1. PURPOSE

1.1. This procedure defines and describes the processes, roles and responsibilities, and the managing and procedural tools required to achieve the required level of operational safety for industry products under CAAI supervision, as required by ICAO and by international bilateral agreements.

1.2. It also gives an overview of the process of risk management that is one of the foundations of the continued operations safety doctrine.

2. BACKGROUND

2.1. As part of its duties and international obligations to insure an acceptable level of Safety for Civil Aviation, the CAAI is required to define the processes and requirements that will provide operational safety for aeronautical products for which Israel is the state of design.

2.2. This is achieved by actively and continuously monitoring the industry and its products, identifying the failures or problems which have a potential impact on safety, ensuring the flow of information required to correct the problem, and monitoring the effectiveness of corrective actions promulgated through Airworthiness Directives issued by the CAAI under article 69(a) of the Air Navigation Law, 2011, CAAI or industry-issued notices, special bulletins, or other means.

2.3. In addition, it is the CAAIs responsibility to ensure that the industry (design and manufacturing organizations) implements the necessary procedures and tools required to continuously monitor its fleet and take the appropriate action to rectify these problems.

2.4. These activities will require CAAI to manage safety by a more process-oriented system safety approach that will be based not only on the promulgation and application of technical standards,

but also on an increased emphasis on the management systems that ensure risk management and safety assurance.

3. REFERENCES

3.1. Article 69(a) of the Air Navigation Law, 2011,

3.2. Regulations 64-66 of the Air Navigation Regulations (Documentation of Aircraft and Aircraft Parts), 1977

3.3. FAA order 8040.1C – Airworthiness Directives

3.4. FAA order 8040.4A - Safety Risk Management

3.5. FAA order 8040.5 – Airworthiness Directive Process for Mandatory Continuing Airworthiness Information

3.6. FAA order 8110.49 - SOFTWARE APPROVAL GUIDELINES

3.7. FAA System Safety Handbook, Chapter 3: Principles of System Safety

3.8. Fault Tree Handbook with Aerospace Applications, NASA, version 1.1, Aug 2002

3.9. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

3.10. RAMS Standards and Guidelines

4. Method

The Continued Operational Safety of the CAAI certified products will be based on the following principles:

4.1. CAAI management involvement and commitment to implementation of the COS principles.

4.2. Early identification of potentially catastrophic or hazardous safety issues.

4.3. Evaluation of the COS systems of TC holders.

4.4. CAAI Staff and applicants COS training.

4.5. Encouragement of voluntary failure reporting.

4.6. Use of data driven and quantitative risk analysis and assessments, for evaluating the Criticality of an event/issue.

4.7. Follow up of corrective action implementation for critical safety issues.

4.8. Periodic audit of the COS system of the TC or STC holders.

4.9. Enforcement of Regulations 64-66 of the ANR (Procedures for Documentation of Aircraft and Aircraft Parts) concerning the reports of failures or events with a safety impact.

4.10. Participation of CAAI COS manager and team in the TC/STC holder's operational safety boards, as required.

5. Organizational Responsibilities

5.1. Description

The implementation of the Continued Operations Safety concept in the CAAI Engineering Branch of CAAI is based on a two level organization:

5.1.1. The COS board, mandated to define the criticality of events or operational issues and determine the optimal way to reduce the risk and imply a corrective action, when required.

5.1.2. The COS Manager, in charge of coordinating activities for the monitoring and surveillance of the Industry.

5.2. COS Board Tasks:

5.2.1. Assists the COS manager in evaluating the criticality of events or hazards related to a specific safety issue of an Israeli certified product.

5.2.2. Reviews the applicants safety assessment of the COS issue.

5.2.3. Performs the CAAI operational safety and risk analysis of the events or safety issue and of the potential mitigating options.

5.2.4. Recommends to the COS manager - the corrective action to be performed, and the controls and parameters that

should be defined in order to effectively implement the corrective action.

5.2.5. Recommends ways or policies required to monitor the corrective action and the related safety improvement achieved through it.

5.2.6. Supports the COS Manager with definition and implementation of the processes and procedures required for monitoring the Continued Operational Safety at CAAI.

5.2.7. Supports the CAAI audits of the manufacturer's COS System, as performed by the COS manager.

5.2.8. The COS board shall include:

5.2.8.1 The product certification project manager;

5.2.8.2 The COS manager;

5.2.8.3 The CAAI flight test pilot, as required;

5.2.8.4 engineers of the engineering branch, as required;

5.2.8.5 Engineering specialists or the manufacturer, as required.

5.3. COS Manager Tasks

5.3.1. Serves as the Continued Operational Safety (COS) focal point in the airworthiness Dept. at CAAI.

5.3.2. Serves as an agency expert in Continued Operational Safety issues and is responsible for detailed follow-up with the CAAI aircraft certification manager or with foreign

aviation authorities (FCAA) for each reported accident and incident.

5.3.3. Organizes, implements and monitors the Continued Operational Safety program at CAAI.

5.3.4. Identifies process improvements to the CAAI Continued Operational Safety program and implement corrective actions.

5.3.5. Identifies trends in the Continued Operational Safety arena and formulates strategies to address the issues:

5.3.5.1 By guiding the industry in performing risk assessments, developing corrective actions and root cause analysis for the identified hazards.

5.3.5.2 By monitoring the implementation and effectiveness of the corrective actions.

5.3.6. Provides CAAI staff assistance and serves as an advisor to the CAAI Director General and to the CAAI Safety Management Group, on all matters pertaining to air vehicle systems (manned or unmanned) Continued Operational Safety issues, including corrective actions.

5.3.7. As required, coordinates CAAI staff assistance to the CAAI Managers on special problems or projects of a nature directly or indirectly related to the Continued Operational Safety activities of CAAI.

5.3.8. Checks and monitors the applicants Continued Operational Safety plan, including participation in applicants operational safety boards (OPSB), when required.

5.3.9. Identifies and participates in research and development studies to ascertain the need for new safety standards or

to implement new technologies to improve Continued Operational Safety.

5.3.10. Presides as the chairman of the CAAI COS board.

5.3.11. Based on the COS Board and on the manufacturer OPSB recommendations, decides the nature of the change and controls through which corrective action will be implemented how (Airworthiness Directives, notice, etc).

5.3.12. Defines and coordinates the COS training requirements of CAAI staff.

5.3.13. Specifies the requirements and monitors the development of computerized COS tools.

5.3.14. Serves as a focal point to the industry on all COS related issues.

5.3.15. Performs a quality evaluation of COS Systems implemented at manufacturers.

5.3.16. Reports to the CAAI Engineering Branch manager.

6. COS Procedure

6.1. The COS procedure to be followed by CAAI Staff when a Continued Operational Safety event or issue has been identified is summarized in Appendix 1.

7. Task Outcomes

7.1. The COS procedure will be followed by the documentation described in Appendix 5.

APPENDIX 1 - COS Procedure

1. Overview:

1.1. Continued Operational Safety or "COS" describes a set of Monitoring Tools, Risk Management Tools, and Corrective actions & activities associated with them. The purpose of these is to ensure that the product confirms to design and is in a condition for safe operation and maintain an acceptable level of safety.

1.2. Continued Operational Safety or "COS" derives its authorization from section 69 of the Air Navigation Law, 2011, directing TC holders to create and maintain a Formalized, Disciplined and Documented procedure to Identify, Evaluate and Control Safety Risks.

1.3. In order to standardize risk assessment methodology across products, the FAA's Aircraft Certification Service established a process called "Monitor Safety/Analyze Data," or MSAD1. The associated MSAD order (8110.107) requires each aircraft certification directorate to develop product–specific, quantitative risk analysis methodology and guidelines for determining risk, in terms of the statistical probability of a fatal accident.

1.4. The current procedure (CAAI – Continued Operational Safety Procedure) is based on MSAD order 8110.107, with adoptions to the Israeli ANR (Air Navigation Regulations).

[1] Link to MASAD 8110.107 Order

2. Objectives:

2.1. Define Continued Operational Safety and key activities related to it.

2.2. Identify the characteristics of the Safety Risk Management and Safety Assessment System.

2.3. Identify the expected procedures and outcome from the TC Holder.

2.4. **Describe a Theoretical method to evaluate the Safety Assessment.**

3. Continued Operational Safety – General description:

3.1. Continued Operational Safety is a closed-loop, technical process activated to ensure safety throughout the aircraft / fleet lifecycle.

3.2. COS is initiated by receiving abnormal in-service data, analyzing the potential safety issue by using Risk Assessment Tools and Methods, to determine if a corrective action is needed, and if so, to determine the action required and time line.

3.3. After completion, all event data, safety issues, risk analysis, Conclusion and corrective action data is stored for documentation and future use.

4. Applicability:

4.1. CAAI – COS Procedure is applicable to all Israeli registered TCs, STCs, PCs etc., and the above certification holders.

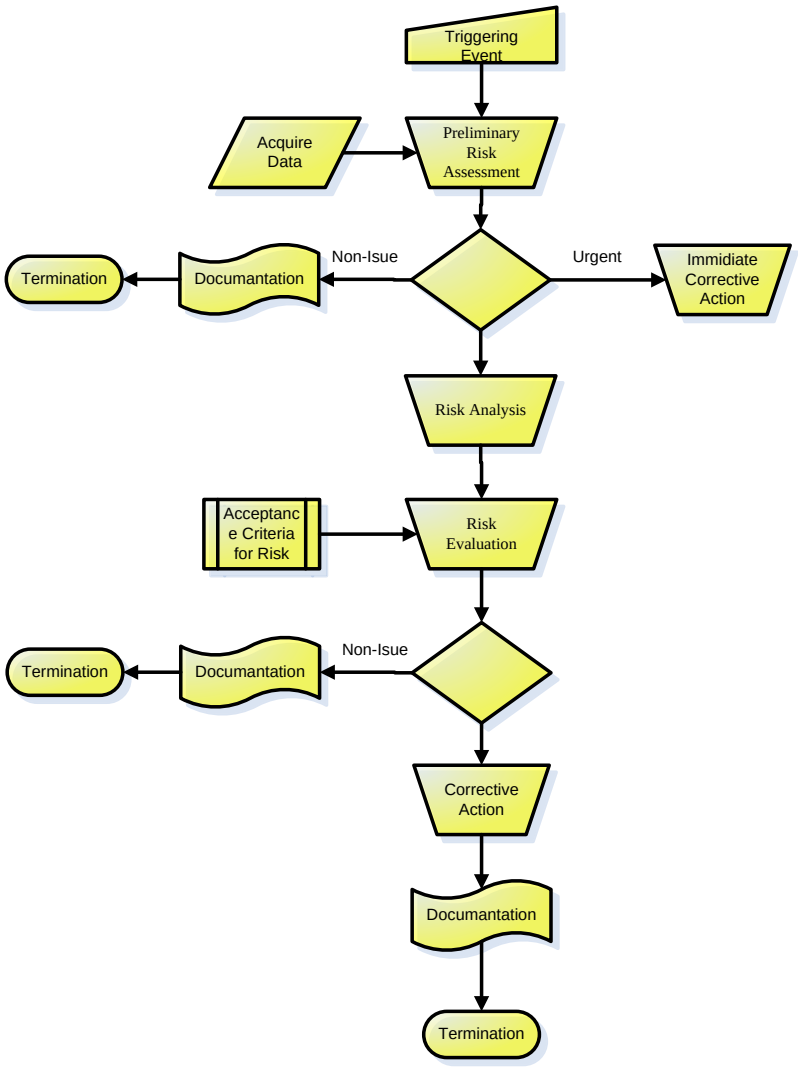
4.2. CAAI COS responsibility is terminated only after final cancellation of an Israeli TC, including notification of national authorities who have notified CAAI that they have Israeli TC'd products on their

registry and transfer of relevant information to those authorities that intend to allow further operation of those products.

Suspension of a TC (for a defined or undefined time) does not terminate COS responsibilities, and these should be continued during the period of suspension.

5. COS – High-Level View

5.1. COS Procedure flow chart:



5.2. Triggering Event/Data:

5.2.1. A COS event or issue may be identified by one of the following:

5.2.1.1 A notice from an operator or TC/STC holder that a safety event has occurred on one of its products, during service.

5.2.1.2 The result of statistical analysis of Israeli products based on the CAAI COS database.

5.2.1.3 A research of other safety management systems. (Such as a result of a periodic check of Safety Events relevant to Israeli products).

5.2.1.4 A notice from a foreign certification authority.

5.2.2. The identified COS event will be directed to the project certification manager and to the COS manager.

5.3. Preliminary Risk assessment of safety issues

5.3.1. Based on the data available at the time, the project manager will perform a hazard assessment of the severity of the finding/event.

5.3.2. The assessment will be considered as a "Safety Issue" (equivalent to "hazardous" or above) as long as not proven otherwise.

5.3.3. Depending on the nature of the data available, the assessment will be qualitative or quantitative. Preference should be given to a quantitative assessment of the severity of the event. The assessment should be performed in coordination with the relevant CAAI specialists. Based on the result of the assessment and on the anticipated impact on the fleet, the project manager will decide if the course of action may be defined and performed at his level through consultation with the COS manager, or if the event and proposed corrective action should be presented to the COS Board for further evaluation. If the first assessment of severity level of the

event indicates a "hazardous" or "catastrophic" level, the event and proposed corrective action must be presented to the COS board.

5.4. Acquired data:

5.4.1. Aviation databases, data collected from automated systems (like FRACAS), official data, operator data, certification holder data, literature, etc'

5.5. Hazard Criteria Analysis and Preliminary Risk Analysis:

5.5.1. These analysis are aimed at answering the following two questions :

5.5.1.1 **Is this a potential safety issue?**

5.5.1.2 **Does an urgent unsafe condition exist?**

5.5.2. If the preliminary assessment of the risk identifies an urgent unsafe condition that requires immediate corrective action, an initiation of emergency AD of FRC is required, even if this causes some delay to the risk and causal analysis.

5.5.3. If the preliminary assessment of the risk determines that no further action is required, the determination must be documented.

5.6. Risk Analysis:

5.6.1. Risk analysis involves the identification of undesired events, and the causes and consequences of these events, and the use of this information to determine how

often specified events may occur and the magnitude of their consequences.

5.6.2. risk analysis must objectively calculate risk as a parameter of probability and severity, as derived from the identified hazard and it's probability.

5.6.3. Risk Calculation :

5.6.3.1 The risk value must be calculate for :

5.6.3.1.1. The Total uncorrected fleet risk, and

5.6.3.1.2. The individual Uncorrected risk.

5.6.3.2 And, As mentioned above, the risk outcome must be presented in two orthogonal dimensions :

5.6.3.2.1. Severity;

5.6.3.2.2. Probability.

5.6.4. Risk Value:

5.6.4.1 Multiplication of the orthogonal parameters (severity and probability) yields the dimensionless comparable risk value.

5.6.5. Risk Evaluation:

5.6.5.1 A comparison of the risk analysis results to predetermined standards or "acceptance criteria for risk" and other decision criteria, gives a non-biased tool to determine whether corrective action is needed.

5.6.6. Corrective Action

5.6.6.1 Identification of undesired events and the consequences of these events, as a part of the Risk Analysis Process, enables identifying the key elements whose correction will prevent the Safety Event from occurring.

5.6.6.2 Existence of several "key elements", enables us to compare and select the most suitable one, in terms of "costs", "time", "needs" and so on.

5.6.6.3 Risk Assessment also enables determination of complince time for corrective action, as well as to

prioritize it by flight hours, Scheduled maintenance, a/c age etc.'.

6. Risk Analysis

6.1. Although Risk assessment can be done in many different methods, in order to maintain consistency, the methods used for the COS process by CAAI is the "Fault Tree Analysis" or "FTA". An extensive description of the FTA method is given in Appendix 2.

6.2. A useful bonus of the FTA method is its ease of transformation into its logical complement: a Success Tree (ST) that shows the specific ways the undesired event can be prevented. The ST provides conditions that, if assured, guarantee that the undesired event will not occur.

6.3. Failure events in aviation can, most of the time, be divided into three groups, which require different statistical approaches[2] :

6.3.1. Faulty manufacturing / installation

6.3.2. Time-depended faults (Burn-In / Wear-Out).

6.3.3. Random failures.

6.4. Two more sets of faults[3], usually contributing events, are human errors and software errors. Both share the impossibility of likelihood estimation.

6.4.1. Human Error :

6.4.1.1 Human performance plays a central role in overall safety. Human interaction with equipment occurs

[2] Of course mathematically they can all be presented by the same "Weibull distribution" equations: while assigning the shape parameter as equal to = 0, the Weibull becomes equivalent to the exponential distribution (used for "random failure distribution") and as the shape parameter increases > 0, a wear-out behavior is modeled. And when the shape parameter decreases to -1<<0 the burn-in behavior is modeled.

[3] The events are termed “faults” if they are initiated by other events and are termed “failures” if they are the basic initiating events

during operation, response to events, surveillance testing, and maintenance.

6.4.1.2 Human-machine interactions can mitigate the effects of accidents through recovery and control actions. On the other hand, Human interactions may also cause initiating events through error.

6.4.1.3 Humans are more perceptive and flexible in performance than machines; hence, during adverse situations, crew members are expected to be able to deal with complex situations and system interactions. However, during this response action errors may be committed that not only do not correct the situation but actually exacerbate it.

6.4.1.4 Types of Human Error

6.4.1.4.1. Test and maintenance related errors

6.4.1.4.2. Errors causing initiating events

6.4.1.4.3. Procedural errors during an incident or accident

6.4.1.4.4. Errors leading to inappropriate actions

6.4.1.4.5. Detection and Recovery errors

6.4.1.5 Research shows that practicing and training improve the human ability to reduce error rate up to a certain point, from which the error rate starts to rise again4.

6.4.1.6 It is commonly practiced to calculate **human Error for trained personnel** as 10^-4. For more "rare" events, which the personal does not practice on a regular basis, it is legitimate to calculate **Human Error Probability** as 10^-3.

6.4.2. Software Failure :

6.4.2.1 Software is generally application-specific and reliability parameters associated with it cannot be estimated in the same manner as hardware. therefore, determining the probability of failure of a single software function is difficult at best and cannot be based on historical data.

6.4.2.2 COS does not relate to with software reliability, most specially critical software. Faults found in such

[4] THE PROBABILITY AND MANAGEMENT OF HUMAN ERROR

software require an immediate focal investigation and focused attention.

6.4.2.3 If ever required, the probability of software failure used for risk assessment calculations is always "1", so there is not much grace in "adding software elements" to calculations.

6.4.2.4 For a "**non-safety**" software, we shall consider the probability of failure to be 10^-3, if we have no other data. But be aware that as this estimation is in contrast to common consensus it should be performed very carefully and with good explanations. On the other hand, if the need arises to calculate the failure probability of "non-safety" software, the implication is that the software is "safety" and we return to square one (probability of failure = 1).

6.4.2.5 Suggested methods in case a software fault is identified:

6.4.2.5.1. Check if the software was developed in accordance with the relevant DAL.

6.4.2.5.2. Calculate risk assessment by setting the probability of software failure as one. If it's critical software, the calculated risk will probably be high and unacceptable, but, by visualizing the risk chain, in some cases, risk mitigation or a supportive tool could be required to decrease total risk.

6.4.2.6 An expanded discussion about "software Risk Assessment" appears in Appendix 3.

7. Risk Assessment

7.1. "Risk analysis" alone has a little value by itself. What makes risk analysis a powerful tool is the ability to compare the calculated risk

with a predefined allowable/acceptable threshold, or "risk assessment".

7.2. Risk analysis/assessment must take in consideration whether the risk occurrence probability is time dependent or uniformly distributed.

7.3. The risk criteria defined by CAAI as allowable is :

Criteria	Fatalities expected Per F/H	Expected Fatalities for fleet life	Comments
Individaul Risk	<10^-7		Airplanes on which the condition under study can occur
Fleet Risk		<3	

7.4. Risk assessment methodology is described in the following appendixes.

7.5. Assigning any event as "non-safety issue" should be followed with a detailed risk assessment analysis.

Appendix 2: "Risk Likelihood" calculation

1. Working with likelihood requires an understanding of the following concepts:

   1.1. Do not change the prediction to match limited data: A probability indicates that a failure, error, or accident is possible even though it may occur rarely over a period of time or during a considerable number of operations. A probability cannot indicate exactly when, during which operation, or to which person an accident will occur. It may occur during the first, last, or any intermediate operation in a series without altering the analysis results. Consider an example of when the likelihood of an aircraft engine failing is accurately predicted to be one in 100,000. The first time the first engine is tried it fails. One might expect the probability of the second one failing to be less. But, because these are independent events, the probability of the second one is still one in 100,000. The classic example demonstrating this principal is that of flipping a coin. The probability of it landing "heads-up" is 1 chance in 2 or 0.5. This is true every time the coin is flipped even if the last 10 trials experienced a "heads-up" result.

   1.2. Consider the statistical nature of probability when formulating a conclusion: Probabilities are statistical projections that can be based upon specific past experience. Even if equipment is expected to perform the same operations as those used in the historical data source, the circumstances under which it will be operated can be expected to be different. Additional variations in production, maintenance, handling, and similar processes generally preclude two or more pieces of equipment being exactly alike. Minor changes in equipment have been known to cause failures and accidents when the item was used. If an accident or failure occurs, correcting it by changing the design, material,

procedures, or production process immediately nullifies certain portions of the data.

1.3. Look for important variables that may affect conclusions based on statistics: Sometimes data are valid only in special circumstances. For instance, a statistical source may indicate that a specific number of aircraft accidents due to birdstrikes take place every 100,000 or million hours. One may conclude from this data, that the probability of a birdstrike is comparatively low. Hidden by the data analysis approach, is the fact that at certain airfields, such as Boston, the Midway Islands, and other coastal and insular areas where birds abound the probability of a birdstrike accident is much higher than average. This example demonstrates that generalized probabilities do not serve well for specific, localized areas. This applies to other environmental hazards such as lightning, fog, rain, snow, and hurricanes.

1.4. Be clear on the conditions that the probabilities used in the risk analysis represent: Reliability predictions are based upon equipment being operated within prescribed parameters over a specific period of time. When the equipment's environment or operational profile exceeds those design limits, the prediction is invalid. Safety analyses based on this data, aimed at predicting safety performance under abnormal and/or emergency conditions may also be invalid. Reliability predictions do not extend to performance of components or subassemblies following a failure. That is, the failure rate or characteristics of failed units or assemblies are not accounted for in reliability generated predictions. Design deficiencies are not accounted for in reliability predictions.

1.5. Consider the impact of human error on accident probability estimations: Human error can have damaging effects even when equipment reliability is high. For example, a loaded rifle is highly

reliable, yet many people have been killed or wounded when cleaning, carrying, or playing with loaded guns.

1.6. Understand the source of prediction data: The confidence in probability prediction, as in any statistic, is based on the sample size of the source data. Predictions based on small sample sizes have low confidence levels; those based on a large sample size provide a high degree of confidence.

1.7. The Risks related to systems that exhibit wear out are more difficult to quantify than those that do not: Reliability predictions of electronic components could assume an exponential failure distribution. This is a reasonable assumption for systems conservatively designed prior to wear out. The confidence that the prediction represents regarding either a newly fielded system or an old system is lower. There are recently developed approaches to reliability predictions that consider mechanical fatigue of electronic components that account for wear out. Such improved prediction is only more valuable than the standard approach applied to a specific unit, when its history is known.

2. When the limitations are understood, the use of probabilities permits a more precise risk analysis than the qualitative approach. Calculated hazard risks can be compared to acceptable thresholds5 to determine when redesign is necessary. They permit the comparison of alternate design approaches during reviews, leading to more thorough evaluations. Performing quantitative analyses requires more work than qualitative analyses and therefore costs more. If the limitations of the numbers used are not clearly stated and understood, incorrect conclusions may be reached. When care is taken, a quantitative analysis can be significantly more useful than a qualitative one.

[5] Acceptable threshold in C.O.S vocabulary means 'Acceptable Risk"

Appendix 3: Software Risk Assessment

1. Overview:

1.1. Today software is all around us and has "finger prints" in any action, evaluation or decision making. Sometimes the presence of the software is visible, such us in displays or control systems and sometimes invisible, such us in actuators or sensors.

1.2. Software should never be considered as an isolated issue, rather as a system issue due to the vast effect of each module on other elements in the system, which makes complete debugging impossible.

1.3. Software failure may occur in a vast and varied way, sometimes without no trace, such as:

1.3.1. Failure of the software to perform a required function, i.e., either the function is never executed or no answer is produced.

1.3.2. The software performs a function that is not required, i.e., receives the wrong answer, issues the wrong control

instruction, or performs the correct action under inappropriate conditions.

1.3.3. The software possesses timing and/or sequencing problems, i.e., fails to ensure that two actions occur at the same time, at different times, or in a particular order.

1.3.4. The software failed to recognize that a hazardous condition, requiring corrective action, occurred.

1.3.5. The software failed to recognize a safety-critical function and failed to initiate the appropriate fault tolerant response.

1.3.6. The software produced the intended but inappropriate response to a hazardous condition.

1.4. The specific causes most commonly associated with the software failure mechanisms listed above are:

1.4.1. Specification Errors: Specification errors include omitted, improperly stated, misunderstood, and/or incorrect specifications and requirements. Software may be developed "correctly" with regard to the specification, but incorrectly from a systems perspective. This is probably the single largest cause of software failures and/or errors.

1.4.2. Design and Coding Errors: These errors are usually introduced by the programmer and can result from specification errors, usually the direct result of poor structured programming techniques. These errors can consist of incomplete interfaces, timing errors, incorrect interfaces, incorrect algorithms, logic errors, lack of self-tests, overload faults, endless loops, and syntax errors.

This is especially true for fault tolerant algorithms and parameters.

1.4.3. Hardware/Computer Induced Errors: Although not as common as other errors, these do exist. Possibilities include random power supply transients, computer functions that transform one or more bits in a computer word that unintentionally change the meaning of the software instruction, and hardware failure modes that are not identified and/or corrected by the software to revert the system to a safe state.

1.4.4. Documentation Errors: Poor documentation can be the cause of software errors through miscommunication. Miscommunication can introduce the software errors mentioned above. This includes inaccurate documentation pertaining to system specifications, design requirements, test requirements, source code and software architecture documents including data flow and functional flow diagrams.

1.4.5. Debugging/Software Change Induced Hazards: These errors are basically self-explanatory. The cause of these errors can be traced back to programming and coding errors, poor structured programming techniques, poor documentation, and poor specification requirements. Software change induced errors help validate the necessity for software configuration.

2. Software Risk Probability

2.1. With all the above, and the influence of software on system level risks, some would say that a tool to assume software failure probability is critical, but at the bottom line, no such tool exist. Determining the probability of failure of a single software function is difficult at best, and cannot be based on historical data. Software

is generally application-specific and reliability parameters associated with it cannot be estimated in the same manner as hardware.

2.2. Therefore, another approach shall be used for the assessment of software's contribution to system risk, that considers the potential risk severity and the degree of control that software exercises over the hardware.

2.3. In this process, you create two vectors, in the first one, you evaluate the risk associate with the process and in the second you evaluate in involvement or the degree of control the software has on the process. Merging those two vectors reveals a new matrix that describes the risk associate with each software element.

Software Hazard Criticality Matrix

Extracted from Mil-Std 882C

For Example Purposes Only

Control Category	Severity			
	Catastrophic	Critical	Marginal	Negligible
(I) Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazards occurrence.	1	1	3	5
(IIa) Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.	1	2	4	5
(IIb) Software item displays information requiring immediate operator action to mitigate a hazard. Software failure will allow or fail to prevent the hazard's occurrence.	1	2	4	5
(IIIa) Software items issues commands over potentially hazardous hardware systems, subsystem, or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.	2	3	5	5
(IIIb) Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.	2	3	5	5
(IV) Software does not control safety critical hardware systems, subsystems, or components and does not provide safety critical information.	3	4	5	5

High Risk - Significant Analyses and Testing Resources

Medium Risk - Requirements and Design Analysis and Depth Testing Required

Moderate Risk - High Levels of Analysis and Testing Acceptable With Managing Activity Approval

Moderate Risk - High Levels of Analysis and Testing Acceptable With Managing Activity Approval

Low Risk - Acceptable

2.4. RTCA DO-178B/C basically divides software to five "Design Assurance Level" (DAL) by examining the effects of a failure

condition in the system. The failure conditions are categorized by their effects on the aircraft, crew, and passengers :

2.4.1. **DAL(A)** - Catastrophic – Failure may cause multiple fatalities, usually with loss of the airplane.

2.4.2. **DAL(B)** - Hazardous – Failure has a large negative impact on safety or performance, or reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers.

2.4.3. **DAL(C)** - Major – Failure significantly reduces the safety margin or significantly increases crew workload. May result in passenger discomfort (or even minor injuries)

2.4.4. **DAL(D)** – Minor - Failure slightly reduces the safety margin or slightly increases crew workload. Examples might include causing passenger inconvenience or a routine flight plan change.

2.4.5. **DAL(E)** - No Effect – Failure has no impact on safety, aircraft operation, or crew workload.

2.5. The FAA applies DO-178C for guidance in determining if software will perform reliably in an airborne environment, when specified by

the Technical Standard Order (TSO) for which certification is sought.

3. Bottom line:

3.1. Hazardous software failures are not supposed to happened, but they will, and in the most inconvenient time.

3.2. If this occurs :

3.2.1. Check if the software was developed by the correct DAL

3.2.2. Calculate the risk assessment by setting the probability of software failure as one.

3.2.2.1 If the software is critical, the calculated risk will probably be high and unacceptable, but, by visualizing the risk chain, in some cases, a risk mitigation or a supportive tool might be applied to decrease the total risk.

Appendix 4 – Safety Risk Definition Table & Risk Matrix

1. The Severity and Likelihood definition tables in this Appendix are generic and are meant to be used for Risk Assessment.

2. It is important to remember that "End Events" can result in more than one outcome, and each outcome might need to be calculated differently/separately.

Severity / Likelihood		Minimal	Minor	Major	Hazardous	Catastrophic
		Negligible safety effect	Physical discomfort to person or slight damage to a/c	Physical distress or injuries to person. Substantial damage to a/c	Multiple serious injuries or fatal up to 2 persons, or a hull los without fatalaties	Multiple fatalities, usually with loss of a/c
Frequent	Occur routinely					
Probable	Occur often					
Remote	Occur Infrequently					
Extremely Remote	Occur rarely					
Extremely Improbable	Not expected to occur					

Whereas :

Unacceptable Risk

Acceptable Risk with Mitigation

Acceptable Rist

Unacceptable with Single failure or Common Cause

3. Obviously, severity is easier to determine, due to more quantitative criteria such as "fatalities" and "loss of a/c". on the other hand, likelihood is much harder to determine and evaluate.

4. Some of the Difficulty in evaluating likelihood is the fact that sometimes, when the fleet is big enough, an "Extremely Remote" event for a single a/c might become a remote or even probable event when considering the fleet.

5. In order to handle the differences between a single a/c and a fleet, a different set of definitions was provided :

Likelihood Scale Definitions			Value
Frequent	Individual	Likely to occur often.	
	Fleet	Continuously experienced.	
Probable	Individual	Will occur several times.	<10E-3 f/h
	Fleet	Will occur often.	
Remote	Individual	Likely to occur some time.	<10E-5 f/h
	Fleet	Will occur **several times in the entire fleet.**	
Extremely Remote	Individual	Unlikely to occur, but possible.	<10E-7 f/h
	Fleet	Unlikely but can reasonably be expected to occur **few time in a fleet life time.**	
Extremely Improbable	Individual	So unlikely, it can be assumed it will not occur.	<10E-9 f/h
	Fleet	Unlikely to occur, but possible. **Less then one in the entire fleet life time.**	

6. The definitions above are based on: FAA System Safety Handbook, Chapter 3.

APPENDIX 5 - Documentation and Decision traceability

1. Any event suspected as having safety implications, requires documentation from initiation, allowing easy review and showing the status and decision making rational.

2. Documentation will include, at least, the followings:

Item	Title	Description
1	**Reference number**	This is a specific number assigned to a SAR
2	**Opening Date**	The date of SAR initiation.
3	**Current Status**	The status of the SAR is indicated as open, monitor, or closed.
4	**Title**	A specific appropriate short title of the SAR.
5	**Description**	The description defines the specific hazardous event under study and its worst case outcome.
6	**Causes/Contributors**	The single or combined contributory events that can create the event under study.
7	**Risk (Severity and Likelihood)**	The risk associated with the event.
8	**Suggested/Possible Mitigations/Controls**	design and/or administrative controls, precautions, and recommendations, to reduce risk.
9	**Evaluation**	appropriate activities and entities involved in the evaluation of the specific event .
10	**Implemented Mitigations/ Controls**	design and/or administrative controls, precautions, and recommendations that have been verified within the design .
11	**Verification and Validation**	verification and validation to assure that system safety is adequately demonstrated .
12	**Narrative History**	Provide a chronological history of all actions taken relative to the SAR.

13	**References**	Appropriate references associated with the specific SAR.
14	**Originator(s)**	The person(s) originating the SAR are listed.
15	**Concurrence**	Appropriate concurrence is required to revise SAR status to closed (or monitor).

APPENDIX 6 - GLOSSARY AND ABBREVIATIONS

Safety Management System

A Safety management System (SMS) is an integrated collection of processes, procedures, and programs that ensures a formalized and proactive approach to system safety through risk management. Risk analysis is required for all activities or process changes to identify safety impact. SMS involves identifying hazards, estimating risk, and reducing known risk to an acceptable level (risk management). The SMS is a closed-loop system ensuring corrective actions or process changes are documented and all problems or issues are tracked to their conclusion

Safety and Risk.

Within this procedure and for all practical purposes related to this procedure, safety is considered as the understood and acceptable risk level of a specific activity that is. If the risk in a specific activity is considered unacceptable, then the activity is unsafe. If the risk of an activity has been analyzed, and the analysis indicates that all reasonable risk controls have been implemented and that any remaining risk is acceptable, then the activity is considered safe. Acceptable risk will vary depending on the application and should be defined appropriately.

Safety Program and Oversight System.

The safety program is a concept developed by ICAO to describe an integrated set of regulations and activities aimed at improving safety. ICAO standards and recommended practices require that States establish a safety program to achieve an acceptable level of safety in aviation operations. Each State establishes its acceptable level of safety. ICAO defines the safety program as including provisions for an array of activities, including incident reporting, safety

investigations, safety audits, and safety promotion. A coherent SMS is required to implement such safety activities in an integrated manner.

Accident

An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.

Air transportation system.

The entirety of the aviation system, including the authority, entities that design, manufacture, or operate aircraft or components of aircraft; training entities; people; infrastructure; and other systems and subsystems.

Aircraft accident

An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight and until such time as all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage.

Aircraft incident

An occurrence other than an accident, associated with the operation of an aircraft, that affects or could affect the safety of operations.

Audit

A scheduled or unscheduled review of an organization's operations to determine the level of compliance with established standards or protocols.

Continual improvement

A set of activities an organization routinely carries out to enhance its ability to meet requirements in response to ongoing system feedback. Continual improvement can be achieved by carrying out internal audits, performing management reviews, analyzing data, and implementing corrective and preventive actions.

Effectiveness

A measure of how well desired outcomes are achieved, generally in reference to a specified standard. Effectiveness in a safety management system (SMS) refers to the results of risk management activities in terms of the applicable standard and the intended results.

Fail safe

A characteristic of a system whereby any malfunction affecting the system safety will cause the system to revert to a state that is known to be within acceptable risk parameters.

Hazard

Any existing or potential condition that can lead to injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident. Note that a hazard may or may not result in a situation of high risk.

Likelihood

The estimated probability or frequency, in quantitative or qualitative terms, of a hazard's effect.

Procedure

A specified way to carry out an activity or a process.

Process

A set of interrelated or interacting activities that transforms inputs into outputs.

Quality assurance

The part of quality management focused on providing confidence that requirements will be fulfilled.

Quality control

Activities after production of a product or service to ensure the final output has conformed to the desired parameters.

Quality management

Coordinated activities to direct and control an organization with regard to quality.

Quality management system. A set of interrelated or interacting processes with regard to quality, accomplished by the management of an organization by establishing policy and objectives and achieving those objectives.

Quality system

The organizational structure, responsibilities, procedures, processes, and resources for implementing quality management.

Risk

The composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state. There are three types of risk:

Initial — The severity and likelihood of a hazard when it is first identified and assessed; includes the effects of preexisting risk controls in the current environment.

Current — The predicted severity and likelihood of a hazard at the current time.

Residual — The remaining risk that exists after all risk control techniques have been implemented or exhausted and all risk controls have been verified.

Risk analysis

The process whereby hazards are characterized for their likelihood and severity. Risk analysis looks at hazards to determine what can happen when. This can be either a quantitative or qualitative analysis. The inability to quantify and/or the lack of historical data on a particular hazard does not exclude the hazard from the need for analysis. Some type of a risk analysis matrix is normally used to determine the level of risk.

Risk assessment

The process by which the results of risk analysis are used to make decisions. The process of combining the impacts of risk elements discovered in risk analysis and comparing them against some acceptability criteria. Risk assessment can include the consolidation of risks into risk sets that can be jointly mitigated, combined, and then used in decision making.

Risk control

Anything that mitigates risk. A risk control should directly map to a safety design requirement. All risk controls must be written in requirement language.

Safety

Safety is the state in which the risk of harm to persons or property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management.

Safety assurance

SMS process management functions that systematically provide confidence that safety objectives are met or exceeded.

Safety culture

Safety culture is descriptive of organizations where each person involved in the organization's operations recognizes and acts on his or her individual responsibility for safety, and actively supports the organization's processes for managing safety. The outcome is that the organization's ability to manage safety continues to improve because decision makers at all levels work to use their knowledge of safety risk to learn and adapt, thus improving the system's ability to support safety outcomes.

Safety management

The act of understanding and making decisions and reducing the risk of actions to acceptable levels.

Safety oversight

A function by means of which States ensure effective implementation of the safety-related laws, regulations, policies, and procedures. Safety oversight also ensures the national aviation industry provides a safety level equal to or better than the acceptable level defined by the State.

Safety risk management

A process within the SMS composed of describing the system, identifying hazards, and analyzing, assessing, and controlling the risk.

Serious injury.

Any injury any injury which:

(1) Requires hospitalization for more than 48 hours, commencing within 7 days from the date the injury was received;

(2) Results in a fracture of any bone (except simple fractures of fingers, toes, or nose);

(3) Causes severe hemorrhages, nerve, muscle, or tendon damage;

(4) Involves any internal organ; or

(5) Involves second or third degree burns, or any burns affecting more than 5 percent of the body surface.

Severity

The consequence or impact of a hazard in terms of degree of loss or harm.

Substantial damage

Damage or failure which adversely affects the structural strength, performance, or flight characteristics of the aircraft, and which would normally require major repair or replacement of the affected component. Engine failure or damage limited to an engine if only one engine fails or is damaged, bent fairings or cowling, dented skin, small punctured holes in the skin or fabric, ground damage to rotor or propeller blades, and damage to landing gear, wheels, tires, flaps, engine accessories, brakes, or wingtips are not considered "substantial damage."

Surveillance

The act of monitoring and evaluating an organization, product, or service in a systematic way to verify compliance with regulations; operation in accordance with their systems and methodologies; and that the desired outcome is achieved or product or service performance meets expectations.

System

An integrated set of constituent pieces combined in an operational or support environment to accomplish a defined objective. These pieces include people, equipment, information, procedures, facilities, services, and other support services, which interact.

System engineering

A discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all the facets and all the variables, and relating the social to the technical aspect. The translation of operational requirements into design, development, and implementation concepts and requirements in the lifecycle of a system.

System safety

The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle.

System safety engineering

An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated risk.

System safety management

A management discipline that defines system safety program requirements and ensures the planning, implementation, and accomplishment of system safety tasks and activities are consistent with the overall program requirement.