Flight Operational Safety Assessment - Requirements for New Procedures (RNP-AR)

C.A. Fernandes Cabaço

1 Instituto Superior Técnico, Lisbon, Portugal, claudiacabaco@gmail.com

Abstract

The utmost development of aircraft operational performance based on navigation performance for approach and missed approach, using area navigation avionics systems is known as Required Navigation Performance – Authorization Required, RNP-AR. Because the implementation of this new operational concept has the potential to contribute significantly to the safety level of flight operations, EASA requires operators to perform a Flight Operational Safety Assessment (FOSA) as part of the operational approval process. The purpose of this FOSA is to demonstrate that the target level of safety is achieved. However, no official documentation produced or supported by EASA is available to the public domain regarding what a FOSA methodology is. The purpose of this research is to assist Aircraft Operators with this requisite. In order to achieve this goal, an analysis of the main methods currently available was performed. This analysis clarified that a FOSA is no different than a safety assessment and proposes a practical methodology, balancing between numeric and qualitative assessment of the interdependence of all potential hazards from all areas, based on the ICAO 7-step safety assessment process. For the execution of the three main steps the use of key informant technique, brainstorming sessions, Excel and @Risk software’s was selected, in order to benefit from the resources, experience and expertise available at the majority of the aircraft operators. It also concluded that independently of the tools used for each step, safety assessment will always be a subjective methodology, highly dependent of the expertise of those participating in it.

Keywords: RNP-AR FOSA, Safety Assessment, Risk Assessment, Safety, Risk, Hazard

1. Introduction and Objectives

The rapid worldwide increase of air traffic and aircraft technological development demands a rapidly changing and adaptation of aviation operational environments, which boundaries are rarely limited to single countries. Along with this continuous change, the assurance of safe aviation operations is paramount. However, absolute safety does not exist, because failures will always occur, in spite of the most accomplished and prevention efforts, as it is impossible to completely eliminate all risks. No human-made system/technology can be free from risk and error. Nonetheless, risk and error are acceptable if controlled in an inherently safe system. So how is it possible to ensure that aircraft operations are safe if it is not possible to eliminate all risks? What is safety? As per ICAO definition, 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.”[11], page 16. Therefore whenever new operations, equipments are to be put in place, it is necessary to ensure that the acceptable level of safety is guaranteed.

Due to the continuing air traffic increase, in order to allow the air space capacity to growth, new procedures and navigation concepts are necessary. Therefore, it is necessary to ensure that acceptable levels of safety risk are guaranteed. One of the latest aircraft navigation operational concept to be regulated and its use permitted to aircraft operators is Required Navigation Performance – Authorization Required, RNP-AR. The application of RNP-AR procedures to terminal area and approach operations is expected to provide an opportunity to utilize current aircraft capability and performance in order to improve safety, efficiency and capacity through the incorporation of additional navigational accuracy, integrity and functional capabilities. It allows operations to be implemented in circumstances where other types of approach procedures are not operationally satisfactory or possible. Safety will be improved when RNP-AR procedures replace visual procedures or non-precision approaches and efficiency through more repeatable and optimum flight paths. Capacity will be improved by de-conflicting traffic during instrument conditions. Once new operational concepts and its implementation have the potential to contribute significantly to the safety level and efficiency of flight operations, EASA requires operators to perform a Flight Operational Safety Assessment (FOSA) as part of the operator approval process for this navigation requirement. The target level of safety or acceptable level of safety for RNP-AR operations is a probability of risk of collision of less than 10^{-7} per flight or approach. The purpose of this type of methodology is to support the formal assessment of the magnitude of the safety risks posed by certain occurrences due to the new type of operation that the operator will or is expected to experience, during the decision making process. However,
no official documentation produced or supported by ICAO or EASA is available to the public domain regarding what a FOSA methodology is. How can the Operator demonstrate to the Authority that its RNP-AR operations meet the target level of safety established in the regulations? Is it a FOSA the same as safety assessment or a risk assessment? But what is the difference between a safety and a risk assessment? Is a FOSA methodology different from a generic safety assessment, since they aim the same objective?

Several aircraft operators are known to request this type of operational approval nonetheless, at the time of production of this report no European aircraft operator had been granted operational approval and several have raised concerns regarding the lack of guidance on the subject of the FOSA methodology. Also several airports are under approval process to allow aircraft operators to fly into it under RNP-AR approach procedures.

The scope of this research is to propose a FOSA methodology to support the implementation of RNP-AR into the daily operation of a European Aircraft Operator. It aims to present a clear, coherent, complete and integrated approach to aircraft operators to perform a FOSA, part of the document package to be sent to the national authority requiring operational approval to conduct RNP-AR operations. In order to achieve this goal a top down approach was used, constituted by the following parts:

- Safety assessment and risk assessment state of the art analysis;
- Clarification of the differences between a safety and a risk assessment;
- Assessment of existing safety and risk assessment methods and tools;
- RNP state of the art analysis;
- RNP-AR analysis;
- Analysis of the RNP-AR FOSA regulatory requisite;
- Development a practical FOSA methodology, based on existing methods and tools readily available to the majority of the aircraft operators;
- Test the proposed FOSA methodology in a business jet operator;

2. State of the Art

2.1 Safety Assessment

Over the year’s aviation regulatory authorities and aviation industry experts have continuously developed and enhanced methods and tools to assess the continuous improvement of the aviation industry, with the aim to guarantee acceptable levels of safety while improving flight operational capability, increasing airspace efficiency and reducing operational costs. Meanwhile the concept of safety in the aviation industry also has different perceptions, such as: zero accidents or serious incidents; freedom from hazards; attitudes of employees of aviation organizations towards unsafe acts and conditions and error avoidance. All of these perceptions have a common understatement: ensure a control state over anything “that can precipitate bad or damaging outcomes”. It is accepted that this control can only be relative rather than absolute, as there is no such thing as zero accidents or even absolute freedom from hazards. Therefore when it is referred ‘acceptable level of safety’ it refers to a reasonable degree of control of the parameters within a system, that can contribute to undesirable scenarios. This acceptable level of safety can be set of numerous ways, based on quantitative or qualitative data, regulatory requirements, operator requirements, manufacturer requirements, user expectations (public opinion), and it is dependent of the activity under safety assessment. For this purpose and of the aviation industry ICAO defines Safety as: “The state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.” [1], page 16.

Investigation revealed that safety assessment, risk assessment, hazard and risk expressions are widely used in the industry, but there is a lack of terminology standardization and understanding regarding its definitions. Nowadays, the terminology safety assessment and risk assessment has merged into each other in such a way that it became difficult to understand whether or not they represent two distinct methods. If distinct, in which situations one should use each of them; or if they complement each other and the performance of one’s mandates the performance of the other. Nevertheless, despite these uncertainties, it is widely understood that their ultimate objective is common and it is to identify what and where actions need to be considered to guarantee the planned acceptable level of safety.

Analysis of the different meanings for safety and risk assessment used by different stakeholders revealed that none of them intends to be prescriptive, rather to provide guidance regarding acceptable methods that can be adopted and adapted to systematically manage safety in a rational and thoughtful way, independently of the environment being assessed. What sets the distinction between the two is their applicability, i.e. a safety assessment is applied to a new operation/system while risk assessment is applied to a known or on-going operation, as first presented in ICAO SMS manual, [1]. Therefore, the main objective of a safety assessment is to identify what are the potential risks that a new operation/system is expected to be exposed to and which are acceptable or not, based on a safety criteria set, normally by aviation regulators. The unacceptable risks need to be corrected or mitigated up to an acceptable level, this is, need to be managed in a systematic manner – risk management, which is an integrant part of the safety assessment process.

A safety assessment methodology is commonly described as a sequence of seven steps and differences are only found on the execution of each of the steps. Therefore a safety assessment is the result of the combination of methods and/or tools used for each of the steps. The selection of the methods and tools to use, depends on the operation/activity being assessed, this is the system complexity. Different methodologies and tools have been developed and used throughout the years in order to come up with more effective and practical approaches to conduct safety assessments.
In December 16th, 2009, EASA published the Decision 2009/019/R amending the ‘General Acceptable Means of Compliance of Airworthiness of Products, Parts and Appliances (‘AMC-20’). AMC 20-26, [6] establishes the acceptable means of compliance for airworthiness approval and operational criteria for RNP - Authorisation Required (RNP-AR) operations and lays out the conditions for which a Flight Operation Safety Assessment (FOSA) should be conducted to obtain the referred airworthiness and operational approval. However, no official documentation produced or supported by ICAO or EASA is available to the public domain regarding what a FOSA methodology is. From the AOC perspective, once it is focused in obtaining the operational approval the following questions need to be answered: What is a FOSA methodology? How can the Operator demonstrate to the Authority that its flight operations meet the target level of safety established in the regulations?

If a safety assessment and a FOSA share the same objective, i.e. demonstrate that the acceptable level of safety of an operation is met (target level of safety, as per EASA AMC 20-26, [6]), according to a pre-set safety criteria and both are to be applicable to a new operation, then a FOSA methodology should be no different from a generic safety assessment methodology, having per basis the 7 step safety assessment process widely accepted in the aviation industry:

1) System analysis and safety criteria definition
2) Hazards identification
3) Estimation of the hazard(s) consequences severity
4) Estimation of the hazard(s) occurrence likelihood
5) Risk estimation
6) Risk acceptability/mitigation
7) Safety assessment documentation

2.1.1 Hazard Identification Methods

The understanding and definition of what a hazard is, has changed all over the years in the aviation industry and still nowadays it continues to be subject of discussion and debate throughout the aviation community. Currently it is accepted that when assessing hazards or contributing factors, their source will be from a combination of different areas. The most used hazard definition is the one published and recommended by ICAO in the SMS manual, [1], page 62, hazard is a “Condition, object or activity with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function”. Therefore a hazard can be any factor within the four main categories: technical, human, organizational and environmental.

Hazard identification is traditionally a subjective task and hence its effectiveness relies on the expertise of the individual or team analyzing it, especially in the analysis of new type of operations where operational observations cannot be used.

Different analytical methods and sources of information are available in the industry to support the hazard identification process, either through operational observations or through process analysis. Such as: interviews with operational experts and key informant surveys; hazard brainstorming sessions; Hazard and Operability Tool (HAZOP); Fault Hazard Analysis (FHA).

2.1.2 Risk Assessment Methods

Risk analysis methods/tools provide a mean to undertake formal or informal analysis of the risk that results from a proposed action or of the risk involved in not performing a certain action. Support the assessment of the magnitude of the risks posed by occurrences that an aircraft operator is or may be exposed to; additionally help to indentify which events pose the greatest threat of leading to a serious incident or accident.

Different risk definitions can be found in the literature, but again in order to promote standardization and avoid redundancy of terminology it is selected to use the ICAO definition, [1], ‘Risk is the likelihood of injury to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function, measured in terms of probability and severity.’

Independently of the definition details, the regulation tendency is to break down the risk is in two components of the hazard, again differences appear on the labeling of the two components: likelihood of the occurrence given the adverse consequence due to a certain hazard, severity of the adverse consequences that can potentially result from the given hazard. Likelihood is dependent of the exposure, as the measurement of the opportunity for the sequence of events to occur set in terms of cycles, intervals, people, etc. Therefore, depending how the likelihood is calculated, exposure can be integrated in the likelihood or not. The likelihood of an adverse consequence becomes greater through increased exposure to unsafe conditions. Therefore it is common to present risk as: Risk = Likelihood x Severity

Different methodologies present the two components through a risk matrix although each one with different levels and acceptance criteria.

If the severity of the consequence(s) and their likelihood of occurrence are both expressed qualitatively (e.g., through words like high, medium, or low), the risk assessment is called a qualitative risk assessment. In a quantitative risk assessment or a probabilistic risk assessment, consequences are expressed numerically (e.g., the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as probabilities or frequencies (i.e., the number of occurrences or the probability of occurrence per unit time).

Should the risk level be considered unacceptable, corrective or mitigating actions should be put in place and then the risk must be reassessed, by the same methods/tools in order to identify if it is already accepted or not. This exercise shall be repeated until the risk achieves an acceptable level. The acceptability of the risk is determined by comparing the assessed level of risk to a predetermined criteria or safety objectives.

Several risk assessment tools and methods are available and can be divided into three main groups: Safety Engineering, Causal Analysis and Risk Prediction. All types of risk assessment tools are time consuming and require the participation of different experiences from subject matter experts, the more the better because the more reliable the results will be. Of the three types of risk
assessment groups analyzed, for the purpose of a safety assessment of RNP-AR operations, risk prediction tools is the appropriate group to use, because it integrates factors from different areas and for each no historical data is available. It uses a probabilistic approach rather than deterministic and it takes in consideration the interdependence of the different types of factors present.

2.2 The RNP concept

In the first ATC system designed, using analog radios, aircraft flew from A to B not in a straight line, but in the direction of one ground-base navigation aid (NAVAID) and then another - beacons. This is, flew in a zig-zag trajectory, connecting the dots across the sky until the aircraft would arrive at the final destination. In the late 60s, a new method of navigation was developed known as RNAV - Area Navigation. It allowed an aircraft to choose any desired flight path course within coverage of a network of equipment available, rather than flying directly from beacon to beacon, using waypoints based on radial navigation facilities: RNAV, [7] - “A method of navigation that permits aircraft operation on any desired course within the coverage of station referenced navigation signals or within the limits of a self contained system capability, or a combination of these”. With the increase of the aerial traffic and aircraft technological development it was necessary to improve the communication between pilot/aircraft and the air traffic controllers and the efficiency of airspace utilization. In line with this need and based on the aircraft navigation capability the RNP concept was developed - ‘a statement of the navigation performance necessary for operation within a defined airspace’. [3]. RNP can be seen as the evolution of RNAV. This is, an RNAV navigation specification that includes requirements for on-board performance monitoring and alerting:

- “monitoring”: onboard equipment monitors the aircraft’s performance, in regard of its ability to determine positioning error and/or to follow the desired path.
- “alerting”: the flight crew is alerted if the aircraft’s navigation system does not perform as expected.

Specific RNP types are identified by a single accuracy value, RNP - X that define the navigation performance, in nautical miles, of the aircraft operating within the airspace appropriate to the navigation capability – Figure 1. This specifies the navigation performance accuracy of the airspace users and of the navigation system combinations within the airspace. Each RNP specification establishes the level of onboard equipment required to monitor and alert the crew, when the RNAV system is not complying with the required performance.

In 2003, it was recognized the vital need of on-board performance monitoring and alerting requirements as it was considered of most importance especially in critical flight phases, such as final approach. As a consequence the Performance Based Navigation (PBN) concept, applicable to all flight phases, was created. The PBN specifies that for proposed operations within a certain airspace concept, RNAV system performance requirements shall be defined in terms of: accuracy; integrity; availability and continuity. PBN relies on area navigation systems that include satellite signals with advanced cockpit technology to fly the aircraft without depending on navigation to/from conventional ground-based navigational aids. The majority of the navigation systems are already implemented and available however, due to lack of regulations its use was not possible before. It allows navigation system technology to grow over time without requiring procedures to be reviewed as long as the navigation performance requirements for a proposed operation are continuously met by the navigation system. Following the PBN concept and in line with already existed in the USA, ICAO utmost development of aircraft operational performance based navigation for approach and missed approach, using avionics systems where authorization is required, is known as RNP-AR.

3. RNP-AR

The utmost development of aircraft operational performance based on navigation performance for approach and missed approach, using area navigation avionics systems where authorization is required is known under two different names: FAA refers to it as RNP SAAAAR - Special Aircraft and Aircrew Authorization Required, ICAO and EASA refer to it as RNP-AR. Albeit the requirements established by FAA and EASA are almost identical, the requirements established by EASA are a little more stringent. This research followed EASA requirements and guidelines.

RNP-AR approach procedures are characterized mainly by:

- Narrow lateral linear segments - RNP values ≤ 0.3 NM;
- Curved segments anywhere along the approach – Radius-to-Fix (RF) legs, before and after the final approach point. The use of RF legs allows access to airports not previously available.

![Figure 1 - RNP Capability](image-url)
Reduced lateral and vertical obstacles clearance surface;
Protection areas laterally limited to 2xRNP value without any secondary buffer;
Default values: Lateral TSE of +/- 1NM in the initial, intermediate and missed approach segments and TSE of +/- 0.3 NM in the final approach segment;
Lateral TSE as low as +/- 0.1NM can be require on any segment of the approach procedure;
Precise missed approach guidance – minima as low as RNP 0.1 on both final approach and missed approach;
The main operational benefits of RNP-AR are:
Additional navigation accuracy, integrity and functional capabilities, by taking advantage of current aircraft capabilities;
Improved safety level of operations, by replacement of visual procedures or non-precision approaches, improved situation awareness;
Allows fully automated operation – reduces pilot’s workload and stress and allows them to focus on monitoring the flight and react quickly and appropriately in case of an unexpected event;
Better access to terrain-challenged airports and special use airspace. For example Samedan/Switzerland airport, in mountains terrain, which prevents the installation of ILS;
Improved access to business airports in proximity to high traffic airports;
Increased airport access in poor weather conditions (low clouds, strong wind, turbulence, etc);
Increase airport capacity;
Increase airspace capacity by de-conflicting traffic during instrument conditions;
Reduced flight time due to optimized routing;
Smaller environmental footprint due to reduced noise and fuel use;
The use of RNP-AR can enable accurate navigation and obstacle avoidance in instrument meteorological conditions (IMC) under the IFR. This can significantly reduce the likelihood of accidents involving controlled flight into terrain (CFIT).

4. FOSA methodology - The Case of RNP-AR

A FOSA methodology should be no different from a generic safety assessment, once they aim the same objective - a safety assessment of RNP-AR flight operations. For the case of safety assessment of RNP-AR flight operations, a failure and top-down approach from the perspective of the aircraft operator is proposed, assuming that in normal conditions the acceptable level of safety is achieved by compliance of the safety requirements for all the system components. This is, demonstration of the safety criteria achievement in rare-normal and abnormal conditions is done by considering what could go wrong and affect the normal system, impair the aimed level of safety and identify where mitigating actions need to be considered by the operator to reduce the risk up to the acceptable level.
The methodology proposed is intended to be applicable to the following conditions:
Any type of AOC holder requesting the operational approval to perform public RNP-AR approach procedures.
Does not address procedure design and approval. It is considered that if the procedure was approved, compliance with the safety criteria has been demonstrated;
Does not address aircraft airworthiness certification.
RNP-AR approach procedures where more stringent aspects of the nominal procedure design criteria may be applied:
- RNP ≤ 0.3;
- RNP 0.1 missed approach;
- RF legs;
- RNP missed approaches with less than 1.0;
- Any aircraft type;

4.1 Step 1: System and safety criteria definition

System Definition

Section 3 provides a simplified description of RNP-AR approach operations. An extensive description can be found in ICAO RNP-AR, [10] and PBN, [2] manuals and EASA AMC 20-26, [6].
As per EASA AMC 20-26, [6] in normal conditions, the compliance of all the requirements provides an acceptable level of safety. Therefore for normal conditions, the FOSA is simplified to the demonstration of compliance of the requirements. However, the FOSA must assess the rare and abnormal conditions that have the potential to impair the TLS. For this reason, in order to assess the rare and abnormal conditions it is assumed that:
- Aircraft performance is capable of RNP-AR (default conditions) demonstrated by the Type Certificate holder;
- Aircraft airworthiness certification has been granted to the aircraft type;
- Aircraft equipment failure conditions probabilities are provided by the manufacturer;
- Maintenance, MEL, Dispatch and Approach procedures approved by the Aviation Regulatory Authority;
- Crew and Dispatch training approved;
- Navigation Database approved;

Safety Criteria Definition

The objective of the FOSA is to provide evidence that RNP-AR approach operations have been implemented to be acceptably safe. Demonstration of target level of safety achievement entails demonstration that the safety criteria is met: The risk collision per flight/approach ≤ 10⁻⁷ ⇔ the probability of the aircraft exiting the lateral and vertical extent of the obstacle clearance volume must not exceed 10⁻⁷ per flight hour.

This safety criteria encompasses qualitative and quantitative objectives. In order to promote standardization
of criteria and avoid developing one more set risk criteria, EASA CS-25, [4] failure conditions safety criteria will be used and applied to any type of hazard, either to an equipment failure or a human or organization failure – Table 1. Minor adjustments were made to the qualitative probability labeling for clarification purposes, this is: Extremely Improvable → Unlikely; Extremely Remote → Rare.

RNP-AR approach operations safety assessment requires input from 3 main areas: Systems Integrity, Aircraft Operations and Air Navigation Services. Due to lack of quantitative data from aircraft operations, it is not possible to assemble quantitative data from these areas, the demonstration that the probability of the aircraft exiting the lateral and vertical extent of the obstacle clearance volume must not exceed $10^{-7}$ per flight hour is achieved by demonstrating that each one of the potential contributing factors has an ’Acceptable’ level of risk, according to the risk acceptability criteria. Should any potential hazard have a ’Not-acceptable’ risk, mitigating actions need to implement to either reduce its likelihood of occurrence or its severity, or preferably reduce both risks’ components.

### 4.2 Step 2: Hazards Identification

Because for new operations, there are no observational data/historical records that can be used, a top-down approach analysis of each one of the sub-systems must be performed, in order to determine the failures and hazards that can impair each sub-system. This approach shall be performed by a team – Assessment team, where expertise, available at the AOC holder’s organization, from each of the contributing areas is represented. This team should aim to answer to the following questions: What can fail and how it can fail? From the analysis of the tools available that can assist the execution of this step, the following tools are identified as the most appropriate to use for new operations:

1) Identification of hazards provided in applicable regulatory documentation;

2) Functional Hazard Assessment brainstorming sessions: This session(s) should focus in identifying the hazards inherent to the AOC holder, such as organizational hazards and human factors related to organizational processes directly related to the stakeholders previously identified, and to the specific approach procedure to be flown, which cannot be predicted in the regulatory documentation due to its individuality, in addition to the generic hazards. This step should be conducted by a manageable group of experts, from all contributing areas, from the AOC holder which will be involved in the future operation. This type of brainstorming sessions was not conducted during this research, since no specific airport approach was under analysis.

The generic hazards applicable to any RNP-AR approach have been identified based on the analysis of the regulatory documentation applicable to any RNP-AR. In total 37 generic hazards have been identified, divided in six groups: Dispatch, Infrastructure, Aircraft, Flight Crew, ATC and Environment. Because an accident/incident is rarely to occur due to a single factor but rather due to a chain of contributing factors/hazards/errors, besides assessing each individual hazard, it is necessary to assess their synergy and its impact in the severity of the final outcome when compared to the outcome severity of a standalone hazard occurrence. In order to analyze the synergy between each two hazards, the Hazard Synergy Matrix was developed - Figure 2. The size of the matrix will be N x N, where N is the number of all generic hazards identified. The synergy of reoccurrence of the same hazard is excluded.

### How to use the Synergy Matrix:

Start reading the matrix in the vertical scale and for each hazard analyze the synergy between its occurrence followed by the occurrence of each one of the hazards in the horizontal hazard scale. For each synergy the appropriate impact in the consequences must be selected, this is the impact on the outcome severity, according to the following criteria:

- **R** – Reduced
- **N** – Not impaired/No change in the severity
- **I** – Increased

For example: The occurrence of hazard 1 accounts for certain consequences and a respective severity. Assuming the occurrence of hazard 1 is followed by the occurrence of hazard 2, the resultant consequences and respective severity will increase/decrease or not be impaired due to the occurrence of hazard 2 when compared to the standalone severity of hazard 1 occurrence?

If two hazards synergy analysis reveals that the severity will increase this represents a new hazard and its severity and likelihood must be assessed in addition to the individual hazards. This represents the potential of
assessing an additional number of new hazards to the generic hazards, resultant from their synergy analysis – Combined hazards. A second hazard synergy and subsequent matrixes have to be performed until the hazards synergies have reached a status where the operator feels comfortable to disregard consecutive possible combinations, based on a low likelihood of occurrence. Therefore a safety assessment may require the analysis of a large number of hazards, resulting in a high-time-consuming and cumbersome manual process.

It was requested to 14 experts from a Business Jet Operator which aims to request RNP-AR operational approval in a near future, to analyse the synergy of the 37 generic hazards. This group accounted expertise from the following areas: Flight Crew – Flight Operations, Flight Crew Training, Dispatch, Maintenance and Safety (accident/incident investigation expertise). At the time of production of this report only 4 answers had been received. Chart 1 presents the summary of the synergy analysis results per expertise. The different results substantiate the subjectivity of the hazard analysis process. From the analysis of the results it is possible to conclude that the hazard synergy identification process is dependent of: individual area expertise, time available to perform the analysis, knowledge of the operation under assessment and knowledge of safety/risk assessment processes (especially of what a hazard is).

In the absence of identical answers from all key informants and in order to decide either or not the synergy needs to be considered as an additional hazard, it is necessary to perform statistical analysis to the answers received for each possible synergy. The acceptability synergy criteria used is presented in – Table 2. For the case of RNP-AR, the statistic analysis of the key informant synergy answers revealed 558 synergies to be considered - Chart 2. A total of 595 hazards have to be assessed. Should a different group of experts had been used, then the result most probably would have been different.

**Table 2 – Synergy criteria for hazard consideration**

<table>
<thead>
<tr>
<th>Severity Increases (I) - % of Answers</th>
<th>Disregard synergy</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤ 50% of the answers</td>
<td>Consider hazard</td>
</tr>
</tbody>
</table>

The hazards identified in this step represent all the conditions that need to be accounted for rare and abnormal conditions and that have the potential to impair the TLS.

**4.3 Step 3 and 4: Hazard Severity and Likelihood Estimation**

Each one of the hazards must be analysed in order to identify what is its potential consequences and likelihood of occurrence, and classify respectively its severity and likelihood according to the risk classification criteria. A proper assessment of the hazard consequences requires the consideration of the one of ARMS concepts highlighted by ARMS work - recoverability, i.e. once a hazard occurs what is currently in place to recover from the potential consequence, worst case scenario a catastrophic accident. Due to the hazards nature, its analyses was divided in two main groups:

- **Aircraft Failure Hazards** – Considered during the aircraft airworthiness certification, therefore the severity and likelihood should be extracted from the regulatory documentation or from the supporting documentation to be provided by the manufacturer, once it was responsible for conducting the SSA for the airworthiness approval.
- **Human Factors and Environment Hazards** – No previous information or classification is available regarding these types of hazards, except the overall acceptance that they do constitute a potential hazard to the operation. Therefore the analysis of these types of hazards is subjective to the individual knowledge and experience because it is very difficult to accurately identify a single severity and likelihood classification due to the uncertainty of occurrence. For this reason, the following approach is proposed: Brainstorming sessions with experts, who have participated in step 2. The aim of these brainstorming sessions is to identify the potential consequences of each hazard and its classification in terms of severity, according to the risk acceptability criteria. Once more it is highly advantageous to have experts from all the areas under consideration. Depending on the expert group analysis per hazard, one or multiple severities will be identified for
each hazard. Due to the lack of availability from experts to participate in this step, it was not possible to perform it. RNP-AR operations depend highly on airplane systems for integrity but the main challenge when performing the RNP-AR safety assessment is the relationship between the airplane systems and the human interactions/human error. Furthermore the latter is in fact the larger contributor to the impairment of the safety level of the operation and the contributor with the highest level of uncertainty. Therefore the main challenge lies in the identification of the likelihood of occurrence of these types of hazards.

Due to the lack of availability from experts to participate in this step, it was not possible to perform the brainstorming sessions. Therefore the results presented below are only examples produced with the sole purpose to exemplify the expected type of results - Table 3.

4.4 Step 5: Risk Estimation

The main challenge of the safety assessment is the calculation of the risk level and demonstration that the safety criteria is achieved, this is, the calculation of the risk index for each one of the hazards identified. As identified in step 3, for non aircraft failures a single or multiples severity classifications were identified per approach, the same occurs for the likelihood of occurrence where an interval(s) of occurrence was identified - both risk components results can be represented as probability distributions. Therefore the risk analysis will output a range of possible risk levels, instead of a single value. The results of the risk analysis per hazard shall be recorded in a Safety Assessment Log - Table 3.

According to the risk classification criteria the risk of ‘Loss of all navigation information during flight’ is uncertain, it can either be ‘Not acceptable’ or ‘Acceptable’. As already referred the purpose of the safety assessment is to identify the safety level associated to a specific action/operation through the identification of the expected risk(s), by providing guidance to the decision-making roles in order to either accept or not the risk(s) to which the operation is expected to be exposed. So, what should be decided regarding this hazard’s risk level? Is the information provided sufficient to support the decision making-process? Two approaches can be used in order to answer to these questions:

- A conservative approach - select the higher risk level obtained. If ‘Not Acceptable’, implement corrective measures and reassess the residual risk until it achieves an acceptable level. Disadvantages of this approach are related to unnecessary costs and business implications.
- Obtain complementary information to support the risk decision making process, in order to ensure a higher confidence level when deciding the risk level. This is only possible through the use of a different risk estimation method. Due to the variability and uncertainty of the parameters, severity and likelihood, a probabilistic approach can be used. Additionally due to the high number of hazards to be analyzed, it becomes an arduous task to perform the risk estimation manually. It is therefore advantageous the use of a mathematical tool to support the risk analysis process, by facilitating the quantitative method for assessing the impact of risk decisions and determining all possible outcomes for each hazard. Based on the tools presented in section 2, it is recommended the use of @Risk from Palisade to support the risk analysis and decision making process regarding risk acceptability or not. This software uses Monte Carlo techniques simulation to provide an iterative process that recalculates spreadsheets hundreds of times based on the @Risk functions entered.

### Table 3 - Safety Assessment Log (examples)

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Loss of all navigation information during flight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequences</td>
<td>The crew loses the capacity of monitoring the aircraft position. Looses the capacity of monitoring deviations. Vertical and/or lateral deviation from the intended flight track; Loss of obstacle and terrain clearance</td>
</tr>
<tr>
<td>Current recoverability defence(s)</td>
<td>Abandon the RNP approach and divert if possible. Visual obstacle and terrain clearance. ATC support.</td>
</tr>
<tr>
<td>Severity</td>
<td>Catastrophic / Hazardous</td>
</tr>
<tr>
<td>Likelihood</td>
<td>Unlikely - 1x10⁻⁹ &lt; Probability &lt; 1x10⁻⁷</td>
</tr>
<tr>
<td>Current Risk Hazard</td>
<td>‘Not acceptable’ and ‘Acceptable’</td>
</tr>
<tr>
<td>Consequences</td>
<td>The crew loses the capacity of monitoring the aircraft position. Looses the capacity of monitoring deviations. Vertical and/or lateral deviation from the intended flight track; Loss of obstacle and terrain clearance. Incorrect speed and altitude information.</td>
</tr>
<tr>
<td>Current recoverability defence(s)</td>
<td>Abandon the RNP approach and divert if possible. Visual obstacle and terrain clearance. ATC support.</td>
</tr>
<tr>
<td>Severity</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Likelihood</td>
<td>From INF1: Unlikely - 1x10⁻⁹ &lt; Probability &lt; 1x10⁻⁷ From FC3: Remote - 1x10⁻⁷ &lt; Probability &lt; 1x10⁻⁵ - Probable - 1x10⁻⁵ &lt; Probability &lt; 1 Synergy likelihood: Rare / Unlikely</td>
</tr>
<tr>
<td>Current Risk</td>
<td>‘Acceptable’ and ‘Not acceptable’</td>
</tr>
</tbody>
</table>
4.5 Step 6 and 7: Risk Acceptability and Safety Assessment Documentation

Once the risk level or distribution is estimated, it needs to be compared to the pre-set target level of safety by regulations and to the safety criteria used - Table 1. Should the risk fall within the non-acceptable range, operation must not commence prior to the implementation of mitigating measures and reassessment of the residual risk until it achieves an acceptable level.

The prime driver of the need to perform a FOSA is the demonstration to the Aviation Authority that the safety requirements are met. Therefore it is extremely important that all safety assessments steps are properly recorded and made available to the Aviation Authority. A Safety Assessment Log shall compile the results from steps 2 to 6.

4.6 Monitoring Proposal

As per AMC 20-26, [6], the operational approval requires the aircraft operator to implement a RNP-AR monitoring programme to ensure continued compliance with the guidance provided by collecting data periodically and analyse it in order to identify any negative safety concerns and trends in operational performance, for a minimum period of 90 days – considered an interim approval period.

This main purpose of this monitoring program is to assess if current safety level of the operations and if additional mitigating measures are necessary to reduce the risk up to an acceptable level.

The information to be collected is presented in AMC 20-26, [6]. Based on this requirement, AOC holders can establish their monitoring program using one or two sources of information:

- The use of a RNP-AR Monitoring Form that shall be filled by the crew after each RNP-AR approach procedure completed. The data collect through this form shall be systematically analysed in order to identify any negative trends related to the procedure performance. The safety reporting system, as required by EU-OPS 1.420 and hazard identification methods used by AOC holder are considered appropriate mechanisms for the data collection and respective analysis.

- Flight data analysis, through the Flight Data Monitoring (FDM) program. This source of information provides more accurate and realistic data. However, once this is only mandatory, per EU-OPS 1.037, to have in place for aircrafts with a maximum take-off mass higher than 27000kg, some AOC holders may not have this program in place and its implementation requires a significant financial investment.

5. Conclusions

Investigation revealed that safety assessment and risk assessment expressions are widely used in the aviation industry across the world as processes to assess the safety and/or risk level of operations, but there is a lack of terminology, standardization and understanding regarding these two approaches and their differences. Many differences have also been identified regarding safety and risk definitions. Analysis of the different meanings for safety and risk assessment used by different stakeholders revealed that none of them intends to be prescriptive, rather to provide guidance regarding acceptable methods that can be adopted and adapted to systematically manage safety in a rational and thoughtful way, independently of the environment being assessed. These two approaches share the same purpose and goal and what sets the distinction between the two is their applicability, i.e. a safety assessment is applied to a new system/operation while risk assessment is applied to a known or on-going operation. If a safety assessment and a FOSA share the same objective, i.e. demonstrate that the acceptable level of safety of an operation is met (target level of safety, as per EASA AMC 20-26, [6]), according to a pre-set safety criteria and both are to be applicable to a new operation, than a FOSA methodology should be no different from a generic safety assessment methodology, having per basis the 7 step process safety assessment widely accepted at the aviation industry.

All types of hazard and risk identification tools analyzed are time consuming and require the participation of subject matter experts, the more the better as the more reliable the results will be. It is concluded that independently of the tools selected safety and risk assessment will always be a subjective assessment, highly dependent of the expertise of the participants, due to the inexistence of historical data for the hazards, their likelihood of occurrence will be identified based individuals judgments. The larger the representation the better because, more data will be available for identifying the distributions and thus the higher the confidence level in the results is. For the execution of the three main steps and in order to benefit from the resources, experience and expertise available at the majority of the aircraft operators, from a practical and finance perspective, for the case of RNP-AR the use of key informant technique, brainstorming sessions and Excel software from Microsoft Office was selected.

Because an accident rarely occurs due to a single factor but rather due to a chain of contributing factors/hazards/errors, besides assessing each individual hazard, it is necessary to assess their synergy and its impact in the severity on the final outcome when compared to the outcome severity of a standalone hazard occurrence. In order to assist this step the concept of ‘Hazard Synergy Matrix’ was created.
Another challenge identified for the case of RNP – AR is the establishment of a numerical relationship between the probability of occurrence between the hazards resultant from the airplane systems integrity, air navigation services and the human interactions/errors, due to lack of quantitative data from aircraft operations. Furthermore the latter is in fact the larger contributor to the impairment of the safety level of the operation and the contributor with the highest level of uncertainty. Therefore the main challenge lies in the identification of the likelihood of occurrence of these types of hazards. The demonstration that the probability of the aircraft exiting the lateral and vertical extent of the obstacle clearance volume must not exceed $10^{-7}$ per flight hour is achieved by demonstrating that each one of the potential contributing factors has an ‘Acceptable’ level of risk, according to the risk acceptability criteria. Should any potential hazard have a ‘Not-acceptable’ risk, mitigating actions need to implement to either reduce its likelihood of occurrence or its severity, or preferably reduce both risks’ components. Because the safety assessment steps that drive the safety assessment are dependent of expertise inputs and consensus most probably will not be achieved between all the participants and due to the high number of hazards, it becomes an impractical task to perform the risk estimation manually. Due to the variability and uncertainty of the parameters, severity and likelihood, a probabilistic approach must be used. It is therefore advantageous the use of a mathematical tool to support the risk estimation process, by facilitating the quantitative method for assessing the impact of risk decisions and determining all possible outcomes for each hazard. The use of @Risk, from Palisade, is recommended to support the risk analysis and decision making process regarding risk acceptability or not.

It is important to understand that a safety assessment tool itself does not guarantee a safe operation. It is only an additional tool to help the Aircraft Operator and the Aviation Regulatory Authority to make sound safety decisions in order to demonstrate that the safety criteria is met. Operational safety is a shared responsibility between all stakeholders.

References


Acknowledgements

I would like to thank Profª Rosário Macário, for her assistance in providing me direction and continuous technical support, encouragement and patient, despite the challenges this research has experienced. Sincere thanks to Paulo Pestana, Nuno Aghdassi, Marco Pereira and Erik Verheijden, for their continuous support and enthusiasm for this research and for devoting their precious time in performing the hazard synergy matrix exercise.