discussion of the Lessons Learned process and the elements needed to make it successful.

3.3 The Integrated Ongoing Safety Assessment

A detailed, integrated industry flow chart is shown in Figure 4. Depending on the types of problems under consideration and decided depth of the ongoing safety assessment process, not all steps described above in 3.2 may be needed.

There are several users of the process described in the previous sections:

- a. Operator
- b. Airframe manufacturer
- c. Supplier
- d. Airworthiness authority

Each user incorporates the set of processes applicable to them. Figure 4 depicts three interactive processes and the communication flow among them. While the processes are similar for each type of user, the activities vary due to differences in the types of information available and considered, and the requirements and expectations. For example, an operator may have a different outlook regarding an in service event than that of the airframe manufacturer or an equipment supplier. The airframe manufacturer may refer to information not readily available to the operator or supplier (e.g., fault trees and/or FMEAs done during development).

Operators, airframe manufacturers, suppliers and airworthiness authorities may receive event notifications from their own monitoring or from other organizations. For example, when an operator recognizes a problem related to a specific supplier product, the operator process "Internal/External Action?" decision in Figure 2 identifies the action as not being an operator issue. The operator should contact the airframe manufacturer, or supplier, advising them of the problem. This identifies the event as an input for the manufacturer or supplier "ASSESS EVENT & RISK" process phase. The problem should be delegated to the responsible organization through the manufacturer and/or supplier processes, and that organization should develop the action. When the action is developed and organizationally approved, the action is given (by AD, SB, etc.) to operators and manufacturers as an input to a potential "Action Applicability Review" step.

The example above identifies three users (operator, manufacturer, and supplier). Parallel implementations of the processes also exist. One operator may detect a problem and advise other operators, or the airframe manufacturer and supplier working the issue may advise other operators. Similar instances may occur with multiple airframe manufacturers or suppliers, leading to a matrix of possible interactions.

There is also a fourth parallel path being executed by the regulatory authorities. This path results in airworthiness directives. In general, the Airworthiness Directive (AD) process is similar to the Ongoing Safety Assessment Process shown in Figure 2. The details in the AD process vary due to differences in the types of AD actions considered. Depending on the types of the problems under consideration and on the decided depth of the AD process, not all steps shown in Figure 2 may be required. The AD process and its regulatory elements, the coordination flow among the authority, manufacturers, suppliers and operators are discussed in detail in Appendix L.

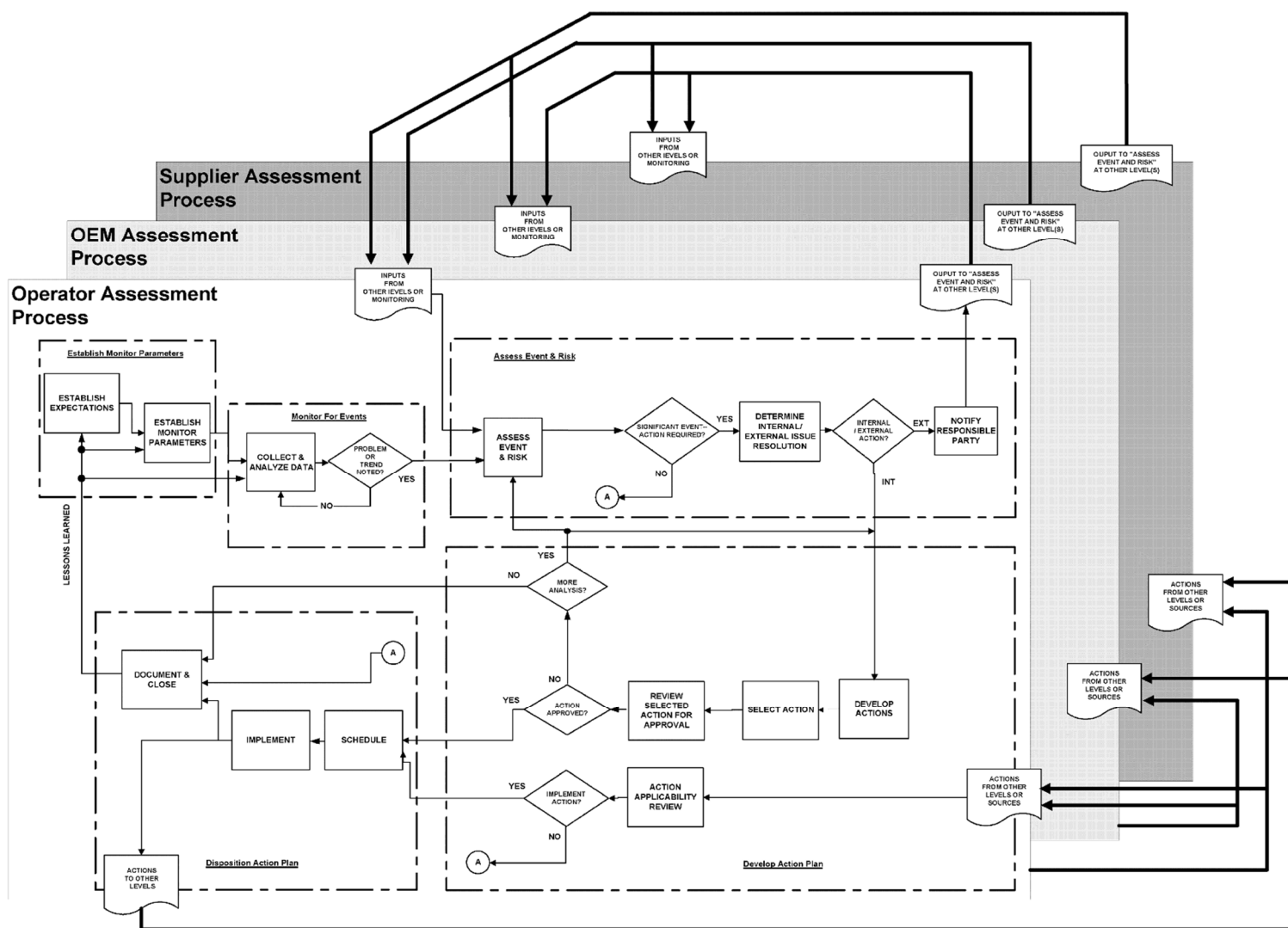


Figure 4 - Integrated ongoing safety assessment process

3.4 Related Topics

The following sub-sections describe independent topics related to the safety assessment process.

3.4.1 Review of Process and Organization Effectiveness

It is recommended that the ongoing safety assessment process include independent safety review practices as an integral part of the safety assessment process conducted by the organization. These reviews may be accomplished either internal or external to the organization. These reviews address the following two questions:

1. Is the organization following the safety assessment process?
2. How effective has the safety assessment process been?

3.4.2 Alternative Dispatch Conditions

The regulatory authorities require that all equipment installed on an airplane in compliance with the Airworthiness Standards (e.g., 14 CFR Parts 121, 135) and the Operating Rules (e.g., 14 CFR Parts 91, 121) must be operative. Experience has proven that, due to the various levels of redundancy designed into an airplane, operation of every system or installed component may not be necessary when the remaining operative equipment satisfies the airworthiness authorities. Therefore, certain conditional deviations from the original requirement are authorized to permit airplane dispatch. These "Dispatch Deviations" identify what is required to operate the airplane in the various non-standard configurations allowed by the type certification authorities-approved Master Minimum Equipment List (MMEL) and Configuration Deviation List (CDL), and by the operations regulatory authorities-approved Minimum Equipment List (MEL).

3.4.3 Design Changes

Where design changes have been made as a result of the safety assessment process, or for other safety-related reasons, it is reasonable to assume that consideration of safety impact has been made. However, there are other reasons for design changes, including producibility, functionality, or cost effectiveness. These should be reviewed for safety impact.

Dealing with these issues can be difficult, as there is frequently no single point or organization that controls the use of components. The most common processes here are likely to be training and awareness of potential issues by operator's procurement and maintenance personnel. The magnitude of the task may be reduced through identification of safety-related functions, products or components. With this identification in place, functions, products or components not identified may generally be excluded from any detailed safety review.

As an example, the primary hydraulic actuators, flight control computers, primary display systems, and engines and their controls frequently qualify as safety-related items and are subject to monitoring, while passenger entertainment and galley equipment may not require further monitoring.

The change categories addressed in this section include non-safety-related design changes, changes due to obsolete or non-procurable parts, and possible use of "counterfeit" or non-traceable parts.

3.4.3.1 Safety Impact of Non-Safety Design Changes

Design changes may be initiated in safety-related equipment to increase productivity, reduce cost, increase interchangeability, or various other reasons. These changes may be initiated by well-intentioned employees for very good reasons; however, those employees may be unaware of safety-related issues associated with the designs. Every change to safety-related equipment should be carefully reviewed by an engineer familiar with the function of the component, its safety implications, and, where possible, why it was initially designed the way it was. Examples of changes that may appear acceptable but may have adverse safety impact may include:

- a. Differences in surface machining or finish plating (e.g., servo slip clutches, components exposed to corrosive environments)
- b. Differences in form factors (some servo housings are intentionally non-symmetrical to preclude incorrect installation of critical parts where incorrect assembly may be difficult to detect and hazardous)

- c. Mechanical or electrical limitations of a component affecting operational characteristics
- d. Cable, tubing, or wire sized for non-standard forces or flows required for emergency situations, but apparently “excessively sized” for normal operation
- e. Changes in wiring that invalidate wire separation
- f. Changes to the finish on composite components

3.4.4 Alternative Parts

3.4.4.1 Substitution for Obsolete or Unavailable Parts

With today's technology and production processes, many parts that were in common usage and production in the past are becoming difficult or impossible to acquire. When parts used in safety-related products become unprocureable, substitute or alternative parts meeting all original requirements and qualifications will be identified, or products will be re-designed or re-certified with alternate parts incorporation.

When investigating alternative parts acquisition, the user should contact the original component manufacturer to identify qualified replacement parts whenever possible. Where this is not possible, the user should acquire the procurement specification of the original equipment parts and obtain assurance from potential replacement suppliers that their parts comply with the original specification, or identify specific areas of non-conformity. These areas of non-conformity should be carefully analyzed to determine if the differences will have a safety impact on the overall operation in all anticipated operating conditions and environments.

When components compliant with all of the original component specifications cannot be located, installation of parts that are non-compliant in a product, may cause the operation of the product to perform outside the limits of product certification. In some cases, analysis may identify these areas; in other cases, repeating some of the original certification testing may be required.

In many cases, the original equipment manufacturer (OEM) may have already generated service bulletin or modification recommendations to address the issue of unavailable parts. The manufacturer may also be able to provide information on the safety impact of certain replacement parts.

3.4.4.2 Counterfeit Parts

The expense and difficulty in obtaining qualified replacement parts for safety-related equipment has resulted in a black market of uncertified, uncertifiable, or counterfeit parts. In some cases, this is unintentional and the parts may meet the necessary qualifications but their compliance may not be verifiable and traceable. In other cases, the parts are intentionally misrepresented by opportunistic suppliers.

One approach to assuring that counterfeit parts are not introduced into the fleet is through training of procurement, supervisory, parts administration, and line maintenance personnel. This training should describe the issues and concerns, especially safety, and recommend that procurement employees deal only with known reputable suppliers, require certification of component traceability to be delivered with components, and beware of “too good to be true” availability or part pricing.

Line maintenance and employees administering parts stocking and distribution should be on the lookout for any differences in parts they usually use, and forward these parts and an explanation of their concerns to the appropriate channels for confirmation of certificability of the parts prior to their incorporation in an airplane.

3.4.5 Safety Processes and Human Performance

Human performance is an area of much current interest and research in the aviation field. The topic spans the spectrum from the original design of the airplane to all aspects of its operation and maintenance. This document considers human performance only as it plays a role in the ongoing safety assessment for a specific scenario or problem under study; it does not attempt to include or summarize the current state of human performance research. However, the Ongoing Safety Assessment Process flow chart (Figure 2) describes a series of activities, tasks, and decisions that are as applicable to human performance as they are for more commonly discussed design and quality problems. These human performance considerations should be integrated into standard in-service event analysis processes and ongoing safety assessment processes.

3.4.6 Maintenance Program Development

The initial maintenance program for an airplane type is created using the Maintenance Steering Group-3 (MSG-3) process. This process contributes to the development of the Maintenance Review Board (MRB) document and Maintenance Planning Document (MPD) created by the manufacturers, operators, and regulators.

The MRB document contains the minimum maintenance requirements for the airframe, engine, and components for a given airplane. The MRB document is established in a series of working group meetings, consisting of engineers from the manufacturer, operators, vendors, and the regulatory authorities. Maintenance requirements are analyzed to determine what task is required and at what interval it is necessary to accomplish the task to ensure that the airplane will be maintained in a safe, reliable, and airworthy condition at a reasonable cost. The MRB document includes scheduled maintenance tasks developed as part of the design process, including certification maintenance requirement (CMRs) tasks.

The MPD or the On-Aircraft Maintenance Planning Document (OAMPD), as some manufacturers call their planning document, is derived from the MRB as well as other recommended maintenance tasks that have come from service bulletins (SBs) or service information letters (SILs). The tasks that have been created from the SBs and SILs are recommended tasks, which, if incorporated into an operator's maintenance program, should be an enhancement.

3.4.7 Process to Appendix Cross Reference

This section provides a handy cross-reference to summarize the significant appendix utilization by each ongoing safety assessment process step.

STEP 1: ESTABLISH MONITOR PARAMETERS:

APPENDIX N LESSONS LEARNED

STEP 2: MONITOR FOR EVENTS:

APPENDIX H FLIGHT OPERATIONAL QUALITY ASSURANCE (FOQA)

APPENDIX L MAINTENANCE ERROR DECISION AID (MEDA)

STEP 3: ASSESS EVENTS AND RISK:

APPENDIX A SAFETY SIGNIFICANT EVENT REFERENCE LISTS

APPENDIX B QUALITATIVE RISK ASSESSMENT

APPENDIX C QUANTITATIVE RISK ASSESSMENT

APPENDIX D ROOT CAUSE (Event Tree) ANALYSIS

APPENDIX E WEIBULL ANALYSIS

APPENDIX F MONTE CARLO ANALYSIS

APPENDIX G RELIABILITY GROWTH MODELING

APPENDIX M HAZARD TRACKING

STEP 4: DEVELOP ACTION PLAN:

APPENDIX J OPERATOR SERVICE BULLETIN PROCESS

APPENDIX K MANUFACTURER SERVICE BULLETIN PROCESS

APPENDIX L AIRWORTHINESS DIRECTIVE DEVELOPMENT PROCESS

STEP 5: DISPOSITION OF ACTION PLAN:

4. IN-SERVICE DATA

This section provides a review of data sources currently available, as well as a recommended framework for collection, analysis, and sharing. Where pertinent, limitations and strengths of the various data sources are also presented in Section 6, which provides a description of each data source as well as a contact point to assist in further definition.

4.1 The Systemic View of Safety Information

Vertical and horizontal integration of safety assessment programs improves the comprehensiveness of field data, assures correct assessment of risk severity, and reduces conflict between organizations. Within an organization, vertical integration promotes a culture of safety from the chief executive officer down to lowest-level employees, while horizontal integration facilitates collaboration and coordination across functional lines (e.g., maintenance, operations, safety). In the aviation industry as a whole, vertical integration encompasses all the organizations required for the airplane to be designed, approved, and safely operated (i.e., engineering/design, manufacturing, operations and maintenance, and regulatory oversight), while horizontal integration refers to collaboration, coordination, and sharing among equivalent functional areas across organizational lines (e.g., maintenance at airline “A” with maintenance at airline “B,” regulatory decision from country “A” with those from country “B”).

4.2 Categories of Data

A thorough safety assessment function requires the collection and analysis of many different categories of data. These range from official sources of data on accidents and incidents to voluntary event/incident reporting to daily operations summaries and reliability reporting. The following sub-sections provide an overview of the basic categories and sources of data. Table 1 identifies who generally has access to the various types of data. For a list of currently available and planned airplane safety-related data sources, see Section 6

4.2.1 Accident Data

Accident investigation is a vital part of safety assessment. Accident data contains safety information that can be used to prevent future severe events. There are two basic categories of accident data: official sources and unofficial sources.

In United States, the only official source of accident data on civil accidents is the National Transportation Safety Board, charged by the Independent Safety Board Act of 1974 with the investigation and reporting of all aviation accidents. The NTSB database contains all reported fatal and non-fatal accidents involving U.S.-registered airplanes and occurring within United States and its territories. All operational categories are included. While by law, all fatal and non-fatal civil aviation accidents must be investigated and reported on by the NTSB, it is important to understand the distinction between a full-blown “Go-Team” investigation of an air carrier accident and a typical general aviation accident. The “Go-Team” accident involves many teams and sub-teams and months of investigation, often involving complete reconstruction of the aircraft. On the other hand, the typical general aviation accident is investigated by a single individual from the FAA or the NTSB, and is usually completed within 24 hours.

To support the international community, ICAO maintains an official accident and incident database containing reports from its 186 member states submitted in accordance with Annex 13. Two important distinctions compared to the NTSB are: this database only contains accident information for aircraft that have a maximum gross takeoff weight in excess of 2250 kg, and, most importantly, the quality of the submitted report varies from member state to member state.

Many countries, such as the United Kingdom, Canada, France, Germany, and others, also maintain official accident report records for occurrences within their countries.

Other sources of accident information are other government agencies (e.g., FAA, NASA), manufacturers, insurance companies, aviation safety associations (e.g., Flight Safety Foundation (FSF)) and even aviation enthusiasts within the general public. Some are listed in Section 6, but they should be used with caution, particularly if their information differs from the official accident investigation report. A notable exception is Ascend, a very large insurance carrier that maintains its own database of accident information to settle claims. There are many cases where there is no official report of the accident, yet the Ascend database contains an “unofficial” report. The Ascend reports also frequently contain updated damage information beyond what the NTSB has.

Though typically not pertinent to civilian operations, each of the US military services maintains a database of its accidents. There are common aircraft makes and models, airspace, and airports, which can frequently yield useful information.

Table 1 - Database access

Data Base	Participant		
	Operator	Manufacturer	Regulatory Authority
Accident Data	√	√	√
Ascend	√\$	√\$	√\$
Incident Investigative Agency (ex. NTSB)	√	√	√
Airworthiness Regulatory Agency (FAA, EASA, etc)	√	√	√
Operator Incident Data			
- Reportable	√	√	√
- Non-Reportable	√*		
NTSB / Regulatory Authority Safety Recommendations	√	√	√
Safety Difficulty Reports	√	√	√
Airworthiness Directives Subsystem	√	√	√
Manufacturer data		√*	
Safety Information/Incident Reporting System	√*		
Daily Operational Summary	√*	√*	V +
Operator Reliability data	√*	√*	√ +

* Own data only. + Local authority only \$ Fee for service

4.2.2 Incident Data

Unlike accident data, incident data may provide information to develop actions before a severe event occurs.

In the United States, there are two primary sources for incident data, the NTSB and FAA. The NTSB maintains a record of all mandatory reporting incidents cited in 14 CFR Part 830, which includes fire in flight, uncontained engine failure, flight control system malfunction, and others. The FAA maintains a record of the incident reports in accordance with FAA Form 8020-5. This database contains a large number of entries on bird strikes, collisions with objects, collisions with other aircraft, component failures, tail strikes, and other events.

The FAA also operates a separate incident monitoring system that contains pilot deviations, operational errors, near mid-air collisions, vehicle/pedestrian deviations, and runway incursions.

Many of the FAA safety-related information systems are collected and made available through Aviation Safety Information Analysis and Sharing (ASIAS) System, the FAA focal point for collection and analysis of safety information.

An extensive database on incidents is also maintained by NASA. It consists of voluntary reports submitted by air crews and air traffic controllers, mechanics, and other interested parties, and it is unique in that it offers FAA violation immunity to the reporter.

The United Kingdom, Australia, Canada, and many other countries also maintain incident reporting databases.

Some of the most valuable sources of incident data, however, are aviation associations and individual operators. The Air Line Pilots Association (ALPA), Aircraft Owners and Pilots Association (AOPA), Flight Safety Foundation (FSF), Allied Pilots Association (APA), and many of the larger U.S. airlines all operate internal incident reporting systems. In the hierarchy of accidents, official incidents, and unofficial incidents, these internal incident reporting systems provide the greatest opportunity for improvement of aviation safety. They represent many minor and some major incidents that could evolve into an accident based upon the circumstances. Collaboration, coordination, and sharing of this incident information may provide the framework for a substantial improvement in safety assessment.

4.2.3 Safety Recommendation Data

The NTSB and FAA operate safety recommendation systems. The NTSB recommendations system contains the formal safety recommendations made to the FAA, the FAA's response, and final adjudication. The FAA safety recommendations system is operated by the Office of Accident Investigation and contains safety recommendations submitted by FAA field personnel.

4.2.4 Other Official Data

There are several other official sources of information pertinent to airplane safety assessment. These include the Service Difficulty Reporting System (SDRS), the Master Minimum Equipment Lists (MMEL) subsystem, the Airworthiness Directives (ADs) subsystem, and the Automated Federal Aviation Regulations (AFAR) subsystem.

The SDRS contains general aviation malfunction/defect reports and air carrier mechanical reliability data. The bulk of this information is submitted by air carriers and general aviation maintenance personnel.

The MMEL subsystem contains a complete list of required equipment and conditions under which each make and model of airplane operated by air carriers may operate. The MMEL Regulations are also included.

The Airworthiness Directive subsystem contains the full text of all airworthiness directives issued for all aircraft with U.S. registry. This system includes both current and archived ADs.

The AFAR subsystem contains the full text of all United States CFRs.

4.2.5 Data from Manufacturers

Fleet-wide information is available from OEMs. This includes service difficulty information, reliability information, service bulletins, and service letters. The key data information available from the manufacturers includes the airplane/systems design and production knowledge.

4.2.6 Operator-Level Data

4.2.6.1 Safety Information/Incident Reporting Systems

As the complexity of the safety assessment function has grown, many of the larger operators have installed sophisticated information systems, which link their organization vertically and horizontally for the sharing of information. With the proliferation of these systems, the distinction between safety information and other information is disappearing. More and more operators are experiencing the benefits of an information collection and feedback process. Much information that was thought to be only safety related in the past now yields other benefits such as lower operational costs. For example, a reliability monitoring program targeted at landing gear performance is capable of predicting a failure sufficiently in advance such that preventive maintenance can avoid both an incident or accident as well as the lost revenue associated with unscheduled downtime.

Accompanying these information systems are standards, policies and procedures related to the reporting, collection, analysis, and dissemination of safety-related information. There are several key attributes of the systems and their associated policies, which determine the effectiveness of the overall safety assessment program they govern. They are:

- a. Support and empowerment from organization executives
- b. Encouragement of voluntary, non-punitive reporting policies
- c. Vertical integration from lowest-level employee to the chief executive officer
- d. Horizontal sharing of information across functional lines within the organization
- e. Positive action and follow-up when problems are detected
- f. Constant feedback from all levels of the organization, both for necessary improvements and positive reward
- g. Requirements-based data collection and analysis; i.e., avoid collecting data for the sake of collecting data, have a purpose
- h. User-friendly applications programs to increase acceptance

There are various off-the-shelf safety information systems, such as the British Airways Safety Information Service (BASIS), which an organization can purchase or lease, thereby avoiding extensive development costs. These systems come with sufficient applications software to support data entry, analysis, communications, networking, and reporting to permit an organization to begin an immediate safety assessment program. Section 6 lists some off the shelf systems/services that currently exist.

4.2.6.2 Daily Operational Summary

The Daily Operational Summary typically consists of the previous day's flight data, on-time performance, canceled flights, diverted flights, operational difficulties with ATC, airports, weather, or other factors. The report may also detail any airplane ground damage, inflight emergencies, load errors, hazardous materials incidents. A summary of the out-of-service airplane may also be provided. This summary may detail specific maintenance requirements, status of work, total number of MEL/CDL items and other information as deemed necessary.

4.2.6.3 Air Carrier Reliability Data

Many carriers operate internal reliability programs. These programs have a positive impact on both safety and operations costs. Through continual monitoring and assessment of daily operations and maintenance, reliability trends (including re-occurrences) can be developed and monitored for exceptions. When exceptions occur, very often before an incident or accident occurs, preventive action may be taken to mitigate the impact on either safety or operations costs. Establishment of an effective reliability program requires collection and analysis of a breadth and depth of information. Examples include:

- a. FOQA (see Appendix I)
- b. Aircraft Maintenance Logs (Pilot Reports, Maintenance Discrepancies)
- c. Fleet Delays and Cancellations (e.g., Air Turnbacks, Diversions, Aborts, Repeats)
- d. MEL/CDL Deferrals
- e. Operational/Service Difficulty Reports (ODRs, SDRs)
- f. Engine Monitoring Data (Inflight Shutdowns, Removals)
- g. Component Maintenance Activity (Removals, Tear-Down Reports, History)
- h. Category I/II/III Landing Data
- i. Hangar Maintenance Discrepancies
- j. Corrosion Prevention Control Program (CPCP)
- k. Structural Sampling
- l. Supplemental Structural Inspections
- m. Hydraulic Gross Flow Check
- n. Flight Recorder Data
- o. Airplane Damages
- p. Flying Time/Cycles

The systematic collection of the types of data listed above and the use of this data in ongoing safety assessment, combined with the preventive action necessary will have a positive effect on both safety and operating costs.

5. METHODS AND TOOLS

The following sections provide brief descriptions of a number of assessment and analysis methods and tools available for use in a safety risk analysis (SRA).

Additional methods and tools, such as Markov Analysis, Fault Tree Analysis, Dependence Diagramming, Failure Mode and Effect Analysis, Common Mode Analysis, Zonal Safety Analysis, and Particular Risk Safety Analysis are identified and discussed in detail in ARP4761.

As described in FAA AC39-8, Continued Airworthiness Assessments of Powerplant and APU Installations of Transport Category Airplanes, any analysis is only as accurate as the assumptions, data, and analytical techniques it uses. Therefore, the underlying assumptions, data, and analytic techniques should be identified and justified to assure that the conclusions of the analysis are valid. Variability may be inherent in elements such as failure modes, failure effects, failure rates, failure probability distribution functions, failure exposure times, failure detection methods, fault independence, human interfaces (e.g., crew actions and procedures), and limitation of analytical methods, processes, and assumptions. The justification of the assumptions made with respect to the above items should be an integral part of the analysis. Assumptions can be verified by using experience with identical or similar systems or components with due allowance made for differences of design, duty cycle, and environment. Where it is not possible to fully justify the adequacy of the analysis and where data or assumptions are critical to the acceptability of the conclusion, extra conservatism should be built into either the analysis or the action. Alternatively, any uncertainty in the data and assumptions should be evaluated to the degree necessary to demonstrate that the analysis conclusions are insensitive to that uncertainty.

It is essential to identify and document any assumptions and uncertainties related to a safety analysis in order to be able to judge their effect on the conclusions of such an analysis and to conduct sensitivity analysis.

On-going field experience should be monitored to continue validation of the assumptions and to mitigate uncertainties, or to obtain the data necessary to alleviate any consequence of the extra conservatism built into the initial analysis. The finding of any shortfalls in the assumptions calls for consideration of revision to the SRA.

Furthermore, the necessity of calibrating the SRA with the past experience helps to ensure that the future prediction is reasonable, assuming that operational parameters (derate schedules, etc.) remain constant. If the analysis does not calibrate, there will need to be further review to determine which safety analysis assumptions may be in error. The SRA will not predict reliably if it cannot calibrate to the actual experience.

5.1 Root Cause (Event Tree) Analysis

Root Cause Analysis (RCA) is a method for establishing the potential root causes of a failure in an organized and thorough manner, providing full documentation of the investigation process. RCA utilizes an event tree, which is based on qualitative fault tree analysis, but shows only the cause-effect relationships of events without the use of logic gates. Potential root causes that may be contributors to the failure can be evaluated independently or in combination. Potential root causes include design deficiencies, crew errors, maintenance technician errors, operational manual deficiencies, etc. The final event tree and the root cause disposition process provide documentation and traceability to ensure thoroughness of the failure investigation.

Failure investigation is an essential tool in the development of various systems. When a failure occurs, an investigation team is assembled to determine the cause of the failure and make recommendations for action. Priority is assigned to the investigation based on how often the failure could potentially occur and how severe its effects may be. During the investigation, it must be determined how the failure is occurring, why it is occurring, and what needs to be done to adequately reduce the frequency or severity of the failure. In the case of failures that may result in potentially catastrophic events, these answers must be generated quickly so that the action can be implemented prior to another occurrence. In the past, this often resulted in a "quick fix" approach, in which a rapid decision was made as to the cause of the failure based on the single most credible scenario. A test program would then be set up to prove that the suspected sequence of events could cause the failure, and action would be proposed and demonstrated. Unfortunately, it was not uncommon for the failure to recur even after the action was implemented because the quick fix approach did not always identify all contributing causes of the failure. Thus, the process would begin another iteration, usually with more urgency and attention than the previous investigation. An approach similar to the fault tree can be used for failure investigations, where the top event on the fault tree is the undesired event (the failure under investigation). The main advantage of the fault tree process over the quick fix approach is that all plausible causes of the failure are investigated and documented, until one *or more* root causes are identified and confirmed as the main contributors to the failure. This way, more than one root cause can be addressed with action, thereby increasing the chances that the action would completely address the failure. This approach produces a thorough analysis of the failure mechanism, and the analyst can be satisfied that the investigation has been carried out in a thorough and organized manner. A standardized process, called "Root Cause Analysis," is defined in detail in Appendix D.

5.2 Weibull Analysis

Weibull analysis provides a tool to statistically analyze service experience data for a selected component. Its primary distinguishing feature is that it quantifies reliability (or risk of failure) as a function of the age of the product. This makes it an ideal tool predicting risk due to age-related failures. Weibull analysis can help assess whether a field recall is needed, and, if so, what the appropriate recall schedule should be. Weibull may also be used to calculate survivability rates to help establish warranty programs (when to replace).

Weibull analysis has many applications. Some typical applications include:

1. Assess the product service life corresponding to a specific risk level
2. Assess the probability of reaching a pre-established life goal
3. Identify the "aging" effect for the product; i.e., identify how the failure risk per hour changes as the product accumulates service time
4. Assess the impact of extending warranty coverage
5. Assess the impact of establishing or extending a scheduled maintenance period
6. Judge the system-level reliability benefit of correcting a specific observed failure mode

Weibull analysis is described in more detail in Appendix E.

5.3 Monte Carlo Simulation Analysis

Monte Carlo simulation is a versatile method of analyzing problems that are probabilistic in nature. The analysis involves defining a mathematical model of the system being studied and operating the model repeatedly in order to observe the range of system outcomes. The model typically involves several probabilistic input parameters, where the parameter values are defined by probability distributions. The model also defines how these input parameters combine with each other and with non-probabilistic parameters to produce specific potential system outcomes.

The inputs to an aviation safety model might include the failure distributions of contributing failure modes, reliability of fault monitoring and accommodation provisions, scheduled inspections and repair intervals, effectiveness of maintenance actions, effectiveness of crew actions, expected range of flight conditions, and other relevant factors. Although the output format of a Monte Carlo simulation is usually tailored to the specific problem being studied, a typical output would be a prediction of the number of hazardous events for the next year, five years, or until fleet retirement.

For fleet problems requiring a corrective action, the Monte Carlo method can be used to help judge the acceptability of various proposed corrective actions and implementation schedules. Corrective action input might take the form of proposed changes to equipment design, revised inspection or maintenance schedules, constraints on flight conditions, or similar mitigations. Likewise, implementation schedule changes can be modeled to judge the benefit of various accelerated schedules. To judge the effectiveness of the proposed corrective action and implementation schedule, the Monte Carlo output (e.g., number of hazardous events) is compared to the original analysis.

Monte Carlo simulation is a stochastic technique, meaning that the outcome is a probabilistic function of the inputs. The simulation typically involves hundreds, thousands, or even millions of “trials” of system operation. For each trial, a specific value for each input parameter is randomly selected from the specific probability function for that parameter. The “random” selection of each input value is accomplished through a random number generator, which is included in most computer programming languages or mathematical modeling software packages.

Details of performing a Monte Carlo Analysis are presented in Appendix F.

5.4 Corrective Action Scheduling

The FAA uses quantitative risk analysis to establish the upper limit on the length of time that can be tolerated to correct an unsafe condition. Additional information on this is contained in Appendix O. Knowing the tolerable upper limit to a corrective action schedule is necessary information to ensure the corrective action schedule does not exceed allowable guidelines. However, a qualitative assessment is also needed to satisfy the principle that the risk from an unsafe condition should be mitigated as soon as it is reasonably practicable to do so, which is typically sooner than the upper limit given regularly scheduled maintenance intervals. These two considerations comprise the corrective action scheduling process; the quantitative risk analysis to determine the schedule upper limit, and the qualitative assessment to satisfy correcting the condition at the earliest reasonable opportunity. For unsafe conditions, the corrective action schedule will become mandatory through the AD process. Additional information on this is contained in Appendix L.

Not all corrective actions address an unsafe condition. Some issues might not be unsafe, but may still benefit from safety enhancement or product improvement modifications. In these cases, there is latitude in setting a recommended schedule for accomplishing the changes.

5.5 Sensitivity Analysis

Sensitivity analysis evaluates the effect of changes to the SRA input parameters on the results. Sensitivity Analysis also allows the analyst to assess the effects of variation in the major assumptions used in the analysis. Acquiring additional data on the analysis inputs will reduce the uncertainty and, therefore, reduce the range of possible results.

Some methods for providing justification of analysis assumptions are described in detail in ARP4761.

5.6 Reliability Growth Modeling

Reliability Growth Modeling is a graphical tool used to depict trends in the reliability of a product or system. Plotting various cumulative reliability parameters (e.g., cumulative events, cumulative failure rate, MTBF) versus a cumulative time function (e.g., hours, cycles) using a Crow-AMSAA or similar reliability growth model can provide insight into whether the reliability is improving or not, and by how much. Equations derived from the plots can be used to project the number and rate of future events and determine whether desired goals can be met.

Reliability Growth Modeling can be used to assess the positive results of improvements in product design, manufacture, or maintenance practices. It also can signal when mitigating action might be required due to an adverse condition or trend.

Details of performing Reliability Growth Modeling are presented in Appendix G.

5.7 Human Factors Methods and Tools

There are tools used for improvement of performance for flight and ground crews in an organization. Two of the more common tools are discussed in the following paragraphs.

5.7.1 FOQA

Flight Operational Quality Assurance (FOQA) is a voluntary program designed to improve aviation safety through the analysis of recorded digital flight data. Since 2006, commercial airlines have used this data to identify and correct deficiencies in all areas of their flight operations, thereby mitigating hazards to safety. Aggregate flight data is also analyzed and sanitized by an external entity and shared with the FAA under memoranda of understanding (MOAs). This allows the assessment of industry-wide trends and targets resources to reduce operational risks in the National Airspace System (NAS). The ultimate objective of a FOQA program is to identify lower-level safety trends in flight operations so that mitigation strategies can be implemented before a higher-level accident or incident occurs. The FOQA system is unique in that it provides insight into objective data that is not available through any other method. Further information on FOQA is available in Appendix H.

5.7.2 MEDA Tool

Maintenance and inspection errors have had serious safety consequences for the aviation industry. A review of airline data for the period of 1982 to 1993 suggests that maintenance and inspection errors are the primary cause of about 6% of the accidents and are a contributing factor in approximately 15% of the accidents. In addition, maintenance and inspection errors can have large monetary consequences to the airplane operator.

The Maintenance Error Decision Aid (MEDA) is a tool developed and distributed by Boeing without charge. It is used to assist in the resolution of maintenance error problems by providing a systematic checklist, which allows the investigator to collect sufficient information to arrive at a complete solution for a given problem. Once a series of events has been investigated, a database exists to aid the investigator on future event resolution. Further information on MEDA is available in Appendix I.

5.8 Fleet Risk Exposure Analysis

Fleet Risk Exposure Analysis is the use of probability analysis to determine the expected number of undesired events of a specific type in a given fleet based on the predicted or historical event or malfunction rate per flight and the actual or expected number of fleet operations (exposure). A graphical presentation of the results can assist in estimation of the probability of occurrence of the event under consideration, and the relative effectiveness of proposed actions, as fleet operations continue. A detailed description is contained in Appendix C.

6. BEING INVOLVED IN THE AVIATION SAFETY COMMUNITY

The sharing of safety information has become a high-profile issue in the aviation community. Sharing of safety data permits a more complete understanding of an issue than might be possible in isolation. It may not be possible to accomplish a complete evaluation without knowledge of problems that have been experienced by others operating the same airplane type. Even sharing with a select few other airlines, a common practice today, is not as effective as determining whether the whole community may have experienced similar problems. Current initiatives, such as the Global Aviation Information Network (GAIN) and the Aviation Safety Information Analysis and Sharing (ASIAS) system, have developed and implemented the means for sharing learned experiences across the industry for common good.

There are some conferences where safety is the main topic and numerous others where it is a subject of discussion. These conferences are opportunities for the safety engineer to talk with industry counterparts and establish contacts. These contacts can provide invaluable assistance in improving operations. Attending conferences is an effective way to expand one's knowledge of the latest safety advances in the participating organizations. The internet provides a convenient tool for finding lists of upcoming aviation safety-related conferences. Some safety-related conferences available at the time of publication are listed in Table 2.

Table 2 - Safety related conferences

Name	Purpose	Location	Date
Advances in Aviation Safety Conference	Conference dedicated to advancing safety knowledge in the industry.	Various USA	Spring
Annual International Air Safety Seminar	Joint meeting of the Flight Safety Foundation, International Federation of Airworthiness and International Air Transport Association held annually in selected cities of the world to ensure contact with the international aviation community.	Varies	Winter
Aviation Safety InfoShare	InfoShare is a confidential biannual conference sponsored by the FAA, in which Government and industry representatives share aviation safety concerns and discuss aviation safety issues and mitigations. Note: By participating in InfoShare, air carriers can fulfill the Title 14, Code of Federal Regulations § 13.401 requirement for disclosing FOQA data.	Various locations within the USA	Biannually
Flight Safety Foundation Annual Business Aviation Safety Seminar	Formerly the Corporate Aviation Safety Seminar, the Business Aviation Safety Summit is recognized as the premier forum for the discussion and exchange of safety information for corporate and business aviation operators.	USA	Spring
Flight Safety Foundation Annual European Aviation Safety Seminar (EASS)	Similar in format to the IASS, but focuses on safety challenges of interest to the European aviation industry.	Europe	Spring
Flight Safety Foundation Annual International Aviation Safety Summit (IASS)	The summit covers safety, training, practical solutions, management, human factors and other issues for scheduled airlines, manufacturers and equipment suppliers, trainers, flight crews, maintenance personnel and industry executives.	Various locations worldwide	Autumn

Name	Purpose	Location	Date
Global Aviation Safety and Security Conference	Annual Aviation Week conference of managers from international airlines and airports, policy makers, airworthiness authorities, equipment suppliers and researchers.	Washington, DC	Autumn
ICAO Accident Prevention and Safety Seminar	Conference of Govt. and private sector aviation officials.	Varies	Spring
ICAO Seminar on Accident Investigation, Prevention, and Human Factors		South America	Summer
International Society of Accident Safety Investigators (ISASI) Seminar	"Pushing the Envelope Towards Improvement."	Europe	Autumn
"Policies, economics, and Technology R&D for Aviation Safety"	Conference sponsored by the American Institute of Aeronautics and Astronautics.	Washington, DC	Spring
SMS Industry Forum	The SMS Industry Forum is a collaborative effort of industry lessons learned while creating SMS for their respective organizations and includes best practices.	Various USA	Spring
The Americas Conference on Aviation	Conference of U.S. Govt., industry, and aviation leadership from Latin America and the Caribbean. Conference themes are aviation safety, systems integration and training.	USA	Autumn
World Aviation Congress	Large gathering of aviation personalities and managers. Usually a session on aircraft safety.	Various USA	Autumn

Many websites have been established for the dissemination of safety information. Some of these are ready references for general safety data, and some provide detailed data on accidents and incidents. Website addresses change frequently; however, some of the websites available at the time of publication are listed in Table 3. Internet search results will yield many resources that discuss aviation safety-related topics. Search for "aviation safety," "aviation safety statistics," "aircraft accidents and incidents," or similar terms for updated information.

Table 3 below provides a list of commonly accessed websites for obtaining aviation-related safety data, and includes the website name, website address, and a brief explanation of the website's purpose and contents. Information in this table may be used in conjunction with Table 2, which provides a description of data sources, as well as a contact point to assist in further definition.

Table 3 - Safety related websites

Name	Address	Purpose
Aerospace Industry of America (AIA)	http://www.aia-aerospace.org/	Contains manufacturer related safety information.
Airlines for America (A4A)	http://airlines.org/	Provides publication list which can be ordered, good airline information handbook, links to airlines, government agencies.
Australian Transport Safety Board (ATSB) Aviation	http://www.atsb.gov.au/aviation/	ATSB Aviation Safety webpage.
Aviation Safety Information System of CAAC	http://safety.caac.gov.cn/	System Contains Aviation Safety Dynamic, International Aircraft Accident, International Safety information, Aviation safety audit information, etc.
Aviation Safety Network	https://aviation-safety.net	A service of Flight Safety Foundation, includes aviation safety database, accident investigation reports and accident statistics.
Civil Aviation Administration of China (CAAC)	http://www.caac.gov.cn/	CAAC Official website that contains CAAC regulations, Advisory Circulars, Aviation Procedures, etc.
CAAC Airworthiness Directive System	http://new.caacaa.org.cn/	System contains CAAC Airworthiness Directives, Biweekly report of CAAC Airworthiness Directives, etc.
Civil Aerospace Medical Institute (CAMI)	https://www.faa.gov/about/office_org/headquarters_offices/av/office_of_medical_operations/aam/cami/	FAA's Civil Aerospace Medical Institute site with links to information on Medical Bulletins, Industry testing programs, Medical certification, Pilots information and more.
European Aviation Safety Agency	https://www.easa.europa.eu/	EASA's main site containing agency information, links to EASA regulations, Agency rules, and a document library.
FAA Accident & Incident Data	https://www.faa.gov/data_research/accident_incident/	Full listing of accidents involving major airlines from 1920 to present, reports of recent accidents, sound files of CVR transcripts.
FAA Aviation Safety Information Analysis and Sharing (ASIAS) System	http://www.asias.faa.gov/	Integrated queries across multiple aviation safety databases; lessons learned from aviation accidents.
FAA Regulatory and Guidance Library	www.faa.gov	A variety of aviation safety information including 14CFR Parts 5, 21, 23, 25, 27, 29, 31, 33, 34, 35, 36, NPRMs, ACs, AD NPRMs and Final Rules, TCDS, Policy, Issue Papers, Special Conditions, Exemptions, Orders, TSOs, STCs, PMAs TARAM Handbook.

Name	Address	Purpose
FAA Engine & Propeller Directorate Technical Reports	https://www.faa.gov/aircraft/air_cert/design_approvals/engine_prop/engine_sp_topics/	Provides links to various technical reports containing propulsion system data, including the various CAAM Reports summarizing rates and outcomes of various engine, propeller and APU occurrences.
Flight Safety Foundation	http://www.flightsafety.org	Contains links to a number of aviation safety resources relevant to all aspects of aviation.
Global Aviation Safety Network	http://flightsafety.org/archives-and-resources/global-aviation-safety-network-gain	Information on GAIN Action Plan, Working Groups, Government Support Team and GAIN Conferences.
International Civil Aviation Organization (ICAO)	http://www.icao.int	About ICAO.
NASA Aviation Safety Reporting System	http://asrs.arc.nasa.gov/	Contains a description of ASRS program, recent ASRS publications, general reporting form as well as special forms for air traffic controllers, mechanics, and cabin crew.
National Transportation Safety Board (NTSB)	http://www.nts.gov	NTSB recommendations, publications, news, & events.
NTSB Aviation Accident Database	http://www.nts.gov/layouts/nts.aviation/index.aspx	Contains over 37000 accident and incidents descriptions involving U.S. aircraft or non-U.S. aircraft in U.S. jurisdiction and which occurred from 1983 to present.
SAE International - Aerospace	http://www.sae.org/aerospace	SAE Aerospace site with links to articles, events, publications and training related to the aerospace industry.
SAE International - Standards	http://www.sae.org/standards/	SAE S-18 standards development activities.
SKYbrary	http://www.skybrary.aero	SKYbrary is a wiki created and maintained by the European Organization for the Safety of Air Navigation, International Civil Aviation Organization, and the Flight Safety Foundation to provide a comprehensive source of aviation safety information.
The Royal Aeronautical Society	http://aerosociety.com/	Dedicated to global aerospace community, the Royal Aeronautical Society, also known as the RAeS, is a British multidisciplinary professional institution dedicated to the global aerospace community. It is the oldest aeronautical society in the world.
Transport Canada	www.tc.gc.ca	Include the Canadian Aviation Regulation Advisory Council (CARAC) and CARs regulatory information.
Transportation Safety Board (Canada)	http://bst-tsb.gc.ca	Transportation Safety Board (Canada) recommendations, publications, news, & events.
United Kingdom	https://www.gov.uk/government/organisations/air-accidents-investigation-branch	UK aviation accident investigation recommendations, publications, news, & events.

7. NOTES

7.1 Revision Indicator

A change bar (|) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY S-18C ARP5150A AND ARP5151A WORKING GROUP

APPENDIX A - SAFETY SIGNIFICANT EVENT REFERENCE LIST

NOTE: The basic ARP5150 document contains information which places the information in this appendix in context. This appendix should be used in conjunction with the body of the document.

A.1 SCOPE

The objective of this appendix is to provide sample lists of safety significant parameters for aircraft for which may be used for monitoring purposes or to enhance present and future aircraft designs.

These samples are intended to be example lists and not inclusive or prescriptive checklists since they may not include all the information necessary for appropriate failure conditions of an aircraft with its various functions and its intended use. It should be emphasized again that these sample lists of significant failure conditions examples should not be applied indiscriminately to a particular aircraft type and configuration.

This appendix has four sample lists - two from the view point of aircraft manufacturers, one from the perspective of an airline, and finally a cross reference list between one of the aircraft manufacturer lists and the airline list:

Table A1 - Aircraft Manufacturers Significant Failures List

Table A2 - Aircraft Manufacturers Failure Condition by System List

Table A3 - Airline Classification List

Table A4 - Significant Failure Conditions to Airline Significant Event Cross-Reference

To facilitate comparisons of design expectations and operational performance, it may be beneficial to monitor "lower level" parameters. In some cases, the objective may be to support compliance with the significant failure condition expectations.

A.2 AIRCRAFT MANUFACTURERS SIGNIFICANT FAILURES/ITEMS LIST BY FUNCTION EXAMPLE

Table A1 - Aircraft manufacturers significant failures list example

Function	ATA	Significant Failure/Item
Avionics	24	Any flight anomalies cause by Portable Electrical Devices (PED)
Avionics	23	Loss of Comm.
Avionics	31	Loss of Displays/Control Display Anomalies
Avionics	34	Loss of Nav. or Navigation Anomalies - FMF or sensor failures
Avionics	31/34	CDU Anomalies
Avionics	39	Configuration Problems (Incompatible HW/HW, SW/ HW) in a system
Avionics	31/50	Failure to warn/False Warnings (T/O Config, Land Config, GPWS, etc.)
Avionics	34	ARINC 629 Bus Failures
Avionics	02	Lightning Strike events
Avionics	22	Uncommanded Autothrottle Input
Avionics	34/10	Loss or Misleading Data from ADIRS or ADIRU
Doors	52	Cargo/Pax door EICAS messages
Doors	52	PED Flight Lock Failures
Doors	52	PED locked on ground
Doors	52	Passenger and Cargo door not fully closed, Latched and locked for T/O or LND
Doors	52	Pass. and Cargo door T/O Configuration Warning
ECS	36	Avionics equipment overheat
ECS	36	Cabin altitude warning/excessive cabin altitude/Loss of pressure control
ECS	36	Cargo fire extinguisher discharge
ECS	36	Cargo Fire Warnings

Function	ATA	Significant Failure/Item
ECS	36	Dual air condition pack loss
ECS	36	Duct burst events
ECS	36	Duct overheat events
ECS	36	Loss of auto cabin pressure control
ECS	36	Loss of equipment cooling - with no warning
ECS	36	Uncontrollable/excessive cabin temp
ECS	36	Use of equipment cooling override mode
Electrical	24	Degrading of wire shielding (Lightning and HIRF protection)
Electrical	24	Electrical smoke or fires
Electrical	24/27	Flight Control direct current (FCDC) system anomalies
Electrical	24	Loss of any IDG during turbulence, zero or negative Gs
Electrical	24	Main Battery Failures
Electrical	24	Power up problems in flight /Load shedding
Electrical	24/29	Failure of RAT Deployment/Inadvertent RAT Deployment
Electrical	24	Wire bundle chaffing (All Areas)
Flight Cont.	27	ACE logic for mode switching (Blocking/Bypass) (PFC Selection) (Direct)
Flight Cont.	27	Controllability with any Hydraulic and/or Electrical power losses
Flight Cont.	27	Control available versus. control required
Flight Cont.	27	Direct mode operations (Time and numbers of events)
Flight Cont.	27	Failure rates of the individual and or multiple PFC events
Flight Cont.	27	In direct mode any problems with dutch rolls or rudder structure damage
Flight Cont.	27	Loss or limited rudder control
Flight Cont.	27	Jams or restrictions of flight controls surfaces and controls
Flight Cont.	27	Secondary Mode Operation (Time and number of events)
Flight Cont.	22	Uncommanded AFDS input to the PFCS
Flight Cont.	27	Uncommanded surface movement
Flight Cont.	27	Use of PFC Disconnect switch (Time and number of events)
Flight Deck	3910	Confusion with Controls/Displays/Switches
Flight Deck	31/33	Lighting Failures
Flight Deck	52	No. 2 Window opening events on Takeoff which causes unnecessary RTOs
Flight Deck	25	Uncommanded crew seat movement
Flight Deck	02	Unplanned RTO - Reason for/ Speed
Mech System	32	Tire Burst/Failure Events: During T/O / LND / Taxi
Mech System	32	Brake Failure Events
Mech System	32	Main Gear Steering Events
Mech System	32	Nose Gear Steering Events
Mech System	32	Tire Burst/Failure Events: In Wheel Well During Flight
High Lift	27	Failure of load relief
High Lift	27	Flap/Slat Asymmetry Events In flight
High Lift	27	Flap/Slat Shutdown during cruise resulting in landing without flaps/Slats
Hydraulic	29	Anomalous low quantity indications on center hydraulic reservoir CHIS
Hydraulic	29	Chaffing of any hydraulic tubes near any ECS ducts - Mist in cabin
Hydraulic	29	Hydraulic System Loss (Single or Multiple)
Landing Gear	31	Inadvertent/Uncommanded gear extension
Landing Gear	31	Main gear tilt sequence anomalies
Landing Gear	31	Unsafe gear indication (Not down/Locked)
Landing Gear	31	Wheel well fire warning events - In flight or on ground
Payloads	38	Clear ice events
Payloads	52	Evacuation Conducted - Slide operation, etc.
Payloads	38	Lavatory flooding events - Flooding results with

Function	ATA	Significant Failure/Item
Payloads	35	Oxygen Events - Deployment failures, Loss of systems, O2 fires, etc.
Payloads	02	Personnel Injury Events - Cabin Interior Furnishings
Payloads	38	Potable water leaks
Propulsion	4910	APU Uncontained Failures
Propulsion	54	Burst duct events (Engine & Strut areas)
Propulsion	5430	Cowl hold open Rods failures
Propulsion	5440	Cowl Fairing separation events
Propulsion	72	Cross Engine Debris
Propulsion	72	Engine Compressor Stall: Engine Start in Tail Winds/Cross Winds
Propulsion	72/26	Engine Fires
Propulsion	7210	Engine Flame-outs/Roll-Backs/Sub-Idle (EFA Performance)
Propulsion	77	Engine indication anomalies
Propulsion	80	Engine Inflight Starts during revenue service
Propulsion	02	Engine personnel ingestion events
Propulsion	7120	Engine/Strut Mount problems
Propulsion	2840	FQIS Reliability versus. FMC Indications
Propulsion	2820	Firewall Shut-off Valve failures
Propulsion	2820	Fuel Crossfeed Valve failures
Propulsion	2810	Fuel Leaks
Propulsion	72	Engine Icing resulting in damage
Propulsion	2830	Inadvertent Fuel Jettison/Failure to jettison on command
Propulsion	7830	Loss of Thrust Reverser/Indications/Malfunctions
Propulsion	7170	Nacelle/Strut Drain blockage
Propulsion	2610	Overheat/Fire Detector failures
Propulsion	72	Uncontained Engine Failure
Propulsion	28	Unplanned Fuel Balance
Structure	51	Fuselage Panel Buckling to determine the no-tear-strip design
Structure	51	Loss of any aircraft panels; Subsequent damage to empennage

A.3 AIRCRAFT MANUFACTURERS CLASSIFICATION LIST BY SYSTEM'S CLASSIFICATION EXAMPLE

The objective of the following table is to describe a sample list of significant Failure Conditions from the perspective of an aircraft manufacturer. The failure condition severity has been classified based on service experiences of aircraft and/or traditional assumptions. Its sole purpose may be to assist users to derive the severity level of the event under consideration by first identifying the "Failure Condition" and its severity, which could be initiated by the event.

This table addresses general applicability, it is intended to be an example list and not an inclusive or prescriptive checklist, and it should not be utilized to replace any specific guideline intended for a particular aircraft type and configuration. It may not include all the information necessary for appropriate Failure Conditions of an aircraft with its various functions and its intended use. It should be emphasized again that this generic list of significant Failure Conditions example should not be applied indiscriminately to a particular aircraft type and configuration.

The classification of the consequences and the definitions below, have been paraphrased from advisory material:

1. **Catastrophic:** Failure Conditions which would result in multiple fatalities, usually with the loss of the aircraft, or would prevent continued safe flight and landing.

2. Hazardous: Failure Conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be:
 - a. A large reduction in safety margins or functional capabilities;
 - b. Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or
 - c. Serious or fatal injury to a relatively small number of the occupants other than the flight crew.
3. Major: Failure Conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.
4. Minor: Failure Conditions which would not significantly reduce aircraft safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.
5. No Safety Effect: Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the aircraft or increase crew workload.

Table A2 - Aircraft manufacturers failure condition by system list example

Systems				
	Classification of Failure Condition			Comment
Function	Total Loss of Function with warning	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of attitude information to control roll and pitch	Catastrophic	Catastrophic, if includes both PFDs. Major, if includes one pilot's PDF.	Catastrophic	
Display of heading	Catastrophic Major if Navigation systems operational	Major	Catastrophic Major if Navigation systems operational.	
Display of altitude information	Hazardous	Minor	Catastrophic	
Display of airspeed information	Hazardous, during landing; otherwise, major	Minor	Hazardous	
Display of rate of turn	Minor	Minor	Minor	
Display of slip-skid	Minor		Minor	
Display of time	Minor		Major	
Display of navigation information	Major Total loss of navigation and communication is Catastrophic	Major	Major. Catastrophic for precision approaches.	
Communication	Major.	Minor	Major, if data link is primary.	
Visibility during landing	Hazardous			
Misinterpretation of flying altitude	Hazardous		Catastrophic	Occur during landing and poor visibility.
Display of radio altitude	Minor		Minor	Category I IFR.
Display of vertical speed	Major		Major	Category I IFR.
Display of flight guidance commands (Category I operation)	Minor		Minor	Category I ILS. For Category II ILS, an autopilot or flight director is required.
Autopilot failure	Minor, with warning. Major, without warning. Hazardous, if without warning during autoland.		Major, single axis and limited authority. Hazardous, multi-axis and limited authority. Catastrophic, if authority is unlimited.	Maximum inputs (hardovers) or (slowovers) to aircraft primary control surfaces should not exceed aircraft structural limits.

Systems				
	Classification of Failure Condition			Comment
Function	Total Loss of Function with warning	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Flight controls for pitch axis	Catastrophic	Major	Catastrophic	
Flight controls for roll axis	Hazardous, if yaw axis is still available	Major	Catastrophic	
Flight controls for yaw axis	Minor to Major, Hazardous to Catastrophic if combined with engine failure or severe cross wind	Minor	Catastrophic	
All hydraulics	Catastrophic			
Manual control flight controls	Catastrophic			
Artificial feel	Variable severity.			Variable severity needs to be evaluated on a case-by-case basis.
Takeoff director and automatic landing system	Catastrophic		Catastrophic, if malfunction of autoland below alert height. Hazardous, if takeoff director provides only lateral guidance.	
Stability augmentation	Variable severity	Minor	Variable severity	Variable severity needs to be evaluated on a case-by-case basis.
Stick pusher failure	Hazardous, if stall regime encountered. Otherwise, Minor.	Minor	Hazardous/ Catastrophic near ground	
Stick shakers/stall warning	Minor	Minor	Major	Assumes that a warning system is in place to notify pilot that loss of system function has occurred (for example, stick force changes, buffeting, inherent aerodynamics features, etc.).

Systems				
	Classification of Failure Condition			Comment
Function	Total Loss of Function with warning	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Trim control	Minor	Minor	Major, if manual trim. Catastrophic or Hazardous for electrical.	Major, for trim runaways if there is a trim-in-motion aural alert. Hazardous or Catastrophic, for trim runaways without a failure indication depending on trim authority.
Display of trim indications	Minor	Minor	Variable severity	Variable severity to be reviewed on a case-by-case basis.
Landing gear control	Hazardous	Minor	Major to Hazardous	
Display of landing gear indications	Major		Hazardous	
Brake control	Catastrophic, if unannunciated loss of braking. Major, if annunciated loss of braking.	Hazardous	Hazardous	Electronic anti-skid and brake systems can cause significant ground handling problems if they malfunction under adverse conditions due to asymmetrical loading.
Visual warnings, cautions, and alerts	Major, for worst case			Failure Conditions depend on the criticality of systems being monitored and pilot action required.
Display of air temperature	Minor		Minor	
Overspeed warning	Minor	Minor	Minor	Airspeed may be used as a backup to the overspeed warning for continued safe flight and landing.