

HUMAN RELIABILITY ANALYSIS IN AN AIRCRAFT DECOMPRESSION EVENT

Christianne Reiser, Alaide Bayma, Domicio Angelo da Fonseca
Embraer S/A

Keywords: *Human Error, Bayesian Networks, Fuzzy Logic, Risk Assessment*

Abstract

Human error contributes to around 70% to 80% of aeronautical accidents. To reduce this rate, an analysis of human reliability in the interaction between man and machine applying Bayesian Network and Fuzzy Logic is proposed. This paper presents an application of this approach in an aircraft decompression event, during a passenger's oxygen system failure to automatically deploy.

1 Introduction

Over the past 40 years, the number of aviation accidents attributable solely to mechanical failure has decreased markedly, while those credited at least in part to human error have declined at a much slower rate. Detailed and complete investigation of these accidents supports and improves safety levels. Some of them showed that many accidents contributors did not come from unknown technical conditions but resulted from the incorrect application of established techniques. As a consequence, current industry safety focus is the monitoring of potentially unsafe conditions in the day by day operation.

The analysis of fleet in service difficulties reports has been a key part of the formal Continued Airworthiness process, where manufacturers and operators are required to report to the Certification Authorities relevant failures, malfunction or defect of an aircraft or component [1]. This traditional way of fleet monitoring can be improved with a systematic process to identify and evaluate the safety risks related with the reports. The core of this process is the risk analysis and assessment. There are

different interpretations and applications for a risk assessment, but the root idea is the same - risk is the combination of severity and likelihood. Interventions like that aimed to reduce the occurrence or consequences of technical failures and are based on its failure rate [2].

Human error has not been treated so directly. Methods based on, for example, the Reason's 'Swiss Cheese' Model has had particularly large use in the analysis of accidents that already occurred, revealing a need for safety improvements at the organizational and supervisory level to equip pilots with the resources and ability to perform their tasks in a safer manner. It does not provide much insight into the errors within the process and their interactions.

Human error has been implicated in a variety of occupational accidents, including 70% to 80% of those in civil and military aviation. It involves humans that, in the course of doing their work, make errors that are later shown to have caused, or substantially contributed to the accident. These are human actions that, if done correctly, result in a safe outcome, but if done incorrectly, can result in an accident. Mechanisms to anticipate the contribution of human error to the overall reliability of a given technical system is not straightforward, since it can be difficult to trace the sequence of causality from human error through system failure. Consequently, preventive risk assessment still has significant limitations in the area of human reliability analysis and organizational factors [3].

This paper proposes the inclusion of human error into a probabilistic risk assessment, which focuses nowadays on the quantification

of likelihood for technical failures. The process involves identifying potential human errors or successes, and quantifying their probabilities under unexpected emergency conditions, based on service difficulties reports.

2 Background

The primary mechanism to include the dimension of human error into failure analysis is Human Reliability Analysis (HRA), characterized by the sequence of steps present in Fig. 1 [4].

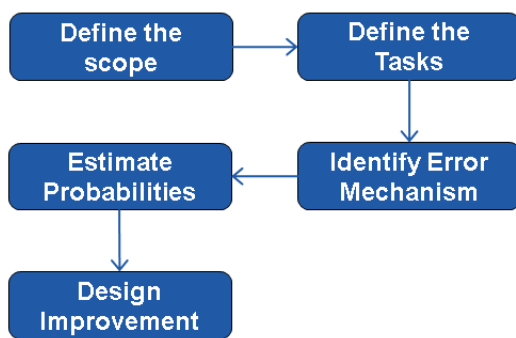


Fig. 1 - Human Reliability Analysis

Potential errors or successes, which are context specific, are identified by task analysis. Performance shaping factors are used to link human errors to other factors such as crew resource management, organizational culture, psychology factors, and individual cognition. A causal network with probabilistic dependency, a Bayesian network, organizes the knowledge about the error mechanism. All the conditional probabilities on the Bayesian network nodes are got by questions done to volunteers, submitted to a specific test, and by Fuzzy logic [5]. Details of the methodology are described below.

2.1 Performance Shape Factors

Performance Shaping Factors (PSFs) were proposed by Swain in 1983 upon the THERP (Technique for Human Error Rate Prediction) development, which is used for qualitative and quantitative analysis of human reliability [6]. PSFs are the human factors that affect human performance. As a large number of distinct factors influence the human being [7], a PSF selection must be done as follows:

- Only the PSFs with major impact shall be chosen.
- The factors must be independent from each other.
- A selected PSF should be measurable.

Among the PSFs in such a complex man-machine system, some are external to the person and others are internal. The external ones include the entire work environment, for instance, the cockpit design and the Quick Reference Handbook (QRH) influence over the flight crew. The internal PSFs represent the individual characteristics of the person - his skills, motivations, and expectations.

2.2 Causal Network

Human error mechanism is defined by his interaction with the equipment, procedure, or design and varies according to the person's characteristics, the environment, and the organizational management. A human error causal network describes the relationship among these components, as shown in Fig. 2 [5].

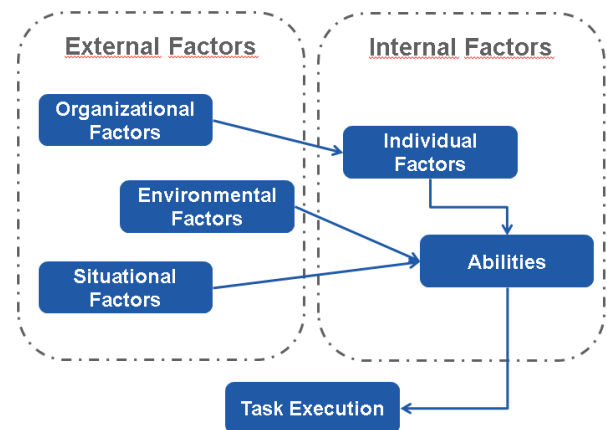


Fig. 2 – Proposed Causal Network

The PSFs are divided into external and internal factors as follows.

- Organizational factors are external, and are related to operational activities such as training, and standard procedures. They affect individual factors such as knowledge.
- Individual factors are internal. They define how the person reacts to the organizational inputs, and impact his ability to cope with the situation.

- Abilities like attention, perception, and decision-making are the direct cause of the human errors or successes. They are influenced by the individual factors as well as the situational and environmental ones.
- Situational factors are a consequence of the equipment design.
- Environmental factors indexes the influences of relative humidity, temperature, noise, visibility, and so on.

2.3 Bayesian Network

Bayesian Networks are then used to develop models which quantify the probabilities of human error, based on the causal network described above.

A Bayesian network is a probabilistic graphical model that represents a set of variables and their conditional dependencies via a directed acyclic graph. Nodes that represent discrete or continuous variables and arches that symbolize conditional dependencies compose the network. Parents are defined as the nodes that derive the arches, and a son node is the place where these arches arrive. Each node is associated with a probability function that takes, as input, a particular set of values for the node's parent variables, and gives, as output, the probability of the variable represented by it [8]. In summary, the son node probability is estimated using its parents' nodes probabilities and a conditional relationship.

For example, a network is composed by two parent nodes F_1 and F_2 (independent from each other), one son node V_1 , and a conditional probability $P(V_1/F_1 \cap F_2)$. Given the probabilities of parents nodes (F_1 , F_2), and the conditional probability of the son node (V_1), the probability distribution of son node is calculated by Eq. 1.

$$P(V_1) = \sum P(F_1 \cap F_2 \cap V_1) \quad (1)$$

$$P(V_1) = \sum P(F_1) \cdot P(F_2 / F_1) \cdot P(V_1 / F_1 \cap F_2)$$

The final probability of a Bayesian network with n son nodes is given by Eq. 2.

$$P(V) = P(V_1, V_2, \dots, V_n) \quad (2)$$

$$P(V) = \prod P(V_i | F_{\text{parents}}(V_i))$$

Where:

- V_1, V_2, \dots, V_n : son nodes;
- $P(V)$: total probability of network;
- $P(V_1, V_2, \dots, V_n)$: probability distribution of the network' nodes;
- $P(V_i / F_{\text{parents}}(V_i))$: probability of the node V_i occurrence, given the probability of its parents.

The conditional probabilities are calculated by Fuzzy Logic, while the parents' nodes probabilities are acquired by questions done to volunteers, who are submitted to a test.

2.4 Fuzzy Logic

Fuzzy logic is an approach based on "degrees of truth" rather than the usual "true or false", "yes or no", "low or high", and so on. Using this methodology, notions like too much or too fast can be formulated mathematically and processed by computers. This logic is based on the fuzzy set theory, which is defined as a collection of elements in an ambiguous, vague and diffuse universe of information [9].

Given a classical set $X \rightarrow [0,1]$, a Fuzzy set is characterized by its pertinence function as follows.

$$A = \{(x, \mu_A(x)) | x \in X\} \quad (3)$$

Where $\mu_A(x)$ represents the pertinence function, that quantifies the pertinence degree of elements x to the classical set X . The more used pertinence functions are: S-function, Gaussian, trapezoidal, triangular, and sigmoidal. The trapezoidal function (Fig. 3) was selected for this work, in order to achieve the conditional probabilities.

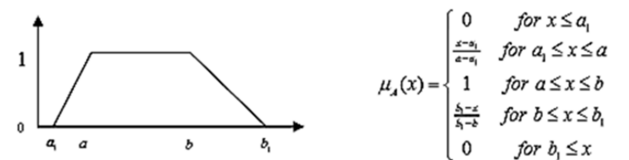


Fig. 3 - Trapezoidal Pertinence Function

To summarize, Fuzzy logic is performed by substituting ambivalent pertinence functions (0 or 1) by fuzzy pertinence functions that is defined in the interval $[0,1]$.

2.5 Human Reliability Diagnoses

The Bayesian network organizes the knowledge of the domain relating causes and consequences of the involved events, and combines causal and probabilistic knowledge (diagnoses).

Human reliability diagnose is then accomplished by a bottom-up inference process, based on the Bayesian network model. As the bottom layer of the model is the Task Execution, the human error probability of the case study is inferred from this node. The model is used to evaluate the sensibility of the human, being errors or successes, due to standard deviations, like technical failures [5].

After having the domain of events probabilities, the Bayesian network sensibility can be completed for updating a parent event (F) based on evidences of son node (V) probabilities. The updating of *priori probability* (P(F)) due to a son node probability (P(V)) evidence is known as *posteriori probability*. This relationship is termed as “Bayes Theorem” (Eq. 4).

$$P(F|V) = \frac{P(F \cap V) = P(F) \cdot P(V|F)}{P(V_i)} \quad (4)$$

2.6 Risk Assessment

Risk may be defined as the combination of severity and likelihood, and represented by a matrix (Fig. 4).

Likelihood	Severity				
	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Frequent	LOW	MODERATE	HIGH	VERY HIGH	VERY HIGH
Probable	LOW	LOW	MODERATE	VERY HIGH	VERY HIGH
Remote	LOW	LOW	MODERATE	HIGH	VERY HIGH
Extremely Remote	LOW	LOW	LOW	MODERATE	HIGH
Extremely Improbable	LOW	LOW	LOW	LOW	MODERATE

Fig. 4 - Risk Assessment Matrix Sample

Instead of using a matrix, the risk assessment procedure adopted by Embraer assigns a value for each Severity Classification and Likelihood Level, and use these values to calculate a Preliminary Risk Index (RI) as shown in Eq. 5 [2].

$$RI = \frac{\text{Severity}}{\text{Classification}} \otimes \frac{\text{Likelihood}}{\text{Level}} \quad (5)$$

Given a specific issue to be analyzed, the RI calculation consists of:

- Severity (S) and Likelihood (L) evaluation of the reported condition;
- Assessment of the conditions or failure combinations that may raise the reported condition severity (scenarios), anticipating its probability;
- Consideration of the highest S x L as the preliminary RI; which is the risk analysis result, and the reference for the issue prioritization.

Embraer risk assessment procedure takes the RBAC/FAR/JAR 25.1309 requirement as a reference, since the effects on safety of foreseeable failures are already performed during aircraft design and certification processes for this requirement accomplishment. The RBAC/FAR/JAR 25.1309 guidance also defines how the severity and likelihood shall be categorized (Fig. 5 and Fig. 6) [10].

Severity		Consequences		
		Airplane	Crew	Passengers
1	Minor	Slight reduction in safety margin or functional capabilities	Slight increase in workload	Some inconvenience
2	Major	Significant reduction in functional capabilities or safety margin	Significant increase in workload	Some discomfort
3	Hazardous	Large reduction in safety margins or functional capabilities	Excessive increase in workload	Adverse effects, like injuries
4	Catastrophic	Inability to continue a safe flight and landing	Fatalities	Multiple fatalities

Fig. 5 - Severity Classification

Likelihood		Average Probability per Flight Hour	Qualitative Description
5	Frequent	Greater than 10 ⁻³	Recurrent conditions that occurs many times during the operational life of each airplane.
4	Probable	From 10 ⁻³ to 10 ⁻⁵	Anticipated to occur one or more times during the entire operational life of each airplane.
3	Remote	From 10 ⁻⁵ to 10 ⁻⁷	Unlikely to occur to each airplane during its total life, but which may occur several times when considering the total operational life of a number of airplanes of the type.
2	Extremely Remote	From 10 ⁻⁷ to 10 ⁻⁹	Unlikely to occur when considering the total operational life of all airplanes of the type, but nevertheless has to be considered as being possible.
1	Extremely Improbable	Lower than 10 ⁻⁹	So unlikely that they are not anticipated to occur during the entire operational life of all airplanes of the type.

Fig. 6 - Likelihood Level

The likelihood for a reported condition is based on the occurrences rate, and for the scenarios, it is estimated by the combination of the individual probabilities that compose it.

As a proposal, the human error derived from the Bayesian network suggested above is used as one of the conditions that may raise a reported condition severity and/or likelihood. Namely, the flight crew may be seen as a part of

the airplane, and their failure is similar to a technical one.

3 Case Study

Most commercial aircraft that operate at high altitudes are pressurized at a maximum cabin altitude of approximately 8,000 feet. These aircraft have oxygen emergency systems, intended for use when the cabin pressurization system has failed, and the cabin altitude has climbed above a safe level. Without emergency oxygen, hypoxia may lead to loss of consciousness [11].

For a particular commercial jet aircraft, an oxygen system supplies oxygen to the crew members and passengers as follows.

- Flight Crew: provided through a sweep-on full-face crew mask, which can be donned with one hand in 5 seconds (Fig. 7a). It includes an oxygen cylinder.
- Cabin Crew/Passengers: chemically generated, and available for 12 or 14 or 22 minutes, depending on the customer aircraft configuration (Fig. 7b).

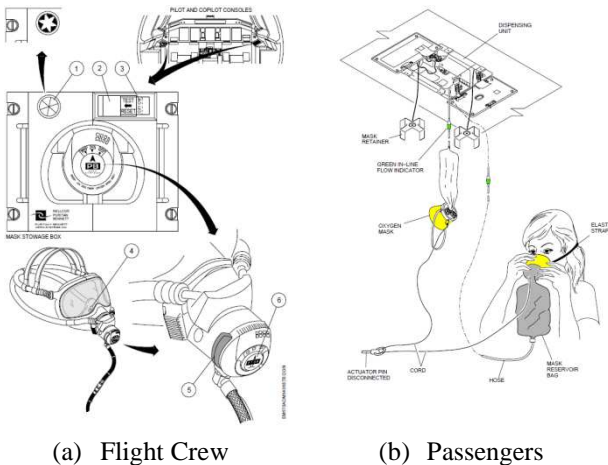


Fig. 7 - Oxygen System

In case of a cabin decompression, the warning message “CABIN ALTITUDE HI” appears on EICAS followed by an aural warning “CABIN” as soon as the cabin altitude reaches 10,000 feet. The flight crew shall don their oxygen masks and start an emergency descent to FL100, or the closest to that while maintaining the Minimum Equivalent Altitude (MEA). If the cabin altitude reaches the range of 14,000 to 14,750 feet, the compartments containing the

passenger oxygen masks open automatically, and the masks drop down in front of the passenger. Fig. 8 shows the procedure present in the QRH to address the “CABIN ALTITUDE HI” message.

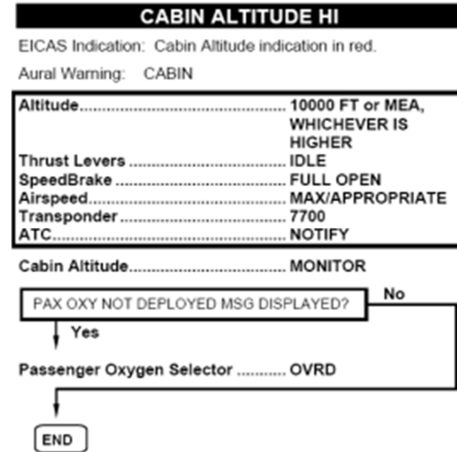


Fig. 8 - QRH Procedure

Where:

- “PAX OXY NOT DEPLOYED” is a caution message that informs the flight crew that the passenger masks did not automatically dropped down;
- The Passenger Oxygen Selector is located in the Passenger Oxygen system control panel (Fig. 9), and gives to the flight crew the option to manually deploy the passenger masks, or even prevent an automatic deployment (OFF position).

The passenger oxygen system panel also has a light called “MASKS DEPLOYED” that comes on when the passenger masks drop [12].

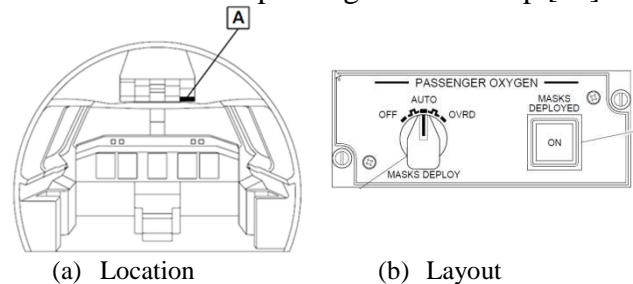


Fig. 9 - Passenger Oxygen System Panel

3.1 Scope and Tasks Definition

A case study was then accomplished to evaluate the “Bayesian Network with Fuzzy Logic Methodology” application during a cabin decompression followed by a non-annunciated

failure of the passenger oxygen automatic deployment system. In this case, the human success is being assessed.

According to the QRH procedure, the flight crew shall not deploy manually the passenger masks as the “PAX OXY NOT DEPLOYED” message does not appear on EICAS (non-annunciated failure). During the execution of the emergency descent procedure, the crew might notice that the “MASKS DEPLOYED” light does not come on in the passenger oxygen system panel. In this case, they will have a dual input from the aircraft and shall make a decision.

The questions raised for this study are:

- Will the flight crew notice that the passenger masks did not deploy?
- Will they deploy the masks manually?

3.2 Error Mechanism

The error mechanism is defined by the causal network shown in Fig. 2, and the chosen PSFs. Based on the tasks involved in this case study, the following factors were elected (Fig. 10).

Abilities	Individual / Situational / Environmental	Organizational
Attention	Individual: Fatigue	-
	Situational: Crew Coordination	Recurrent Training
Perception	Individual: Crew Oxygen Masks	-
	Situational: Knowledge	Recurrent Training
	Situational: “MASKS DEPLOYED” light	QRH Procedure
Decision Making	Situational: “PAX OXY NOT DEPLOY” message	Test Demonstrations
	Individual: Knowledge	-
	Situational: Crew Coordination	Recurrent Training
	Situational: Cabin Altitude	-

Fig. 10 - PSFs Modeled by Abilities

3.3 Probabilities Analysis

The Bayesian network is then traced (Fig. 11) with the GeNIe 2.1 Academic software. The roots' nodes probabilities are got by questions done to volunteers, who are submitted to a test or simulation. Son nodes conditional probabilities are acquired by Fuzzy Logic.

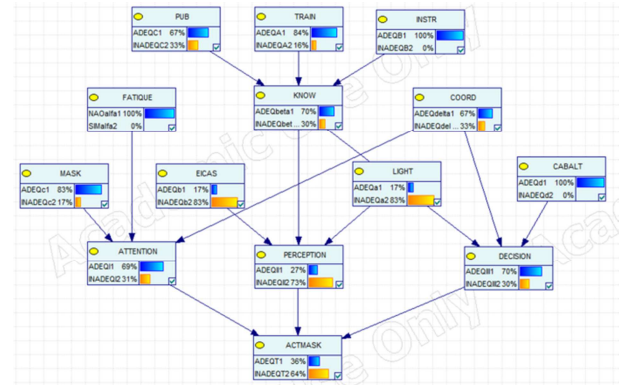


Fig. 11 - Bayesian Network of the Case Study

3.3.1 Simulation and Questionnaire

Simulation of the “cabin decompression followed by a non-annunciated failure of the passenger oxygen automatic system” event was performed on the Iron Bird. A total of 11 pilots were submitted to the test, resulting in 6 simulations. The test comprised the following steps.

- Cut out of both air conditioning packs while cruising at FL400. As a result, the cabin altitude starts climbing;
- Appearance of the "CABIN ALTITUDE HI" message on EICAS associated with its aural warning upon a cabin altitude of 10,000 feet;
- Exceedance of the cabin altitude 14,000 feet limit without the appearance of the "PAX OXY NOT DEPLOYED".

However, the passenger oxygen masks are not automatically deployed. This might be noticed only by the "MASKS DEPLOYED" light, that remains off.

After the test, the volunteers filled in a questionnaire, giving the Bayesian network roots' nodes probabilities. Questions such as “Do you consider the recurrent training adequate for an emergency descent procedure?” provide a probability for “Recurrent Training”. Even the “Crew Coordination” probability is based on the result of the question “Given that you are prepared to an emergency descent procedure due to your recurrent training, were the tasks between pilot and copilot well-coordinated?”

3.3.2 Fuzzy Logic

For nodes whose conditional probabilities are dependent of more than one parent probability,

the credibility of an answered question become unreliable. Consequently, a Fuzzy Logic with trapezoidal pertinence function is used to estimate the marginal priori probability of these nodes. For example, the conditional probabilities a priori of the son node "Perception" are presented in Fig. 12.

EICAS P(F ₁)	Know P(F ₂)	Light P(F ₃)	Perception P(V/F ₁ , F ₂ , F ₃)	
			P(V _{ok})	P(V _{nok})
P(F _{1,ok})=0.17 ADEQUATE	P(F _{2,ok})=0.70 ADEQUATE	P(F _{3,ok})=0.17 ADEQUATE	0.5	0.5
		P(F _{3,nok})=0.83 INADEQUATE	0.431	0.569
	P(F _{2,nok})=0.30 INADEQUATE	P(F _{3,ok})=0.17 ADEQUATE	0.202	0.798
		P(F _{3,nok})=0.83 INADEQUATE	0.323	0.677
P(F _{1,nok})=0.83 INADEQUATE	P(F _{2,ok})=0.70 ADEQUATE	P(F _{3,ok})=0.17 ADEQUATE	0.5	0.5
		P(F _{3,nok})=0.83 INADEQUATE	0.202	0.798
	P(F _{2,nok})=0.30 INADEQUATE	P(F _{3,ok})=0.17 ADEQUATE	0.255	0.745
		P(F _{3,nok})=0.83 INADEQUATE	0.202	0.798
		Result	0.27	0.73

Fig. 12 - Conditional Probability of the node "Perception"

3.3 Probabilities Analysis

Fig. 11 refers to Bayesian Network with the priori probabilities, where the human success in deploy the masks manually given additional technical failure is equal to 36%, while the human error is 64%.

The causal analysis starts by assuming that human error happened, such as task "Actuate Masks" 100% "Inadequate" (Fig. 14), the posteriori probabilities of all nodes are recalculated in accordance with the "Bayes Theorem" (Eq. 4), revealing the variable with more influence in this result – the "Decision" node (rating 13%)(Fig. 13).

NODES	"Attention"	"Perception"	"Decision"
"ActMask" 100% INADEQUATE	$\Delta = \frac{31-33}{31} = 0.06$	$\Delta = \frac{73-73}{73} = 0$	$\Delta = \frac{30-34}{30} = 0.13$

Fig. 13 – Probabilities Variation of the Abilities' Nodes

The causal analysis continues by considering that a poor decision making occurred, namely the ability "Decision" 100% "Inadequate". The individual factor related to the knowledge was the influencer one, differing 33%. The analysis ends when the "Know" node is deliberated to 100% "Inadequate", recognizing that "Train" is the organizational node with more impact. Namely, a training reevaluation is recommended.

As the focus of this study is "Perception", and this ability does not have any rating (Fig. 13), the "PAX OXY NOT DEPLOYED" message might not have a so direct influence in the human reliability, despite of being failed during the simulation accomplishment.

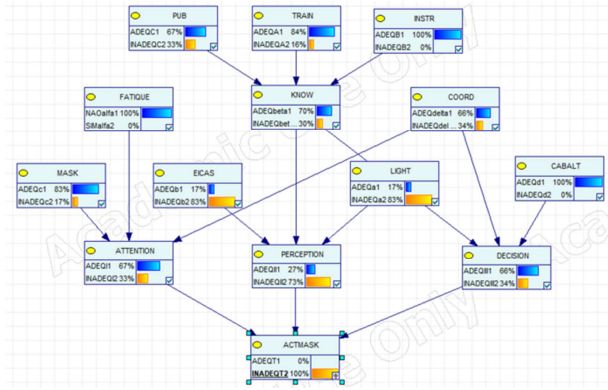


Fig. 14 - Bayesian Network after a Human Error

Even evaluating the node "Perception" directly, the changes in its parents' probabilities are slight, and the node "Light" is recognized as the key influencer. The "PAX OXY NOT DEPLOYED" message influence remains minor.

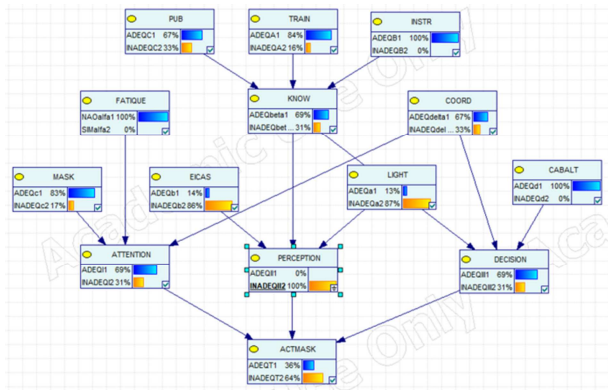


Fig. 15 - Bayesian Network after an Inadequate Perception

3.4 Results

The Bayesian Network with the priori probabilities shows that the "PAX OXY NOT DEPLOYED" EICAS message shall be functional to guarantee the human success during an event like that. Depending on the passenger oxygen automatic deployment system failure rate, the correct information regarding the masks condition is essential to prevent hypoxia among the passengers. For a risk

assessment, the severity of this scenario is associated with the system failure rate and the human error probability (equal to 64%).

Nevertheless, the cabin altitude indication is considered adequate, and monitored by the copilot. To deploy the passenger oxygen masks manually upon a cabin altitude of 14,000 feet despite of the automatism is trivial. Based on the network results and the influence of the “PAX OXY NOT DEPLOYED” EICAS message over the flight crew, shall the QRH procedure prevent that trivial task?

4 Conclusions

This paper practices a Bayesian Network approach to investigate the human reliability under unexpected emergency conditions. The analysis is based on Performance Shape Factors (PSFs) quantification, and explores the influence among human characteristics and also interactions. The integration among organizational, situational, and individual factors is quantitatively measured through the human reliability in executing a task.

The methodology is complex, very time-consuming, and its results are influenced by former assumptions. As a consequence, it must be used prudently, focused on issues that comprise relevant human actions or decisions. A human error may lead to an undesirable outcome, as well as his ability to make it right in adverse conditions may improve the aircraft safe operation.

References

- [1] 14 CFR 21.3 - Reporting of Failures, Malfunctions, and Defects. In: <https://www.gpo.gov/fdsys/granule/CFR-2002-title14-vol1/CFR-2002-title14-vol1-sec21-3>, accessed on June 05, 2018.
- [2] Irgang U, Pereira SR, and Catani F. *Risk Analysis and Product Safety Monitoring at Embraer*. IASS – International Air Safety Seminar, 59th, Paris, 2006.
- [3] Pons D, and Dey K. *Aviation Human Error Modelled as a Production Process*. The Ergonomics Open Journal, No. 8, pp 1-12, 2015.
- [4] Kirwan B, Ainsworth LK. *A Guide to Task Analysis*. Taylor&Francis, 1994.
- [5] Bayma A, and Martins MR. *Human Reliability Analysis in the Emergency Evacuation from an Aircraft*. European Safety and Reliability Conference - ESREL2017, Slovenia, 2017.
- [6] Swain AD, Guttman HE. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. NUREG/CR-1278, 1983.
- [7] Gawron VJ. *Human-Factors Taxonomy*. Guide written by members of a MORS working group and expanded by members of the Human Factors and Ergonomics Society, 2009.
- [8] *Bayesian Network*. In: https://en.wikipedia.org/wiki/Bayesian_network, accessed on June 05, 2018.
- [9] Mesquita RN, Nascimento CS. *Application of Fuzzy Methodology in the Quantification of Human Error Probability in the Nuclear Installation*. 2010.
- [10] FAA. *System Design and Analysis*. Advisory Circular AC 25.1309, 1988.
- [11] *Emergency oxygen system*. In: https://en.wikipedia.org/wiki/Emergency_oxygen_system, accessed on June 08, 2018.
- [12] Embraer. *Oxygen System Description Section*. Aircraft Maintenance Manual Part I, Revision 49, 2018.

5 Contact Author Email Address

christianne.reiser@embraer.com.br
 alaide.bayma@embraer.com.br
 domicilio.fonseca@embraer.com.br

Copyright Statement

The authors confirm that they, and/or their company or organization, hold copyright on all of the original material included in this paper. The authors also confirm that they have obtained permission, from the copyright holder of any third party material included in this paper, to publish it as part of their paper. The authors confirm that they give permission, or have obtained permission from the copyright holder of this paper, for the publication and distribution of this paper as part of the ICAS proceedings or as individual off-prints from the proceedings.