Chapter

Risk Assessment under Uncertainty

Rosa Maria Arnaldo Valdés,
Victor Fernando Gómez Comendador and Luis Perez Sanz

Abstract

System safety assessment (SSA) has become a standard practice in air traffic management (ATM). System safety assessment aims, through a systematic and formal process, to detect, quantify, and diminish the derived risks and to guarantee that critical safety systems achieve the level of safety approved by the regulatory authorities. Verification of compliance with the established safety levels becomes the last but an essential part of the safety assurance process. This chapter provides a Bayesian inference methodology to assess and evaluate the compliance with the established safety levels under the presence of uncertainty in the assessment of systems performances.

Keywords: risk assessment, Bayesian inference, uncertainty, safety compliance

1. Introduction

Safety in aviation, and particularly in air traffic management (ATM), has evolved to the concepts of safety management and risk management. To achieve and guarantee safety, operators and providers develop and implement safety management system (SMS). SMS is a methodical and explicit approach for handling safety that comprises the required organisational arrangements and accountabilities, as well as the applicable safety policies and safety procedures. Hazard identification, risk assessment and risk mitigation have become essential processes within the framework of the SMS. Manufacturers, air navigation service providers (ANSPs) and operators shall implement a formal risk management process within their SMS.

This process, known as safety assessment (SA), has become a standard practice in the aviation industry. The global aim of SA is to ensure (by means of formal and systematic identification, evaluation and management of risks connected with hazards) that the design, production and operation of a system attain the safety levels settled by the safety regulatory authorities. Safety assessment has become a standard practice in the aviation industry [1–8].

SA typically implies three major phases that advance alongside the whole lifespan of the system [9, 10]:

- FHA—Functional hazard assessment
- PSSA—Preliminary system safety assessment
- SSA—System safety assessment

Figure 1 illustrates the liaisons between these three phases and the system life cycle.

System definition is the first stage of the system lifecycle. Its purposes are as follows:

i. To establish initial objectives for the system operating within its pertinent operational environment

ii. To define the functions to support these objectives

iii. To agree on high-level system requirements and interfaces

From the safety perspective, the first phase in the SA is referred to as functional hazard assessment (FHA). FHA aims to specify the safety level to be attained by the system in terms of safety objectives. A safety objective is a qualitative or quantitative statement that outlines the maximum acceptable frequency or probability of occurrence for a specific hazard or failure condition. If the hazard is a system failure, the safety objective will be the maximum allowed rate of failure. FHA is executed at the start of system design and development before the functions of the system have been deployed into procedures, equipment, or people components.

To determined system safety objectives, each function and combination of functions is assessed by safety analysts to:

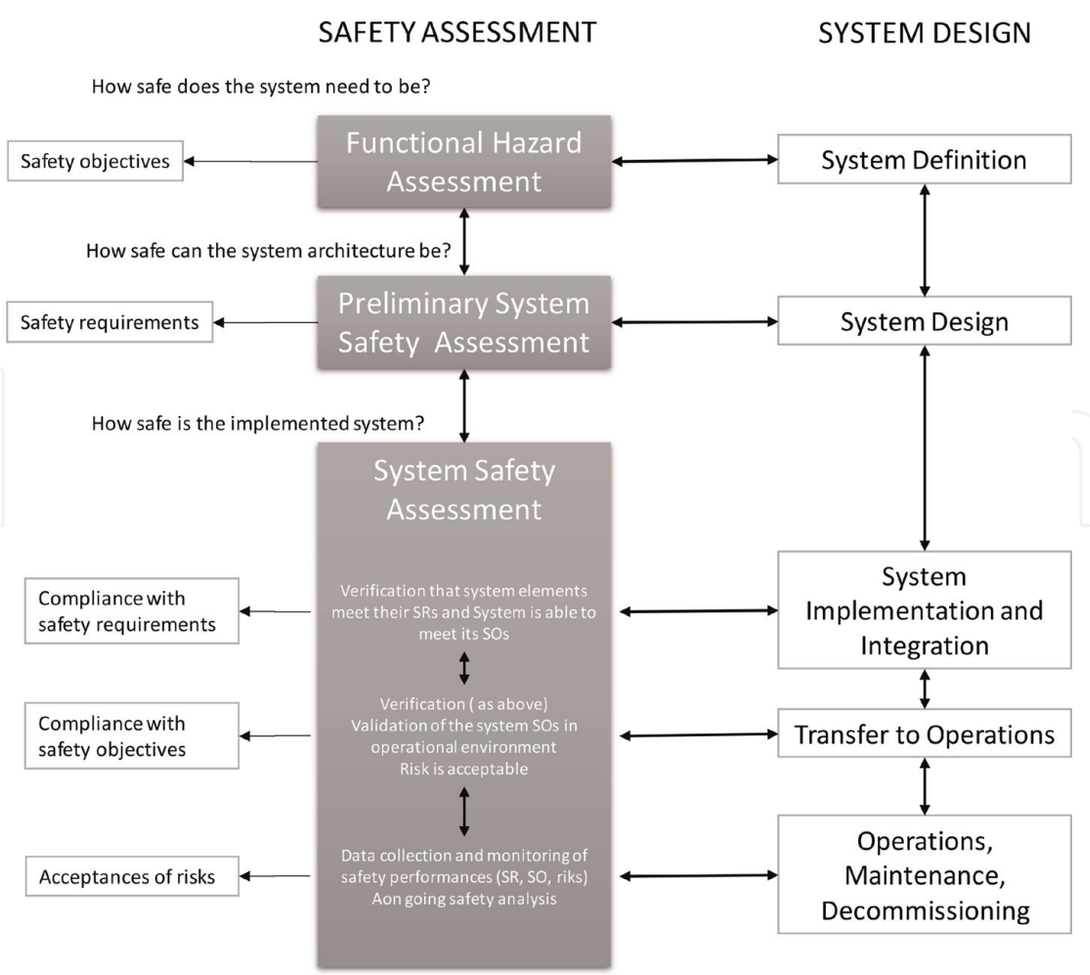

Figure 1.
Safety assessment phases alongside and system life cycle.

- Identify possible hazards and failures modes derived from the system definition.
- Identify hazard consequences or effects on operations.
- Evaluate the severity of each hazard consequences.
- Determine safety objectives, i.e. the maximum acceptable frequency for each hazard's occurrence.
- Assess intended aggregated risk.

The main step in this phase is the identification and classification of failures by their severity [11, 12] and the definition of safety objectives.

The following lifecycle stage is a system design. At this stage, the system operation and functions are defined in detail, describing the new system as an assortment of subsystems or components. In parallel, the risk assessment process develops a preliminary system safety assessment (PSSA). The objective of the PSSA is to prove that the designed system architecture can soundly attain the safety objectives stated during the FHA.

PSSA inspects the system architecture and concludes how failures could cause the hazards acknowledged in the FHA, it identifies required mitigations to minimise the risk or even eradicate them, and it specifies these measures in the form of safety requirements. A safety requirement is a risk measure, which may cover several different aspects such as operational, human, functional, organisational, procedural and performance, among others. Therefore, the PSSA process apportions safety objectives to the system elements and generates safety requirements, and then it stipulates the level of risk of each system element. The system architecture will meet the safety objectives established at the system level at the FHA, only if the architecture components satisfy their safety requirements.

After design, the next steps in the system lifecycle are implementation and integration. System implementation includes the production of the individual components, and integration refers to their amalgamation into the system. The next step, known as transfer into operations, refers to the system deployment, its on-site installation, its integration as part of an operational environment and the validation of its performances. During the system operation, maintenance actions, preventive and corrective, are accomplished in order to preserve the required safety and service level. Finally, once the system has reached the end of its operational life, decommissioning stands for the system withdrawal from the operation.

The last stage of the safety process, the system safety assessment (SSA), is developed in parallel to system implementation to verify whether the system, as implemented, achieve an acceptable risk. This means that the envisage mitigations have been put in place; all safety goals, objectives and requirements have been satisfied; and the expected level of safety has been successfully attained during the system operation [13, 14].

SSA monitors the safety performances of the system through its lifetime. It collects evidence and arguments to confirm that each implemented system component satisfies its safety requirements and safety objectives. It is, in the end, a continuous safety compliance assessment [15].

The SA process, although extended and widely accepted in aviation, is affected by a series of limitations. The main limitation neither resides in the fact that the process does not sufficiently considers nor widely capture the inherent uncertainty

in every step of the safety assessment. The process has also shown limitations in dealing with lacking data if when the system is brand new or when there is few measurable information about its performance. These limitations severely affect the effectiveness of the last step in the process, the system safety assessment. Additionally, many times, decision-makers cannot support their safety compliance decision on objective tools. As a consequence, the process has not enough objectivity or transparency.

This chapter illustrates that a systematic approach for dealing with uncertainties in safety compliance evaluation is possible through Bayesian reasoning. Bayesian inference is a systematic method that helps decision-makers to select a suitable path in relation to the acceptance of a system against its safety results. It is particularly useful if under the presence of uncertainty about the actual failure rates of a system and/or about the consequences of the decision-making process. It could also take into consideration the predilections of the decision-makers, experts' understanding and the consequences of the decisions to be made.

2. System safety assessment limitations

Most safety assessment decisions are taken under the assumption that the magnitudes of the variables and parameters describing the system performance are equal to their estimates. But, this postulation is valid as long as there is enough data or precise expertise for an accurate estimation of the system parameters [16]. This does not happen in many situations, particularly for new systems where only tiny information is accessible about its performance. Uncertainty also comes from partial or imprecise models or deficient data gathering.

There are several approaches to the concept of uncertainty [17–19]. Uncertainty is often understood as a "state of knowledge" [20]. Ayyub [21] describes it in terms of knowledge imperfection due to intrinsic shortages of knowledge acquisition. Walker [22] expresses uncertainty as "any departure from the unachievable ideal of complete determinism". Aven [23] defines it as "....lack of understanding about the behaviour and outcomes of a system, and discernible magnitudes".

Although there is a wide variety of definition for the concept of uncertainty, the common element in all of them is the notion of deficient or partial knowledge of a system and its performances because of shortages in apparent information and noticeable data [24, 25].

Uncertainty denotes the nondeterministic conduct of a system and the ambiguous magnitudes of the parameters that define how the systems behave or perform. It might have an epistemic or aleatory nature. Aleatory uncertainty accounts for the usual disparity of the physical phenomena. Epistemic uncertainty accounts for the limited knowledge of the parameters used to describe and explain the system [26, 27].

Both types of uncertainties are an essential component of any safety assessment. Uncertainty is introduced through the SA process at several stages. During FHA uncertainty is related to the modes of failure and the consequences of such failures. There are also uncertainties related to the extent of the consequences and consequently to the severity assigned of every failure condition. All these uncertainties are also translated into the assignment of SO—safety objective (the lower frequency of occurrence admissible for each failure circumstance), and into the derivation of safety requirements during the PSSA. During the SSA, uncertainties will come from inaccurate or incomplete medialization or data gathering.

The current safety compliance process acknowledges that multiple potential failure situations are possible, i.e. a single failure condition or hazard might lead to

several failure modes and, accordingly, to diverse effects and consequences. This uncertainty has been traditionally mitigated with the definition of the worst-case scenario. This way to proceed appears to be too biased and over-conservative, which lead to excessively conservative safety requirements. The consideration of worst-case scenario incorporates a sort of guard band to reduce the chance of accepting a system that does not perform safely enough. This guard band implies a cost to the system. This could only be evaded if the decision-maker has truthful (i.e. not conservative neither optimistic) guesses of the uncertainties in the magnitudes backing up the decisions.

As can be seen, most decision-making processes in safety compliance assessment during SSA imply judgement of safety performance in a context with uncertainty [28, 29]. However, the existing SSA process does not comprise a methodical process to cope with all those uncertainties. Today, SSA is reduced to gathering evidence and a simple binary comparison of those evidence towards safety goals and requirements.

3. System acceptance decision under uncertainty

Let us consider that the outcome of the SSA process is a dual pronouncement by the safety regulator to authorise, or not, the operation of a system. To help decision-makers in such a judgement, six uncertainties should be computed: two related to the acceptance of the system, two linked with the nonacceptance of the system and two linked with the consideration of insufficient information.

An essential step is also to evaluate the decision-maker's utilities. Decision-maker's utilities reflect the consequences, expressed typically as costs, connected to each of the former listed uncertainties. Determining an individual's utilities typically comprises expressing preferences among different options [30–33].

Figure 2 shows a decision diagram for safety assessment. Rectangles stand for decision node. The decision-maker choices a_i are as follows:

a_1—Judge the system compliant.

a_2—Judge the system as noncompliant.

a_3—Judge the information insufficient.

Circles are random nodes representing the "states of nature", where:

S_1 represents that the system is actually compliant.

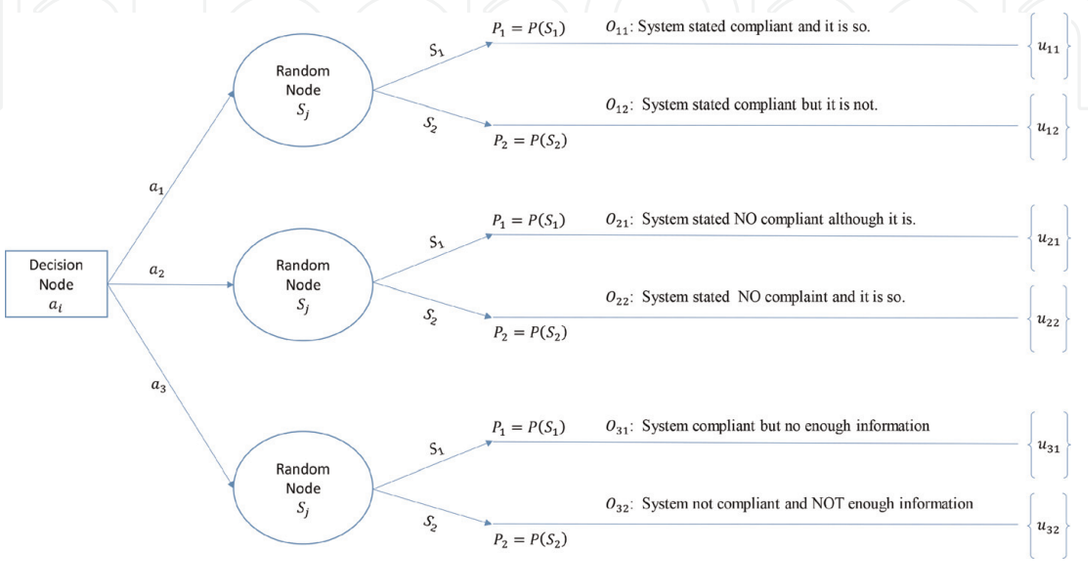

Figure 2.
Safety assessment decision tree.

S_2 represents a NOT compliant system.

The uncertainties about the system states P_j are dependent on the data "Data" and information "Inf"available and will be calculated in subsequent sections of the chapter.

$$P_1 = P(S_1) = P(S_1|Data, Inf);$$
$$P_2 = P(S_2) = P(S_2|Data, Inf) = 1 - P_1 \quad (1)$$

The paths in the tree correspond to the likely outcomes O_{ij} following the actions by the decision-maker. Six outcomes are considered:

O_{11}: The system is affirmed compliant and it is so.

O_{12}: The system is affirmed compliant though it is not.

O_{21}: The system is affirmed NO compliant while it is truly trustable.

O_{22}: The system is affirmed NO compliant and it actually is so.

O_{31}: Although the system is truly compliant, it is not enough to make a decision.

O_{32}: It is not enough to make a decision.

The rightmost end of the tree indicates the decision-maker's utilities u_{ij} for each of the six branches. Each pair $(a_i, S_i) \in C = AxN$ determines a consequence of decision-making. The utility $u_{ij}(c)$ which is defined on $C = AxN$ can be expressed as $u_{ij}(c) = u(a_i, S_j)$ and defines the preferences of the decision-maker.

If action a_1 is taken, larger compliance is preferred over a smaller one:

$$u(a_1, S_1(a_1, S_2) \text{ if and only if } S_1 \geq S_2 \quad (2)$$

If action a_2 is taken, diverse preferences can be outlined.

a. After a nonacceptance decision, the actual state of the system becomes irrelevant. This situation is equivalent to a constant utility for each value of S_j, i.e. $u(a_2, S_j) = cte \quad \forall S_j \in N$.

b. The combination of a nonacceptance decision and low system compliance is perceived as an opportunity loss. With a_2 decision-maker loses the occasion to admit a trustworthy system. The utility function $u(a_2, S_j)$ would not be constant any more, and smaller values of the actual system compliance would be preferred over larger opportunity loss). $u(a_1, S_1) \geq u(a_1, S_2)$ if and only of $S_1 \leq S_2$.

Despite the precise forms of $u(a_1, S_1)$ and $u(a_1, S_2)$, there is an "equilibrium" value S_0 such as

$$u(a_1, S_0) = u(a_2, S_0) \, \forall Ns_j \in [0, 1] \quad (3)$$

Therefore, the utility functions must follow the following relations:

$$\begin{aligned} u(a_1, S_j) > u(a_2, S_j) \text{ if } S_j > S_{j0} \\ u(a_1, S_j) < u(a_2, S_j) \text{ if } S_j < S_{j0} \end{aligned} \quad (4)$$

A decision-maker should choose the action that maximises the predictable utility $P(S_j) = P(S_j|Data, Inf)$. He should choose the action a^* such that satisfy the following expression:

$$E_N[u(a^*, S)] = \max_{a_i \in A,} E_N\left[u(a_i, S_j) * P(S_j)\right] \quad (5)$$

4. Quantification of the uncertainties

Safety compliance has been allocated a probability of truth or falsity. This probability corresponds to the decision-maker uncertainty (or state of knowledge), about safety compliance being true.

This probability is, namely, the uncertainty on the state of nature of the system compliance considering previous knowledge and information which is expressed as $P(S_j) = P(S_j|Data, Inf)$, where a proposition "Data" stands for data, while "Inf" stands for background information. This section details how $P(S_j) = P(S_s|Data, Inf)$ are calculated.

The proposed structure subscribes the concept that probability is not a frequency, rather a measure of uncertainty, belief or a state of knowledge. That is, probability allows doing credible thinking in situations where reasoning with certainty is not possible.

The result is the predictive probability that the system meets the safety objectives for what it has been designed, considering the envelope of data, knowledge and information gathered about the system during its design, production and operation.

To that aim, compliance assessment is redefined as the calculation of the degree of belief in the fulfilment of the applicable SO by the candidate system. The system is considered compliance if all the rate of failures λ_n satisfy their pertinent safety objective O_n.

Here the basis of Bayesian theory is applied to obtain an improved estimation of the system's components rate of failure λ_n.

Let us define a set of propositions, each one with a probability stating the grade of confidence in its states, being these states either TRUE if λ_n is lower than its safety objective, O_n, or FALSE otherwise.

$$S = \{S_n : n \in Q\} \text{ where } S_n = \begin{cases} TRUE\ if\ |\lambda_n| \le O_n \\ FALSE\ otherwise \end{cases} \tag{6}$$

This grade of confidence $P(S_n|Data, Inf)$ is denoted as a conditional probability. Each conditional probability $P(S_n|Data, Inf)$ mirrors our grade of assurance in λ_n satisfying its mandatory safety objective, O_n.

The grade of assurance in the system compliance $P(Cs|Data, Inf)$ will be evaluated as the intersection of the belief of compliance of all particular failure conditions:

$$\begin{aligned} P(S_j|Data, Inf) &= \bigcap_{n=1}^{N} P(S_j|Data, Inf) \\ &= P(S_1|Data, Inf) \bigcap P(S_2|Data, Inf) \bigcap ... \bigcap P(S_n|Data, Inf) \end{aligned} \tag{7}$$

Uncertainties about the magnitude of the variables that govern the stochastic performance of the system are random variables which follow particular probability functions (pdfs). Consequently, rates of failure λ_n become, therefore, also random variables. Therefore, safety assessments are reduced to the determination of the failure rate pdfs.

For straightforwardness, we adopt probability function for the failure rate of a component, λ_n, conditional upon one or more unknown parameters θ. Other indicators could be selected instead, for example, the delay time between defect and failure or the number of failures in a period of time, but the theory hereafter applies equally.

The corresponding probability function is indicated as $(\lambda_n|\theta)$. To some extent previous knowledge about the expected values of λ_n should impact decisions about the system acceptability. However, θ is commonly unknown, and $f(\lambda_n|\theta)$ is not known unambiguously, so it cannot be used directly in making such decisions about system acceptance. $f(\lambda_n|\theta)$ is usually approximated by estimating θ over data and supposing the parameters are equal to estimates.

Maximum likelihood method is applied [34, 35]. Eq. (24) expresses the likelihood function:

$$L(\theta; \mathrm{D}) \propto \prod_{i=1}^{n} p(\lambda_i|\theta) \propto \prod_{i=1}^{n} f(\lambda_i|\theta) \tag{8}$$

The Maximum likelihood estimate (MLE) is

$$L\left(\hat{\theta}; \mathrm{Data}\right) \geq L(\theta; \mathrm{Data}) \quad \forall\, \theta \neq \theta \tag{9}$$

In practical applications, previous inequality is usually strict, and a single maximum exists. The classical approach to inference now substitutes θ by the first-order approach. In this case, as few data are available; this approximation would be very poor:

$$f(\lambda_n|\theta) \approx f\left(\lambda_n|\hat{\theta}\right) \tag{10}$$

Decisions concerning compliance assessment, which seek for unknown values of λ_n, might alternatively be resolved conditional upon the observation, information, data or available knowledge, rather than on the unknown parameters. This allows to base decisions upon $f(\lambda_n|\mathrm{Data}, \mathrm{Inf})$ instead on $f(\lambda_n|\theta)$, provided that Data and Inf are known.

The conditional probability distribution $\mathrm{P}(\lambda_n|Data, Inf)$ describes then the uncertainty in the parameter under study (λ_n) considering observed data "Data" and the prior understanding of the system Inf. It denotes the sample of the rate of failure distribution, conditional upon the observed data, and it is exactly the magnitude required for the decision-making process, with no approximation. $\mathrm{P}(\lambda_n|Data, Inf)$ is calculated using the Bayes' theorem:

$$P(\lambda_n|ata, Inf) = \frac{P(Data|\lambda_n, Inf) \times P(\lambda_n|Inf)}{P(Data|Inf)} \tag{11}$$

where:

$P(\lambda_n|Data, Inf)$ is referred to the posterior distribution. All inference regarding λ_n will be derived from the posterior distribution.

$P(Data|\lambda_n, Inf)$ corresponds to the likelihood distribution, at times mentioned as sampling.

$P(\lambda_n|Inf)$is the prior distribution.

$P(Data|Inf)$ is the marginal probability.

Epistemic uncertainty is incorporated through the prior distribution $P(\lambda_n|Inf)$. It synthesises the level of confidence in our model parameters λ_n, and it expresses experts' preliminary state of information or knowledge. The prior distribution might be informative or non-informative.

The first ones deliver important information about the unquantified parameters. They are the way to capture past data and expert knowledge into a probability distribution and incorporate them into the model. Conjugate priors streamline the assessment of the preceding equation and permit analytical resolutions. However,

prior can follow any distribution, and the preceding equation can be solved using numerical integration.

Non-informative priors are sometimes named as flat priors, vague priors, diffuse priors or reference priors. They are used when there is just very little background information about the parameters.

Most of the times, the Bayesian method requires numerical simulation because of the complexity of the distributions involved. That implies that the solution of Eq. (27) has to be obtained by numerically Markov chain Monte Carlo (MCMC) simulation [36, 37].

The resulting posterior distribution, $P(\lambda_n|Data, Inf)$, stands for updated knowledge about λ_n and, as stated before, will be the foundation for all inferential conclusions regarding λ_n.

The distribution $P(Data|\lambda_n, Inf)$ signifies the aleatory uncertainties or change naturally included in data and models. It also accounts for inefficiencies in the data assembly as well as inadequacies in the models. Likelihood function most commonly employed in system safety assessment are binomial, Poisson or exponential ones [38–40].

And finally $P(Data|Inf)$ is just a normalisation factor.

$P(S_n|Data, Inf)$ can be obtained from the posterior distributions $P(\lambda_n|Data, Inf)$ through the marginalisation of the parameter λ_n, as shown in the next equation:

$$P(C_{sn}|Data, Inf) = \int_{\Lambda} P(O_n, \lambda_n|Data, Inf).\mathrm{d}\lambda = \int_{O}^{O_n} P(O_n|\lambda_n)P(\lambda_n|Data, Inf).\, d\lambda$$
$$= \int_{O}^{O_n} P(O_n|\lambda_n)\frac{P(Data|\lambda_n, Inf) \times P(\lambda_n|Inf)}{P(Data|Inf)}.\,\mathrm{d}\lambda \tag{12}$$

Eq. (12) calculates an average of the model uncertainty through the integration of the sampling $P(O_n|\lambda_n)$ through the posterior distribution $P(\lambda_n|Inf)$ [36]. The outcome is a predictive probability of a failure rate λ_n meeting its safety objective.

5. Conclusions

The safety assessment is a methodical and prescribed procedure applied by ANSP to find, quantify and diminish risks in ATM systems and ensure that new services or systems reach assurance levels required by the aviation authorities. The assessment of safety compliance against approved safety levels becomes the last but essential part of the safety assurance process.

Nevertheless, this method is still exhibiting a series of limitations, the most important being its failure to cope with the uncertainty intrinsic in each step of the assessment and its lack of ability to deal with the lack of data in early stages of operation, and only small measurable information about its performance can be accessed. While most choices in the safety assessment involve a trial under uncertainty, the present system safety assessment process does not embrace any organised process or help to address all these uncertainties. So, the process misses the simplicity and impartiality essential for regulatory decision-making.

This chapter discussed the mathematical grounds for a cohesive Bayesian inference methodology, to assess and evaluate compliance with system safety goals and requirements, taking into account the uncertainty in performances. This work proposes a Bayesian structure that assesses safety compliance as a decision-making issue taken place under the presence of uncertainty.

Bayesian approach enables more comprehensive management of the uncertainties inherent to all system safety assessments and improves impartiality and accepting of compliance decisions and judgements, particularly in the cases where uncertainty is a limitation. This method might be applied to any safety or regulatory compliance process. It might be directly implemented by either operator or manufacturers, as well as by safety oversight authorities.

This work aims to increase the use of statistical Bayesian methods in the ground of aviation safety compliance assessment, up to a level equivalent to the one achieved so far in other critical industries, such space or nuclear power industries. The method offers a significant improvement to how ANSP presently take on regulatory safety compliance. Whereas the theoretical grounds are not new, their application to aviation signifies a noteworthy progression over current practices.

Conflict of interest

The authors declare no conflict of interest.

Author details

Rosa Maria Arnaldo Valdés*, Victor Fernando Gómez Comendador and Luis Perez Sanz
Universidad Politecnica de Madrid, Madrid, Spain

*Address all correspondence to: rosamaria.arnaldo@upm.es

References

[1] SAE International. SAE ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Pensilvania, USA: SAE International; 1996

[2] SAE International. SAE ARP 5150: Safety Assessment of Transport Airplanes in Commercial Service. Pensilvania, USA: SAE International; 2013

[3] Federal Aviation Administration. Advisory Circular 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes. Washington, USA: FAA; 2011

[4] European Aviation Safety Authority. Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes CS-25 / Amendment 17. Cologne, Germany: EASA; 2015

[5] European Aviation Safety Authority. Special Condition: Equipment, Systems, and Installations. Cologne, Germany: EASA; 2015

[6] EUROCONTROL. ESARR 4: Risk Assessment and Mitigation in ATM. Brussels, Belgium: EUROCONTROL; 2001

[7] EUROCONTROL. Review of Techniques to Support the EATMP Safety Assessment Methodology - Volume I EEC Note No.01/04. Brussels, Belgium: Bruxelles; 2004

[8] Federal Aviation Administration, Advisory Circular 25.1309-1A, System Design and Analysis. Washington, USA: Federal Aviation Administration; 1988

[9] Di Gravio G, Patriarca R, Costantino F, Sikora I.Safety Assessment for an ATM System Change: A Methodology for the ANSPs. Safety and Security in Traffic. Zagreb, Croacia: University of Zagreb; 2016

[10] Smith CL, Dezfuli H. Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis. Technical report. Washington, USA: NASA; 2009

[11] Weishi C, Jing L. Safety performance monitoring and measurement of civil aviation unit. Journal of Air Transport Management. 2016;**57**:228-233

[12] Pial Dasa K, Kumer Dey A. Quantifying the risk of extreme aviation accidents. Physica A. 2016;**463**: 345-355

[13] Spence TB, Fanjoy RO, Chien-tsung L. International standardization compliance in aviation. Journal of Air Transport Management. 2015;**49**

[14] Button K, Clarke A, Palubinskas G. Conforming with ICAO safety oversight standards. Journal of Air Transport Management. 2004;**10**:251-257

[15] E. Sanchez Ayra. Risk Analysis and Safety Decision-Making in Commercial Air Transport Operations. PhD Thesis. Madrid, Spain; 2013

[16] Urho Pulkkinen T. STUK-YTO-TR 95. Model Uncertainty in Safety Assessment, Strälsäkerhetscentralen Finnish Centre for Radiation and Nuclear Safety. Helsinki, Finland; 1996

[17] Aven T. Some reflections on uncertainty analysis and management. Reliability Engineering and System Safety. 2010;**95**(3):195-201

[18] Aven T, Zio E. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliability Engineering and System Safety. 2011;**96**:64-74

[19] Paté-Cornell M. Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering and System Safety. 1996;**54**:95-111

[20] Dezfuli H, Kelly D, Smith C, Vedros K. Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis. NASA/SP-2009-569. Washington, USA: NASA; 2009

[21] Ayyub BM. Elicitation of Expert Opinions for Uncertainty and Risks. Boca Ratón, Florida, USA: CRC Press; 2001

[22] Walker W, Harremoës P, Rotmans J, Van der Sluijs J, Van Asselt M, Janssen P, et al. Defining uncertainty: A conceptual basis for uncertainty management in model-based decision support. Integrated Assessment. 2003;**4**:5-17

[23] Nilsen T, Aven T. Models and model uncertainty in the context of risk analysis. Reliability Engineering and System Safety. 2003;**79**:309-317

[24] Riesch H. Levels of uncertainty. In: Essentials of Risk Theory. New York, USA: Springer; 2013. pp. 29-56

[25] Zio E, Pedroni N. Methods for Representing Uncertainty: A Literature Review. Toulouse, France: Foundation for an Industrial Safety Culture; 2013

[26] Leonong C, Kelly T, Alexander R. Incorporating epistemic uncertainty into the safety assurance of socio-technical systems. In: Computer Science Department University of York. Proceedings CREST. York, UK: University of York; 2017

[27] Zhihuang D, Scott MJ. Incorporating epistemic uncertainty in robust design. In: ASME 2003 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. Cleveland, USA: ASME Design Engineering Division; 2003

[28] Fenton N, Neil M. The use of Bayes and causal modelling in decision making, uncertainty and risk. UPGRADE, Journal of CEPIS (Council of European Professional Informatics Societies). 2011

[29] Percy DF. Stochastics and statistics Bayesian enhanced strategic decision making for reliability. European Journal of Operational Research. 2002;**139**: 33-145

[30] Smith JQ. Bayesian Decision Analysis: Principles and Practice. Coventry: University of Warwick; 2010

[31] Hansson S. Decision Theory, A Brief Introduction. Stockholm, Sweden: KTH; 2005

[32] Peterson M. An Introduction to Decision Theory. New York: Cambridge University Press; 2009

[33] Wang JX. What every Engineer Should Know About Decision Making under Uncertainty. Michigan, USA: Marcel Dekker; 2012

[34] Aughenbaugh J, Herrmann J. Reliability-based decision making: A comparison of statistical approaches. Journal of Statistical Theory and Practice. 2009;**3**(1)

[35] Deneve S. Making decisions with unknown sensory reliability. Frontiers in Neuroscience. 2012;**6**:1-10

[36] Hamada M, Wilson A, Reese C, Martz H. Bayesian Reliability. Springer-Statistics; 2008

[37] Kelly DSC. Bayesian Inference for Probabilistic Risk Assessment: A Practitioners Guidebook. New York, USA, London: Springer; 2011

[38] Covello V, Merkhoher M. Risk Assessment Methods. Approaches for Assessing Health and Environmental Risks. New York, USA: Springer; 1993

[39] Landon J, Özekici S, Soyer R. A Markov modulated Poisson model for software reliability. European Journal of Operational Research. 2013;**229**: 404-410

[40] Bolstad W. Introduction to Bayesian Statistics. New Yersey, USA: John Wiley and Sons; 2007