Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P240-cd

Risk analysis for in-flight refueling missions between a jet-powered aircraft and helicopters

Daniel Rondon Pleffken

Aeronautics Institute of Technology, Brazil. E-mail: rondon@ita.br

Moacyr Machado Cardozo Júnior

Aeronautics Institute of Technology, Brazil. E-mail: moacyr@ita.br

Rodrigo Mendes Cordeiro
Aeronautics Institute of Technology, Brazil. E-mail: mendesrmc@fab.mil.br

Alexandre Cantaluppi Silvestre Freitas
Aeronautics Institute of Technology, Brazil. E-mail: cantaluppiacsf@fab.mil.br

Paulo Hamasaki
Aeronautics Institute of Technology, Brazil. E-mail: hamasakipa@gmail.com

Christopher Shneider Cerqueira

Aeronautics Institute of Technology, Brazil. E-mail: chris@ita.br

Since the beginning of military aviation, the development of projects and their operation associated with innovation and the assumption of a certain degree of risk. One example was the development of projects capable of carrying out the in-flight reconfirmation operation (REVO). In order to remain at the forefront of international aviation, Brazil invested in developing a jet aircraft capable of performing REVO with helicopters. In this context, the present work focuses on the risk analysis of the REVO operation, based on Safety II, through the Functional Resonance Analysis Method (FRAM). A model is presented from the perspective of Safety I, applying the bow tie and risk matrix techniques to compare and discuss with the Safety II approach. Finally, it was possible to notice that the safety I approach has relevant techniques regarding component failure and automated procedures. However, Safety II complements the analysis, especially when it involves sociotechnical systems, where human and organizational factors are prominent in operation success. In this sense, the two approaches are complementary and can be used in other similar contexts: modern medicine, machine operation, air traffic management, and others.

Keywords: In-flight refueling, FRAM, risk analysis, Safety I, Safety II.

1. Introduction

In 1964, the US Air Force designated its Search and Rescue service, the Air Rescue Service (ARS), responsible for combat rescue during the Vietnam War. ARS' area of responsibility covered 1.1 million square miles, including South Vietnam, North Vietnam, Cambodia, Laos, Thailand, and the Gulf of Siam. Colburn (1997).

Given the low autonomy of the old Kaman HH-43 helicopters, from 1965, new Sikorsky CH-3C helicopters were used, with more incredible speed and range of up to 250 nautical miles. Despite their greater autonomy, rescue personalities exceeded the range of helicopters.

Based on the operational requirement of rescue over long distances and the inherent need to execute the mission quickly, considering that it is a combat operation, the US Air Force began the development of in-flight reinforcement (REVO) between HC-130 and its HH-3 helicopters, an evolution of the CH-3C.

Currently, in-flight refueling is carried out by several rotary-wing aircraft within the United States Armed Forces, including the HH-60 Blackhawk, which is constantly being supplied by versions of the KC-130 refueling aircraft.

In addition to the United States, Airbus has developed in-flight refueling in its version of the

EC225M helicopter, which is compatible with the KC-130J and the Airbus A400M.

Concerning in-flight refueling with helicopters within the Brazilian scenario, a contract was signed in 2008 for acquiring 50 EC225M helicopters with the consortium Helibras and Airbus Helicopters, whose objective was to equip the Brazilian Navy, Army, and Air Force. Among the purchased configurations is the Operational FAB version with a capacity forecast for in-flight refueling. Paula (2022).

Currently, in-flight refueling with helicopters is a reality in the Brazilian Air Force, operated by the pair KC-130H and EC-225M, being used not only in training for combat rescue missions but also in order to increase the range in rescues over land and sea.

1.1. *Future perspectives of REVO with helicopters*

The Brazilian Air Force acquired the KC-390 Millenium aircraft, a multi-mission transport aircraft whose in-flight refueling capability includes fighter aircraft and helicopters.

Considering that, at present, all tanker aircraft capable of REVO helicopters have turbo-propeller engines, the development of REVO with helicopters from a jet aircraft is a challenge whose risks are even more significant.

The influence of aerodynamic flow, both from the wing and the hot gases from the engine, can affect the controllability of the helicopter. In addition, there are risks related to the proximity between the refueling basket and the rotor disk and the high fuel flow, which may be greater than the physical resistance of the pipes that make up the receiver's tank. Such situations constitute risks that must be anticipated, mitigated, and measured in terms of consequences and severity.

Thus, this study aims to identify and analyse potential risk situations during the in-flight refueling manoeuvre between EC225M aircraft and the new KC-390 Millenium, both from the Brazilian Air Force.

Considering that the system under analysis is highly complex, the main risk conditions will be studied, thus making it possible to extend this evaluation to the other aspects to be identified.

Risk analysis is present in most people's daily lives, as there are almost no risk-free activities, even more so when it comes to events of considerable uncertainty, as is the case of REVO with helicopters from jet aircraft.

2. Risk analysis from the perspective of Safety I

The Safety I risk analysis tools lists potential events for a given activity, assigning the causes and consequences. It is, in general, an analysis based on linear structures where the line of events is well defined.

One can cite methods such as Brainstorming, Delphi, and Hazop to identify the events. The first consists of meeting with specialists to conduct an on-site survey to identify the most significant possible number of hazards; after all, unidentified risks are not analysed and deliver a super optimistic perspective on the situation under analysis. Smith (2008). Delphi is similar to Brainstorming, but opinions are collected anonymously, inhibiting the formation of dominant groups in the discussions but requiring more time to conduct and solid engagement of all involved. Yoe (2019). Hazop is a tool that facilitates the identification of risks using guidewords, evaluated at each stage of the activity under analysis.

To identify the causes and consequences, Fault Trees, Event Trees, and the technique known as Bowtie can be used. The latter presents the events pictorial, similar to a tie, where the causes and consequences are linked to the main event. The technique also suggests inserting containment and mitigation barriers, already treatment methods linked to the event.

One of the most famous Safety I techniques is the risk matrix. This tool assigns degrees of probability and impact to events to cross this information and arrive at a risk magnitude result. Thus, the manager will be able to identify the most critical events and prioritize approaches and means of treatment. It is a relatively easy method because its essence is the attribution of qualitative degrees. This requires a certain degree of attention on the part of managers, as it allows for reaching results with a low degree of reliability. In this sense, it points out the importance of the manager knowing the knowledge base in which a specific event classification occurred. Tegen (2016).

Within the context of the topic addressed in this article, a risk analysis involving the combination of Safety I techniques was carried out to present a comparative basis with the Functional Resonance Analysis Method (FRAM). Through a Brainstorming involving pilots from the Institute of Research and Flight Test (IPEV) of the Brazilian Air Force (FAB), a risk event related to the REVO mission was chosen, raising its possible causes and consequences and proposing barriers to containment and mitigation. Thus, it was possible to assemble a Bowtie, as shown in Figure 1.

Figure 1. Bowtie referring to the event: Loss of Control in Flight.

Subsequently, the event was classified based on the Risk Matrix shown in Figure 2.

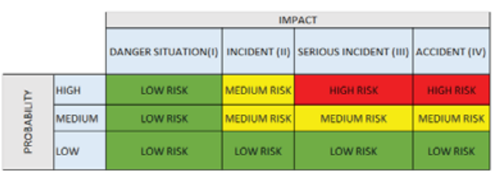


Figure 2. Risk Matrix used in the event analysis: Loss of Control in Flight.

By crossing the data assigned to Probability and Impact, this matrix expresses the magnitude of the risk the Organization is willing to assume. Thus, Table 1 presents the result obtained.

Table 1. Analysis of the Risk of Loss of Control in Flight using the Matrix in Figure 2.

EVENT	Loss of Control in Flight	
PROBABILITY	**IMPACT**	**MAGNITUDE**
High (3)	Accident (IV)	High risk

In general, risk analysis from the perspective of Safety I end up demanding a great effort to think about hypothetical scenarios that lead to the occurrence of risk events and their consequences. Depending on the evaluated event, such an approach becomes impracticable, requiring an endless list of possible causes and consequences.

Safety I techniques are solid and recommended for purely technological events where there is no influence of human action. In these cases, it is possible to arrive at reliability values and probabilistic calculations that would allow a safe analysis, with adequate attribution of the degree of knowledge of the data, which can be high. As for events involving social issues related to activities that require human actions, the Safety II approach appears.

3. Risk analysis under the perspective of Safety II

Recently, technological evolution and the continuous growth of its users within a sociotechnical context have made the systems too complex to establish Cartesian relations for all accidents. This complex systems approach is characterized by Safety II, which is more in-depth and is preceded by the analysis of Safety I.

Before, in Safety I, there was a concern about describing the system as a whole to make it traceable in terms of having mapped all possible scenarios for a failure. Already in Safety II comes the understanding that adopting such a procedure will only sometimes be possible. On many occasions, there will be a need to analyse innovative systems to the point of being unknown in certain respects. When considering sociotechnical systems, the level of unpredictability tends to increase since human action involves psychological and emotional issues that can impose variability in how tasks are performed.

In this way, Safety II will seek to understand how the system works on a day-to-day basis, describing the associated functions for its operation and looking for ways to improve the capacity for monitoring, anticipating, and responding to deviations. It is understood that various functions will not necessarily imply a system failure, as the people involved can adapt, promoting a return to normal conditions. In this sense, there is no interest in knowing whether the function will vary but whether this variation will be enough to destabilize the system and lead to its collapse. Hollnagel (2012).

Concerning the system in the focus of this work, it is noted that there is a strong tendency to have gaps in knowledge, as there is no database of previous experiences since it is an unprecedented event worldwide of an in-flight refueling involving a helicopter and a turbofan aircraft. There must be a concern not only in the components' functioning in isolation but also considering a dynamic system, where the materials may be exposed to extreme and unusual conditions, especially when considering their fatigue life. An example of this is the exposure of helicopter blades to exhaust gases from the aircraft turbine under high temperatures and turbulence.

There is also a strong presence of the social aspect since the pilots, both the helicopter and the tanker aircraft, perform most of the system's functions. For these reasons, we sought to apply the FRAM model, which is based on the principles of Safety II.

4. Model description

Initially, it is necessary to understand the variability of human performance involved in the process to act in favour of accident prevention. Macchi (2010):

> People are the primary source of performance variability in sociotechnical systems. The technology is designed, built, and maintained to be reliable. Technological progress produces extremely reliable systems in which variability can almost be forgotten. This does not mean that technology cannot fail; it does, and accident analysis often identifies technological failures. It just means that the technology works in a bimodal way, which means "it works" or "it does not work." It usually works and rarely fails; when it does, humans must deal with and adjust to a critical situation. Thus, describing performance variability is inevitably a matter of describing human performance.

In order to identify the various stages of the in-flight refueling manoeuvre, their dependencies, and the inherent variability of performance, modelling using the FRAM Visualizer software was used. For this purpose, an interview was conducted with a pilot with experience in the referred manoeuvre, who can detail the systematic from the pre-take-off planning through the aircraft assembly to the connection, fuel transfer, disconnection, and separation of the formation.

For each specified function, all relevant aspects were surveyed, in addition to input and output, as well as the necessary preconditions, resources, and, when relevant, controls and temporal involvement.

5. Results and Discussions

The modeling was comprehensive, with several background functions to capture the operation's socio-technical aspect. The "communicate" activity stood out in front of the others, with 18 adjacencies. This first finding already highlights that the Safety I tools are less effective than the Safety II ones in identifying and evaluating human functions.

An evaluation considering the possibility of varying all inputs and outputs of all activities would generate a complex combinatorial problem and escape the intended scope of this work, despite opening the way for future analysis. This article aims to demonstrate an analysis from the perspective of Safety II. Therefore, the variability of the "communicate" function was considered throughout the system, based on the premise that the other functions remain in a steady state.

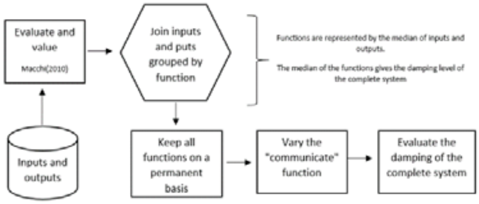
The variability of the inputs and outputs of all activities was evaluated and quantified similarly to that presented by Macchi (2010) and exemplified in Table 2. It is emphasized that each input and output is evaluated individually.

Table 2. FRAM model with "communicate" function highlighted.

Authorization for pre-contact		Temporal characteristic					
		Too early		In time		Very late	
Precision	Accurate	a	2	b	3	c	-2
	Appropriate	d	1	e	2	f	-2
	Inaccurate	g	-1	h	-2	i	-3

The level of damping for each function is determined by the median of the inputs and outputs. Additionally, the system damping is determined by the median of all the functions. Figure 3 presents a flowchart of how the data treatment was carried out in a generic analysis.

Figure 3. Analysis flowchart



The last three activities of the flowchart, represented by Figure 3, were executed in different interactions to generate results with the various damping combinations and to evaluate the system's sensitivity to the different damping values of the communication function.

Table 3 presents the results of different damping combinations. The first column represents the damping regime of the activities listed in the FRAM model, where the system indicator represents the function varies according to Table 2. To exemplify, the cell with the text "System A" represents the regime in which all the functions, except "communicate," with the entries in regime "a" of Table 2, which represents actions "I need" and "Very soon." The second line represents the numeric variation of the "communicate" function. The intersection of rows and columns represents the result of the combination of variabilities.

The term damping used in system analysis is a quantitative way of measuring the degree of resilience of the system and the ability of operators to overcome unwanted situations. The system's damping levels can vary from +3 to -3, where negative values represent a risk that operators will not be able to manage the combination of variability, and the system will enter into resonance.

Table 2 presents a comprehensive elucidation of the specific regimes associated with each function in the FRAM model. In contrast, Table 3 serves to exemplify the outcomes derived from diverse combinations of damping levels, aligning with the aforementioned regimes identified in Table 2.

Table 3. Results of different damping combinations.

Damping	Communication					
System A	3	3	3	3	3	3
System B	3	3	3	3	3	3
System C	2	2	1	1	1	1
System D	2	2	1,7	1,7	1,7	1,7
System E	2	2	1	1	1	1
System F	-1	-1	-1	-1	-1	-1
System G	-2	-2	-2	-2	-2	-2,7
System H	-2	-2	-2	-2	-2	-2
System I	-3	-3	-3	-3	-3	-3
System BEH	2	2	1,2	1,2	1,2	1,2
System DEF	2	2	1,4	1,4	1,4	1,4
System EF	1,2	1,2	1	1	1	1
System EF2	0,9	0,9	0,9	-0,9	-0,9	-0,9

Continuing with the analysis of the results and interpretation of Table 3, it is noted that if the system is in regime "e," inputs "Appropriate" and "In time," the system still does not enter into resonance, no matter how bad the variability in the "communicate" function. Furthermore, adversely to the case mentioned above, a system in regime "f" inputs "Appropriate" and "Very late" after regime "e" remains resonant regardless of the variation of "communicate." Therefore, there was a need to expand the investigation and analysis of 'hybrid' systems were carried out, in order to narrow the search for the "sensitive point" in which the system ceases to be damped to enter into resonance.

Initially, the BEH system was idealized with a third of the functions in regime "b" and a third in "e." A third in "h" the system did not enter resonance, as well as for the DEF system and for the EF system, in which half of the functions are in "e" and the other half in "f." None of the three proposed hybrid systems presented a damping regime switching point.

A new system was idealized, the EF2 system, where two-thirds of the functions are in regime "f" and the rest in "e." A "sensitive point" was observed in this system, in which the system changes from damped to resonant due exclusively to the variation of the "communicate" function.

The first lesson learned in choosing a model based on Safety II lies in the modeling carried out using the FRAM method. It is possible to highlight the “communicate” function as central and interactive with several other stages of the in-flight refueling process, as illustrated in Figure 8. Such an approach would not be focused on when analysing the same manoeuvre in conventional approaches.

Once the importance of the communication function has been identified and, in the event of its degradation, the consequences on the other functions, it is possible to determine actions and delegate greater attention to standardization, quality, and clarity in communications, thus mitigating possible dangerous situations.

The importance of this conclusion is emphasized because, based on the model and the proposed analysis, if the activities associated with communication during REVO with helicopters are not treated with great attention, the system may enter into resonance and cause accidents, even without any activity occurs imprecisely and with part of them occurring at the correct time.

The study method applied here limited itself to degrading communication to the limit where it would be carried out in a delayed and imprecise manner. There was no point in evaluating the case in which the communication function was prevented from taking place since, in this situation, the manoeuvre would be interrupted.

Although communication is an essential object of briefings and planning for this type of operation, the Safety I analyses did not draw attention to the danger associated with this activity.

6. Conclusions

The present work contextualized the beginning of the operation and development of projects capable of in-flight refueling (REVO), emphasizing the importance of this use between airplanes and helicopters. This demand arose within the operational need to carry out long-range rescues.

As a study model, the originality of a REVO operation involving a helicopter and a jet aircraft was used. In general, it was noted that when applying Safety I, the team was required to think of an infinity of failure modes that the system could present. Thus, this approach proved to be more adherent to purely technological events, where the wide range of variability is less present, unlike events linked to human actions, which bring an associated unpredictability. The Safety II approach was employed to deal more adequately with the latter situation.

The modeling of the system using the FRAM method increased the situational awareness of the steps involved in the In-Flight Refueling mission, identifying how the functions interact. Special attention was given to the "Communicate" function, which was perceived as critical and influenced several other functions. Its variability has high interference in the system, which could hardly be noticed through the exclusive use of Safety I techniques.

Thus, identifying critical functions allows the analyst to prioritize security actions and dedicate more intense training. As in the case studied in this work, it was noted that even when no function is executed imprecisely, the system could become resonant and collapse.

Although the analysis by the FRAM method proved to be more favourable for the presented scenario, the Safety I techniques are still valid and can be used in a complementary way. This is especially true for events in which the purely technological factor predominates, such as the study of an engine failure.

Regarding presenting the results, it is noted that the Safety I techniques provide tools that favour understanding by readers who are not specialists in risk analysis. Decision makers are often not knowledgeable about specific techniques, so a pictorial presentation, such as a bowtie or risk matrix, facilitates understanding. Thus, as a suggestion for future work, one can evaluate models that facilitate the visualization of the results obtained in the resonance analysis and model the functions by the FRAM method.

Finally, another suggestion for future work is developing a program that allows evaluating the variability of different functions and working with an optimization process to identify critical paths. In this way, the analyst would have the combinations of specific regimes for each function in hand, which would lead to the worst scenarios. Having this knowledge would allow for prioritizing training actions and implementing more efficient barriers, all being thought of concerning "work as done" and focusing on the correct functioning of the system, the basis of Safety II.

References

Aérea, R. F. (27 de 08 de 2022). Fonte: https://forcaaerea.com.br/kc-390-e-certificado-pelo-dcta-para-missoes-de-revo/

Aeronaval, D. (27 de 08 de 2020). defesaaereanaval. Fonte: https://www.defesaaereanaval.com.br/aviacao/franca-realizou-o-primeiro-reabastecimento-em-voo-de-um-airbus-h225m-caracal-usando-o-a400m

Aven, T. 2016. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research. 253, 1–13.

Aviation, T. d. (27 de 08 de 2022). This day in aviation. Fonte: 1972, 12 april: https://www.thisdayinaviation.com/12-april-1970/

COLBURN, T. W. (03 de 01 de 1997). Running on Empty: The Development of Helicopter Aerial Refueling and Implications for Future USAF Combat Rescue Capabilities. p. 11.

FAB, F. A. (27 de 08 de 2022). www.fab.mil.br. Disponível em: https://www.fab.mil.br/noticias/mostra/24159/REAPARELHAMENTO%20%E2%80%93%20FAB%20recebe%20helic%C3%B3ptero%20capaz%20de%20reabastecer%20em%20voo%20e%20com%20sistema%20de%20autodefesa

HOLLNAGEL, E. FRAM: the Functional Resonance Analysis Method: modeling complex socio-technical systems. Ashgate. 2012.

MACCHI, L 2010. A Resilience Engineering approach for evaluating performance variability: development and application of the Functional Resonance Analysis Method for air traffic management safety assessment. Business administration. Ecole Nationale Sup´erieure des Mines de ´ Paris, 2010. English.

SMITH, Brian E.; DE JONG, Hans H.; EVERDIJ, Mariken HC. A prognostic method to identify hazards for future aviation concepts. In: 26th International Congress of the Aeronautical Sciences, ICAS. 2008.

Yoe, C. Principles of Risk Analysis: Decision Making Under Uncertainty. Boca Raton: Taylor and Francis, CRC Press; 2019.