

FLIGHT TEST RISK ASSESSMENT “THREE FLAGS” METHOD

Author: Maximilian Kleinubing BS.

Field: Aeronautical Engineering, Flight Test Operations

Keywords: Flight Test, Safety Assessment, Flight Test Safety Assessment

ABSTRACT

A trustworthy evaluation criteria and risk management related to development flight test and certification of aircraft is necessary in order to stimulate the process of reasoning and keep tests safety-oriented, identify risk factors and take corrective measures to minimize them. The method described here is used at present day at Embraer for Risk Assessment for flight tests.

Government Certification agencies such as the Federal Aeronautical Administration (FAA) and the European Aircraft Safety Agency (EASA) require that the aircraft manufacturers have an internal policy to mitigate exposition to risks to allow its crew to participate in the certification flights. Moreover, from 2012 and on, the International Civil Aircraft Organization (ICAO) requires the all aircraft manufacturers follow the Safety Management System (SMS), which are a set of procedures to ensure that the safety related events get appropriate treatment throughout the organization.

The method that will be presented can be used during development Flight Test Campaigns and certification of military and civilian aircraft. In addition, also applies to the activities of production flights.

The method is divided in three different steps that are focused on the aircraft flight envelope, the test maneuver that will be performed by the pilot and the possible failures that might affect the test safety. Each analysis results in a risk classification. The final risk classification is the highest of all three analysis.

After definition of the risk classification, a Risk Management Process is conducted to find minimization and mitigation procedures to control risk exposure. A minimization procedure is the one that tries to avoid unnecessary risks (pro-active) and mitigation procedures is the one that tries to reduce the side effects of a known hazard once it has happened (re-active).

Desirable byproducts of this method are the definition of the safety support of the tests, the required crew qualification, minimum meteorological conditions and the minimum level of authorization to perform the tests.

INTRODUCTION

Safety Assessment is the process of identifying risks and quantifying or qualifying the degree of risk that the event will cause to individuals and resources. The risk assessment of a testing campaign will always be held by a test pilot and a flight test engineer.



EMBRAER Proprietary Information - Use or disclosure of this information is subjected to written authorization.

Safety Management Systems and Safety Assessment Methods try to control the risks associated with product development and certification. In the aeronautical industry, safety related events are classified into four categories: catastrophic, hazardous, major, minor and no safety effect events.

Catastrophic events must always be avoided in the aeronautical industry. A catastrophic event is any occurrence related to the operation of the aircraft, which occurred between the shipments with the intention to perform a flight, up to the time of landing, during which at least one of the following situations occur:

- Any person suffers serious injury or pass away as a result of being in the aircraft, in direct contact with one of its parts, including parts detached or subjected to direct exposure of propeller, rotor or blasting leakage or to its consequences;
- The aircraft suffers damage or failure which adversely affects the structural strength, performance or flight characteristics, requires the replacement of major components or major repairs to the affected component. Exception is made for damages limited to the engine, its cowlings or accessories, or for damage limited to propellers, wing tips, antennas, tyres, brakes, fairings-landing gear, light dents and small holes in the aircraft skin;
- The aircraft is missing or is inaccessible.

Hazardous events should be reduced to a minimum acceptable and are defined as every occurrence, including air traffic, associated with the operation of an aircraft, with flight plans, which did not come to be characterized as an accident as defined above, but seriously affecting the safety of operation or safety margins.

Major events should be also be reduced to a minimum and are defined as fault conditions that present significant reduction of safety margins or functional capabilities of the aircraft, significant increase in workload or conditions that have an impact on the efficiency of the crew.

Minor events should be also be reduced to a minimum and are defined as fault conditions that present small reductions in flight safety and functional capabilities of the aircraft. Require crew actions that are within their normal operating capacity or even a small increase in workload.

No safety effects events are negligible and are defined as fault conditions that do not affect the operational capability of the aircraft or increase the workload of the crew.

A risk is defined as an undesirable event in terms of probability and severity of occurrence. A hazard is a condition, event, or circumstance that could lead to an unplanned or undesirable event (crew injuries, damage to the aircraft or loss of function).

Risk Management is a Risk Assessment step to reduce the risks to an acceptable level by the Flight Test Organization. The risk management process should be guided by the following guidelines:

- do not accept unnecessary risks (risks that do not contribute significantly to achieving the objectives of the test);
- when possible, reduce the risk through actions that will reduce the probability of occurrence of the harmful event, minimize its effects or reduce the exposure to it.



GENERAL METHODOLOGY FOR RISK CLASSIFICATION (CR)

The risk rating is accomplished through the analysis of the following factors:

- Aircraft Flight Envelope
- Test Point Execution
- System Failures

For each test point or maneuver these factors must be classified according to the following increasing severity values: Low, Medium, High, or Unacceptable. The final risk rating is the highest among them.

The Flight Test Director can, in advance and based on expertise, sort the given test to an unacceptable risk.

Measures to minimize the risks must be taken so that they can reduce the risk to an acceptable level.

The rating methodology can be summarized in Figure 1 below.

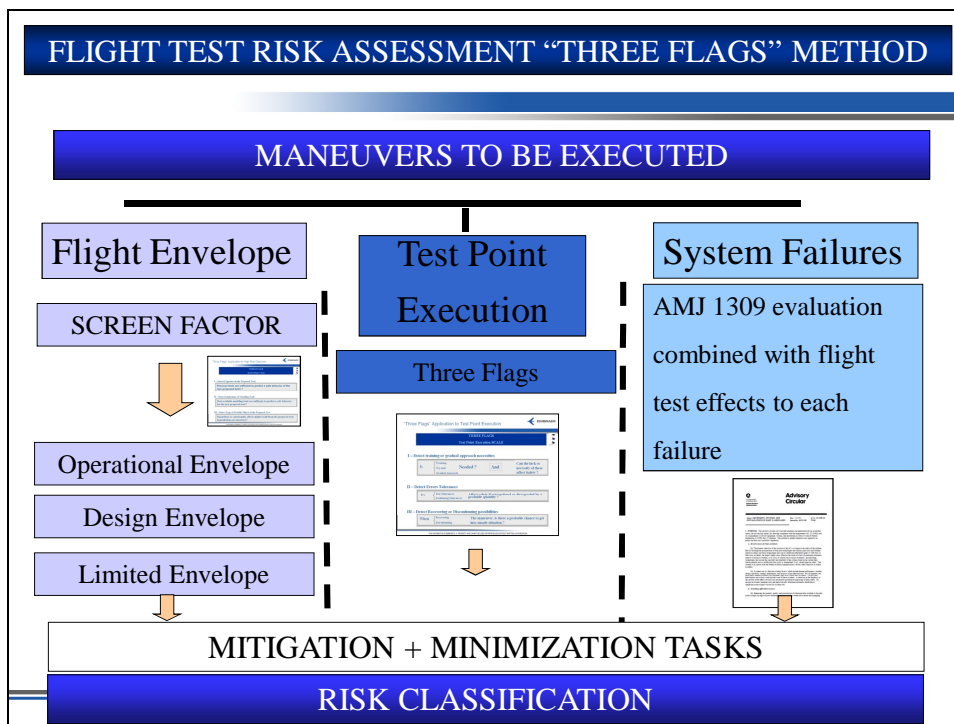


Figure 1 – Simplified diagram of the Risk Assessment Method

THREE FLAGS RISK ASSESSMENT METHOD

FLIGHT ENVELOPE SCALE

Screen Factor

The first step of the methodology for risk Classification is to determine the Flight Envelope classification. And to achieve that, a so called “Screen Factor Tool” is applied to detect whether the essay is classified as high risk as a result of:

- Tests carried out previously;
- Engineering models available; and
- Dangerous or catastrophic effects that may result from it.

The screen factor is defined by responding to the questions proposed in Figure 2.

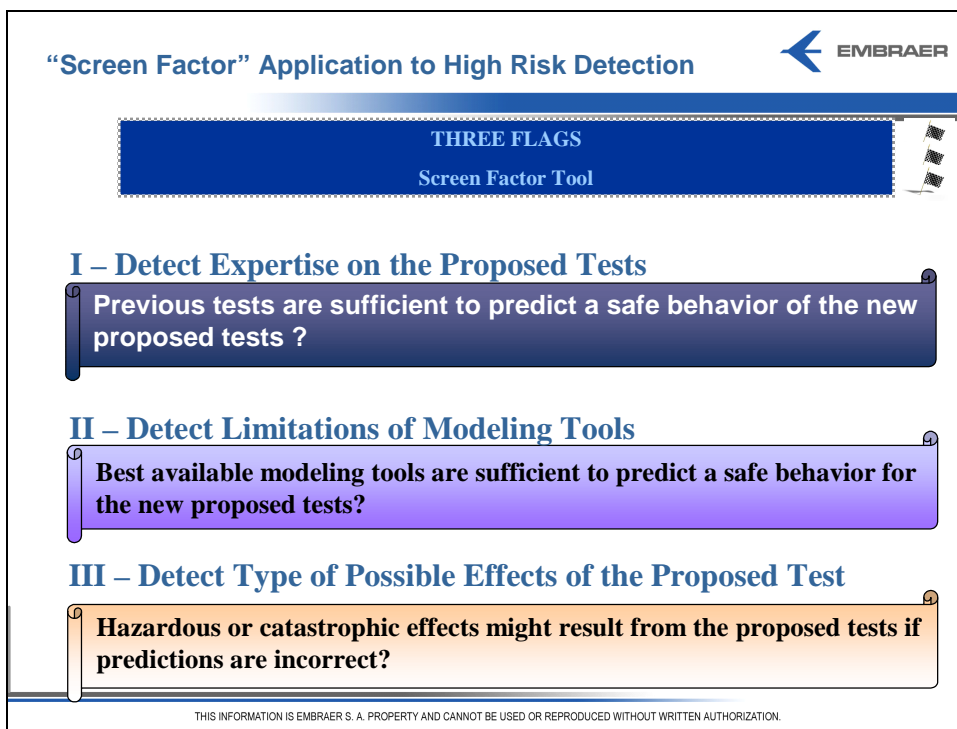


FIGURE 2 – SCREEN FACTOR DETERMINATION

A flagged question is, by definition, the one that got its answer pointed towards the unsafe condition.

The Screen Factor is considered High if one gets 3 flags by answering the questions proposed in Figure 2. If that is the case, the Flight Envelope is considered High Risk and the test will also be considered High Risk, however, the Test Point Execution and the System Failures Analysis should still be evaluated.

If the Screen Factor is not High, the test should be classified according to one of three possible envelopes:



- Limited flight Envelope: limited envelope during a given test campaign due to engineering constraints.
- The operational Flight Envelope: Envelope that will be defined by protections and scoreboards on the production aircraft and defined in the operational manuals of the aircraft.
- Design Envelope: Envelope that is established by the aircraft's description and engineering reports, which are in addition to the operational flight envelope.

The risk associated with the flight Envelope will be classified according to the table 2.

TABLE 1 – RISK CLASSIFICATION FOR THE FLIGHT ENVELOPE

FLIGHT ENVELOPE	RISK CLASSIFICATION
OPERATIONAL FLIGHT ENVELOPE	LOW
INSIDE LIMITED FLIGHT ENVELOPE	LOW
OUTSIDE LIMITED FLIGHT ENVELOPE (FOR THE FIRST TIME)	MEDIUM
DESIGN ENVELOPE	MEDIUM

TEST POINT EXECUTION SCALE

The operational assessment, the second step of the methodology for Risk Assessment, must be performed in order to determine the risk of the maneuver according to the degree of danger or difficulty running the test point from the pilot’s point of view.

The risk in this case is always related to the task to be performed, without considering the occurrence of failures.

The method proposed is based on a qualitative assessment of the maneuver and was developed by the Embraer Flight Test team using past experience and knowledge doing risk assessments.

The operational assessment will be carried out according to the following steps:

- Determine the task to be evaluated;
- Answer the questions in Figure 3;



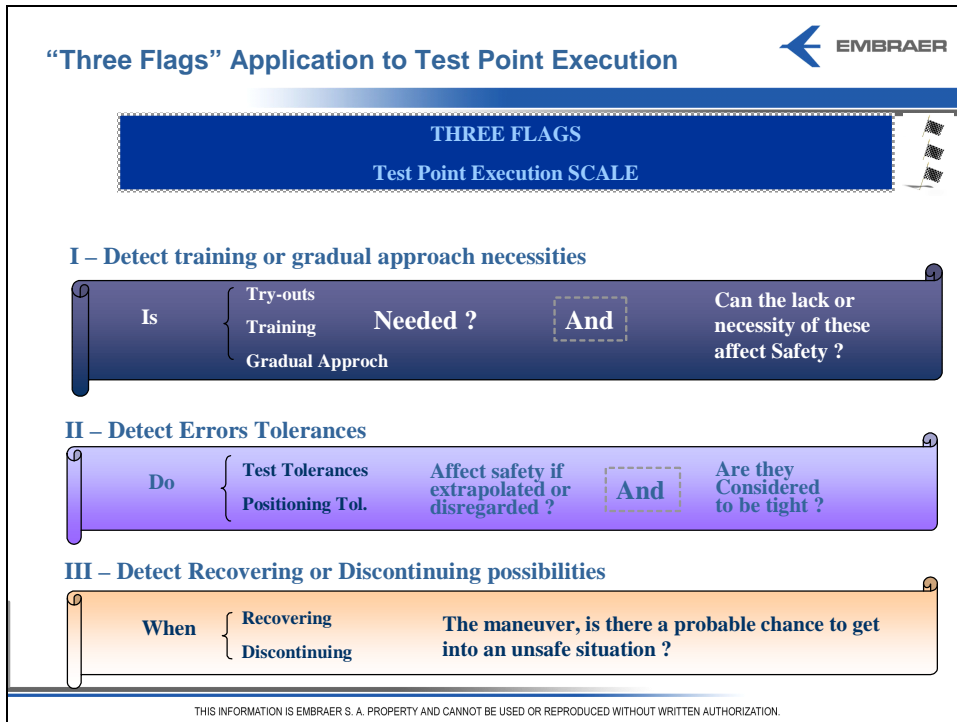


FIGURE 3 –TEST POINT EXECUTION

- According to the responses obtained, one will find the risk concerning the execution of the maneuver by considering that: if you have one flag or no flags the risk classification is low, if you have two flags the risk classification is medium and if you have three flags the risk classification is high. The order of the flags does not change the result, but rather the amount of flags found in response to the questions. The operational assessment may be re-discussed during the Safety Review Board, during which definitions of tasks will be confirmed or reviewed.

SYSTEMS FAILURE SCALE

The failures rates are identified and listed based on System Safety Assessment Report (SSA) and the Functional Hazardous Analysis (FHA) reports. However, you should consider the current conditions at the time of the test and operational situations peculiar to tests that can affect the effect of the possible failures. The limitations of each prototype, properly documented in the Prototype Operational Limitations document, or the limitations of the Airplane Flight Manual, in the case of testing on production aircraft, should also be considered. The flight test crew should be able to compile the necessary information and perform functional failure analysis of relevant systems in an integrated manner to the type of tests that will be performed. Critical systems and systems that are test subject should be analyzed for the execution of the maneuver.

The risk associated with the failure of systems should be obtained by following the steps as follows:



- Survey of relevant failures to the test, found in System Safety Assessment (SSA) Reports issued by the systems engineering team. It is known that the probability of failure is obtained by multiplying the rate of failure by the exposure time, which is a function of aircraft mission. In this way, the probability value correction may not have modifications to their values. Therefore, it is suggested the direct application of the System Safety Assessment Reports failure rates in the Flight Test System Failure analysis. The probability of each fault should be classified using table 2 below;

TABLE 2 – ACCEPTABLE FAILURE PROBABILITY OF OCCURRENCE

Aircraft Category	Failure Probability (P)				
	Highly Probable	Probable	Remote	Extremely Remote	Improbable
Militar*	$P > 10^{-3}$	$10^{-3} > P > 10^{-4}$	$10^{-4} > P > 10^{-5}$	$10^{-5} > P > 10^{-6}$	$P \leq 10^{-6}$
FAR 23 Normal/Acrobatc	$P > 10^{-3}$	$10^{-3} > P > 10^{-5}$	$10^{-5} > P > 10^{-7}$	$10^{-7} > P > 10^{-8}$	$P \leq 10^{-8}$
FAR 23 Commuter	$P > 10^{-3}$	$10^{-3} > P > 10^{-5}$	$10^{-5} > P > 10^{-7}$	$10^{-7} > P > 10^{-9}$	$P \leq 10^{-9}$
FAR 25	$P > 10^{-3}$	$10^{-3} > P > 10^{-5}$	$10^{-5} > P > 10^{-7}$	$10^{-7} > P > 10^{-9}$	$P \leq 10^{-9}$
* Highly dependent on Costumer Requirements.					

- Classification of fault effect, if it occurs during the execution of the test point, according to the definitions given in the Introduction section above (no SAFETY EFFECT, MINOR, MAJOR, HAZARDOUS or CATASTROPHIC). For maneuvers whose flaws are not defined by the Safety Assessment Reports, the classification must be defined by the flight test crew. For maneuvers whose failures have already been analyzed in the System Safety Assessment Reports, the effect of the failure during flight tests can be the same or not. It is accepted a modification of the purpose effect defined in the System Safety Assessment Report if an internal discussion concludes that the effect of the failure is different in the context of the test.
- Risk classification of the maneuver using the table 3 below. Risk classification is found crossing the x-axis and y-axis of table 3. Maneuvers whose failures were analyzed in the Safety Assessment Reports and comply with the established in the AC-23.1309-1c and JMA-25.1309 are considered LOW RISK from the point of view of Systems Failure, unless it is shown during the campaign that the probability or the effects considered are incorrect or not applicable.



TABLE 3 – RISK ASSESSMENT DUE TO SYSTEMS FAILURE

FINAL PROBABILITY	HIGHLY PROBABLE	LOW	MEDIUM	HIGH	UNACCEPTABLE	UNACCEPTABLE
	PROBABLE	LOW	LOW	MEDIUM	HIGH	UNACCEPTABLE
	REMOTE	LOW	LOW	LOW	MEDIUM	HIGH
	EXTREMALLY REMOTE	LOW	LOW	LOW	LOW	MEDIUM
	IMPROBABLE	LOW	LOW	LOW	LOW	LOW
		NO SAFETY EFFECT	MINOR	MAJOR	HAZARDOUS	CATASTROPHIC
FAILURE EFFECT						

RISK CLASSIFICATION OF THE MANEUVER

After being assessed by the criteria of Flight Envelope, Test Point Execution and Systems failure, the risk of the maneuver is obtained considering the highest rating obtained (see Figure 5 below). This is not yet the final ranking, because it must be reevaluated considering minimization procedures that might reduce it or not.

It is important to note that the procedures for minimizing the risk may lessen the risk classification by one level. Reductions of two or more levels of risk classification are highly not recommended and should be subject to discussions and approval during the Safety Review Board so that they can be carried out.

Mitigation procedures DO NOT decrease the risk of the test but act as tools for risk management.



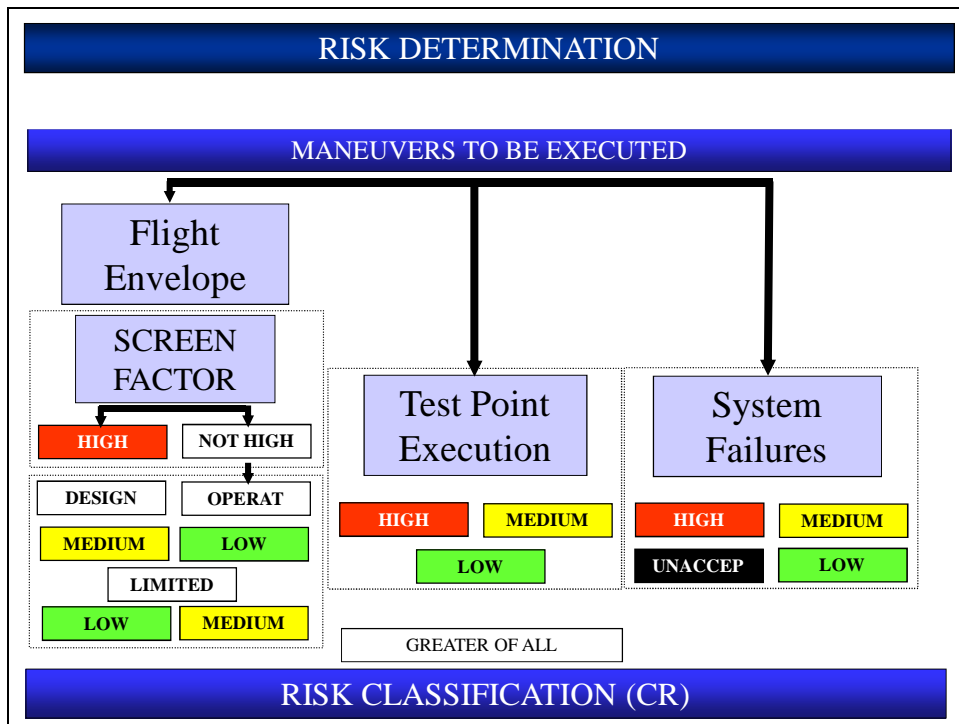


FIGURE 4 – RISK CLASSIFICATION DETERMINATION

RISK MANAGEMENT PROCESS

Each test has peculiarities that might require the adoption of different measures for the purpose of minimizing risks, increasing safety margins and mitigating the damage. The risks in flight test activities should be minimized by creating and applying a set of procedures that:

- Promote discipline and standardization in the conduct of all phases of the flight testing;
- Create formal processes to identify risk situations and measures to mitigate them;
- Contribute always to increase the safety margin of the test.

The risk management process begins when compiling the Flight Test Proposal (FTP), which should contain information that enable and support the risk assessment of the test maneuvers and ends with the authorization of the test by the authority with required responsibility.

The risk assessment of the proposed test maneuvers will be held by flight test crew responsible for the Flight Test Campaign.

The main steps of the risk management process are as follows:



- Test Request;
- Planning;
- Technical Review Boards;
- Risk assessment:
 - a. Identification of hazards and its causes
 - b. Estimation of the effects
 - c. Risk Minimization
 - d. Classification of Risk (preliminary)
 - e. Mitigation of damages
 - f. Set minimum requirements for carrying out the test
 - Safety Review Board (when necessary)
 - Risk Classification (Final)
 - Test authorization
 - Review of the classification of Risk (if needed)

RISK MINIMIZATION PROCEDURE AND MITIGATION OF DAMAGE

Although the Flight Test Organization considers acceptable Risk Classifications high or medium, it should be used whenever possible to minimize risk criteria applied in order to increase the safety of the test. There are no pre-defined risk minimization criteria. However, there are criteria that are the fruit of experience and boundary conditions that allow the minimization of risk.

The Risk Management procedures to be adopted for the tests maneuvers should contain:

- Title of Maneuver: spell out the task which will be applied to the process of risk minimization
 - Hazard: an event that potentially can cause damage or loss, personal injury or loss of life.
 - Causes: describe the cause (s) that could result in the occurrence of hazard, event;
 - Effects: describe the possible effects within the context of the test;
 - Risk Minimization procedures: enunciate the factors or actions that minimize the risk of occurrence of the harmful event.
 - Risk Mitigation Procedures: to be adopted in case of occurrence of the harmful event, can and should be considered as mitigating against damage to crew: use of flame-retardant clothing, helmet, gloves, parachute, LPU, device for emergency escape from aircraft, minimum crew among others.

Search and rescue team, fire brigade, ambulance medical staff warned are features that are also part of mitigating the damage in case of occurrence of a harmful event.



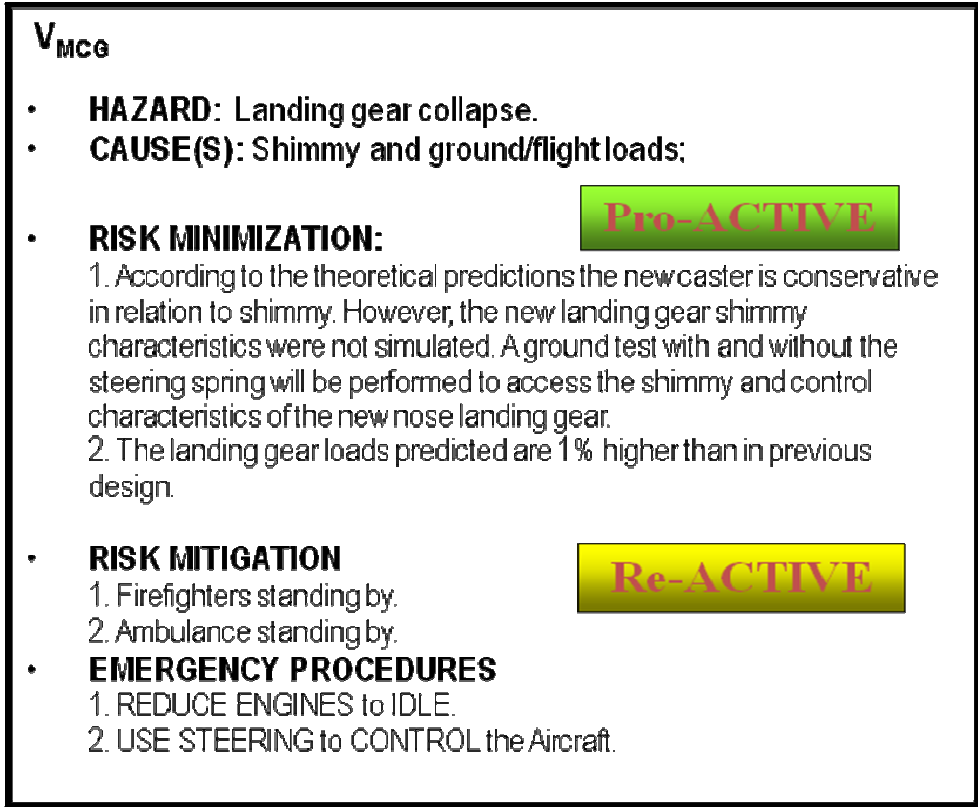


FIGURE 5 – RISK MANAGEMENT PROCESS



REFERENCES

[Ref.1] - AC 23.1309-1C – Equipments, Systems and Installation in Part 23 Airplanes.

[Ref.2] - AMJ 25.1309- Advisory Material Joint 25.1309 Arsenal.

[Ref.3] - US FAA Order 4040.26A - Aircraft Certification Service Flight Safety Program.

[Ref.4] – Embraer Normative System ENS 000650 Rev. 6 – Avaliação e Gerenciamento de Riscos em Ensaio em Vôo, 2010.



EMBRAER Proprietary Information - Use or disclosure of this information is subjected to written authorization.