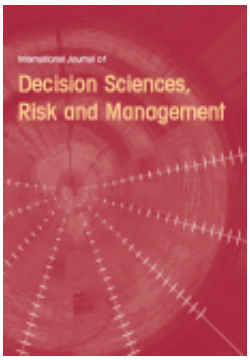


International Journal of Decision Sciences, Risk and Management

ISSN online: 1753-7177 - ISSN print: 1753-7169
https://www.inderscience.com/ijdsrm

Integration of STPA and TOPSIS fuzzy methods for risk analysis in aerospace projects

Sarah Francisca de Souza Borges, Mischel Carmen Neyra Belderrain, Moacyr Machado Cardoso Junior, Diogo Silva Castilho

DOI: 10.1504/IJDSRM.2022.10049887

Article History:
Received: 25 April 2021
Accepted: 27 December 2021
Published online: 22 August 2022

Integration of STPA and TOPSIS fuzzy methods for risk analysis in aerospace projects

Sarah Francisca de Souza Borges*,
Mischel Carmen Neyra Belderrain and
Moacyr Machado Cardoso Junior

Department of Science and Space Technologies,
Aeronautics Institute of Technology,
Square Marechal Eduardo Gomes 50, 12228-900,
Vila das Acacias, São José dos Campos, Brazil
Email: sarahfsborges2021@gmail.com
Email: carmen@ita.br
Email: moacyr@ita.br
*Corresponding author

Diogo Silva Castilho

Flight Test and Research Institute,
Square Marechal Eduardo Gomes 50, 12228-900,
Vila das Acacias, São José dos Campos, Brazil
Email: castilhods@msn.com

Abstract: There are several types of risks in organisations and projects, including technological, financial, environmental, legal, and operational. This article focuses on a risk analysis framework for complex aerospace research projects, some of which are innovations in the area and do not have a history of data from previous activities. The objective of this study is to analyse the feasibility of integrating the systems theoretic process analysis (STPA) method for systemic assessment of safety and fuzzy technique for order preference by similarity to ideal solution (TOPSIS) for prioritising unsafe control actions (UCAs). The proposed integration method was applied to the Laboratory of Injection Systems for Liquid Propellants at the Aeronautics Institute of Technology (ITA). The results obtained were the need for an emergency response plan, signalling, access control, and safety training for laboratory technicians. Therefore, risk analysis is essential to support the decision-making process, to identify and reduce hazards and losses.

Keywords: aerospace engineering; decision analysis; risk analysis; safety; project management; STPA; topsis fuzzy.

Reference to this paper should be made as follows: Borges, S.F.d.S., Belderrain, M.C.N., Cardoso Junior, M.M. and Castilho, D.S. (2022) 'Integration of STPA and TOPSIS fuzzy methods for risk analysis in aerospace projects', *Int. J. Decision Sciences, Risk and Management*, Vol. 10, Nos. 3/4, pp.212–226.

Biographical notes: Sarah Francisca de Souza Borges has a degree in Logistics from FATEC Jesen Vidal in 2011. She has a Master's and current Doctoral student in the area of Technological Management in Space Sciences

and Technologies, from the Technological Institute of Aeronautics. Currently, she is a project analyst at TecSUS Technologies for Sustainability. She has experience in project management, administration, and risk analysis.

Mischel Carmen Neyra Belderrain has a degree in Operations Research, Master's in Systems and Computer Engineering from the Federal University of Rio de Janeiro, and PhD in Aeronautical and Mechanical Engineering from the Aeronautics Institute of Technology – ITA. She is currently a Full Professor at ITA. She has experience in problem structuring and multicriteria decision methods.

Moacyr Machado Cardoso Junior has a degree in Agronomic Engineering from ESALQ/USP in 1986. He holds a Master'ss in Agricultural Machines from ESALQ/USP in 1989, Master's in Technology and Environmental Management from the Institute of Technological Research of São Paulo – IPT, and PhD in Aeronautical Engineering and Mechanics from Instituto Tecnológico de Aeronáutica – ITA in the area of multivariate statistics, in 2013. He has experience in the areas of risk analysis, occupational safety, quantitative methods applied to risk analysis, and risk modelling. He currently teaches disciplines in the area of risk management and analysis for ITA undergraduate and graduate courses in the Technological Management Program-CTE-G/ITA.

Diogo Silva Castilho is a test pilot of the Brazilian Air Force. He flew more than 2,400h in 35 different types of aircraft. As a fighter pilot, he flew for the Grifo and Adelphi squadrons. As a test pilot, he participated in 10+ flight testing campaigns, launched the first Brazilian guided bomb, and became an instructor of the Brazilian Flight Testing School. In his research at MIT, he developed a model to develop an active hazard analysis tool for complex systems.

1 Introduction

The risk of a project originates from intrinsic uncertainty, which organisations and stakeholders need to control and mitigate. There are many ways to reduce the probability and impact of negative events, risk management includes the processes of identification, analysis (qualitative and quantitative), response planning, and continuous control of a project (PMI, 2013).

Soon, organisations are exposed to several types of risks, including environmental, legal, operational, financial, and technological. This article discusses a risk analysis framework for complex aerospace research projects, some of which are innovations in the area and do not have a history of data from previous activities.

The objective is to analyse the feasibility of integrating the systems-theoretic process analysis (STPA) to identify requirements and constraints for safety, and TOPSIS Fuzzy (technique for order preference by similarity to ideal solution) for prioritisation of defences.

STPA is a technique for analysing hazards before exposure to unsafe situations, which proposes a model based on systemic thinking and setting up a top-down control structure (Underwood and Waterson, 2012).

Thus, it is different than the reliability-based models that focus on system components. STPA considers a holistic view, the variety of actors and their activities, resulting in the identification of hazards and a wide range of causal scenarios (Leveson, 2011; Leveson and Thomas, 2018; Yousefi et al., 2018). These scenarios, in turn, need to be prioritised to carry out efficient and effective risk management. At this stage, it is proposed to use the TOPSIS multi-criteria method to assess the performance of alternatives (Panda and Jagadev, 2018; Zyoud and Fuchs-Hanusch, 2017; Nouri et al., 2016). Together with the TOPSIS method, the fuzzy method is used, which considers the largest number of linguistic variables for the treatment of uncertainty.

It should be noted that this study aims to analyse the integration of the STPA and TOPSIS fuzzy method. In a bibliographic search in the SCOPUS and Web of Science databases in January 2021 (with the keywords: 'systems theoretic process analysis' AND 'TOPSIS Fuzzy'), no studies were found with the integration of both methods.

The STPA has the advantage of identifying more UCAs and accident causal scenarios, but there are no mechanisms to prioritise the mitigating measures at its end. Thus, this article presents the proposal for integration with the TOPSIS Fuzzy multi-criteria method. After all, for the decision-maker to take action, knowing what is more critical is essential, either to eliminate hazards or mitigate them. Besides, the risk study and analysis will serve as a basis for the proper planning of goals and activities in projects.

2 Materials and methods

This study had for material: bibliographic base (books and scientific articles) and interviews with professors responsible for the Laboratory of Injection Systems for Liquid Propellants (CEPROS). The professors are specialists with more than 10 (ten) years of experience in research and teaching, in areas such as combustion in propulsive systems; numerical simulations in combustion; characterisation and development of atomisers for engines; thermodynamics; fluid mechanics; space propulsion and liquid propellant rocket engine.

Furthermore, in the application of the STPA model, the XSTAMPP platform (eXtensible STAMP Platform), and version 2.5.3, was used. This is an open-source platform designed for the safety engineering area, aiming to meet the wide adoption and use of STAMP methodologies (system-theoretic accident model and processes), STPA and CAST (causal analysis using system theory), in different areas of knowledge (Abdulkhaleq and Wagner, 2015; Hata et al., 2015).

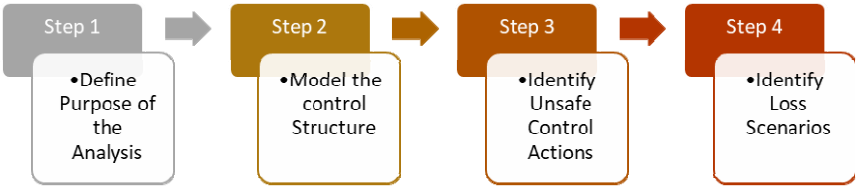
2.1 Method STAMP/STPA

The STAMP method is recommended to identify a greater number of potential causes of losses in complex systems and respective control actions or defences. It was proposed by Professor Nancy Leveson of MIT (in the areas of aeronautics and space, and systems engineering).

Based on the steps of STAMP, Leveson proposed as an extension the method of theoretical-systemic process analysis (systems theoretic process analysis, STPA), widely described in the book "Engineering a Safer World: Systems Thinking Applied to Safety", published in 2011.

STPA provides preventive accident analysis and is recommended for software development, system design, and human behaviour projects (Stanton et al., 2019). Proposing the analysis of unsafe conditions to the operation, with a list of their respective causal scenarios (Bjerga et al., 2016; Wróbel et al., 2018). There are four steps of the STPA method (Figure 1).

Figure 1 Steps of the STPA method (see online version for colours)



Source: Leveson and Thomas (2018)

Step 1 of STPA is to define the purpose of the analysis, identifying losses, hazards, and define system boundary. Hazard is a system state that in the worst environmental conditions will lead to a loss. The definition of loss involves something of value to stakeholders wherein loss is unacceptable (Leveson and Thomas, 2018). For example, a loss of human life or human injury, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information. In addition, when describing losses in terms of a hierarchy of control, based on feedback mechanisms, it is considered that each one has a context or process that led to the occurrence (Leveson, 2011).

Step 2 of STPA is to model the control structure. The development of a Control Structure is essential to define the limit of the system, as well as to understand the control loops. A hierarchical security control structure is an instance of the more general concept of system theory. The objective is to impose safety restrictions and, therefore, eliminate or reduce accidents (Leveson et al., 2003). Besides, hierarchical control allows analysis at levels, wherein the lower levels are closer to the physical structure where the accident occurs and the levels above have mechanisms to reinforce defenses. In this process, the controller (top level of the hierarchy) indicates control actions and receives feedback and reports from the controlled process. Thus, it makes it possible to assess whether security measures are being successful or failing (Leveson, 2011).

STPA step 3 is to identify unsafe control actions (UCAs), divided into 4 (four) types:

1 not providing the control action conducts to a hazard (for example, the air traffic controller does not issue a warning necessary to maintain safe separation)

2 providing the control action conducts to a hazard (for example, an air traffic controller issues an incorrect or inaccurate warning and leads to an accident)

3 providing a safe control action but too late, too early, or in an order not accepted

4 the control action lasts is stopped too soon or too long.

For example, the pilot performs the required ascension maneuver but continues after the flight level is reached (Leveson, 2011; Leveson and Thomas, 2018).

Step 4 in STPA is to identify loss scenarios, wherein it leads to unsafe action, considering environmental, behavioural, procedural conditions, among other aspects (Leveson, 2011; Leveson and Thomas, 2018).

Thus, through the STPA method, it is possible to identify hazards, losses, UCAs, causal scenarios, and requirements or defenses (implementation of safety actions).

Besides that, it is necessary to implement a hazard analysis into a safety management system as it identifies indicators of risk analysis to eliminate or control hazards during operations (Castilho, 2019).

In hazard analyses, there are specialists in human factors who consider the operator's behaviour as the result of the social, psychological, and even climatological context in which he is inserted. Therefore, human error cannot be treated statistically due to its natural unpredictability (Castilho et al., 2018).

The most effective way to control human behaviour is to design a system in such people simply behave according to safety standards (Leveson, 2011). The point that security costs so much is that it is often considered only after major architectural decisions, so once the basic design is completed, the only option is to add expensive redundancy or excessive design margins. The security-oriented design should help stakeholders to identify security-related requirements, design potential mitigation strategies, and analyse alternative architectures (Leveson et al., 2003).

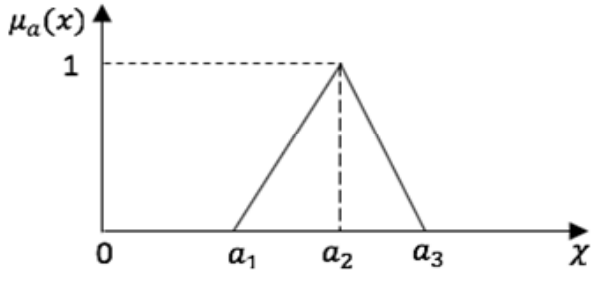
2.2 Method TOPSIS fuzzy

Hwang and Yoon, in 1981, proposed the TOPSIS multi-criteria method to evaluate the performance of alternatives that contemplate the similarities with the ideal solution (Panda and Jagadev, 2018). Presented by Chen in 2000, the fuzzy extension was considering that the best alternative it is that less distant from the fuzzy positive ideal solution (FPIS) and more distant from the fuzzy negative ideal solution (FNIS). An FPIS denotes the best performing values for each alternative, while an FNIS is a worst performing value (Lima-Junior and Carpinetti, 2015; Sodhi and Tadinada, 2012).

The fuzzy method considers the largest number of linguistic variables for the treatment of uncertainty. Fuzzy logic is capable of capturing vague information, described in language and converting it to a numerical format (Chenci et al., 2011).

For that, linguistic variables are used, which can be sentenced, using proper terms (low, medium, high), logical connectives (non-negatives, connectors and/or), modifiers (very, little), and delimiters (as parentheses) (Chenci et al., 2011).

Figure 2 Fuzzy triangular system



Source: Kore et al. (2017)

The following are conceptual definitions for understanding the TOPSIS Fuzzy technique:

a A fuzzy set $\tilde{a}$ in a universe of X designated by a function $\mu\tilde{a}(x)$ that composes each element x in X to a real number in the range [0, 1]. The value of the function is $\mu\tilde{a}(x)$ named the degree of membership of x in $\tilde{a}$. The closer value of $\mu\tilde{a}(x)$ to the unit, the greater degree of association of x in $\tilde{a}$ (Sodhi and Tadinada, 2012).

b A triangular fuzzy number is formed to a triple $\tilde{a} = (a_1, a_2, a_3)$, represented in Figure 2 (Kore et al., 2017).
Being that:

a_2 is the maximum degree of μ_a, where $\mu_a = 1$

a_1 is the minimum degree of μ_a, where $\mu_a = 0$

a_1 and a_3 are the lower and upper limits of the area available for assessment or support data (Kore et al., 2017).

The membership function of association of triangular fuzzy number [equation (1)] (Kore et al., 2017):

$$\mu_a(x) = \begin{Bmatrix} \dfrac{x-a}{b-a} if & a \le x \le b \\ \dfrac{c-x}{c-b} if & b \le x \le c \\ 0 \quad Otherwise & \end{Bmatrix}$$

The steps for applying the TOPSIS Fuzzy method can be summarised as follows:

1 Aggregate the weight of criteria to find the aggregate fuzzy weight $\tilde{w}$ of criterion C_j [equation (3)] and cluster the decision-makers ratings to have the aggregated fuzzy rating $\tilde{x}_{ij}$ of alternative A_i under criterion C_j [equation (4)].

2 Develop the normalised fuzzy decision matrix [equations (7) to (8)].

3 Develop the weighted normalised fuzzy decision matrix [equation (9)].

4 Establish the FPIS and FNIS [equations (10) to (11)], and compute the distance of each alternative [equations (12) to (14)].

5 Compute the closeness coefficient of each alternative and classify the alternatives [equation (15)] (Sodhi and Tadinada, 2012; Rahim et al., 2018).

3 Results and discussion

The proposed structure for integrating the STPA and TOPSIS fuzzy methods was applied to support the analysis of hazards and accidents at the CEPROS Laboratory.

3.1 Method TOPSIS fuzzy

Brazil has invested in projects that enable the development and launch of satellites, minimising the dependence on supplier countries and expanding national results in the research of this area. The CEPROS Laboratory was created in 2012, with the support of

researchers from ITA, Institute for Advanced Studies (IEAv), Aeronautics and Space Institute (IAE), and National Institute for Space Research (INPE), creating a cooperation network for liquid propulsion research, aiming to develop a combustion chamber powered by ethanol and cryogenic oxidant.

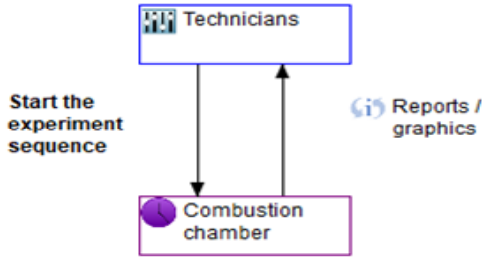
As part of this study, we applied STPA and TOPSYS Fuzzy methods to the context of the CEPROS Laboratory and conducted interviews with university professors. In the beginning, the control structure was assembled as shown in Figure 3. Presenting the controller and the controlled process, sequentially: technicians and combustion chamber.

The following hazards were identified with STPA: oxygen in the gaseous state reaching the head and coming into contact with a spark; leakage of gaseous oxygen in the laboratory and contact with a spark; incorrect operator action; leakage of ethanol and contact with a spark; improper procedures or equipment for the operation; loss of electrical energy during the test; lack of rescue and emergency support.

Likewise, the following accidents were identified: loss or damage to human lives; damage to equipment or infrastructure; environmental damage; loss of research project/reputation. in addition, in this phase, the following items could be identified:

- Safety restrictions (safety constraint): Have an emergency plan in case of accidents; Hire qualified professionals and offer training; Leader needs, beforehand, to establish procedures and plans; Check the power failure information in advance.
- Goals: Identification of hazards; Accident identification; Identification of causal scenarios.
- Project requirements (design requirements): Hiring qualified professionals to work in the Laboratory; Acquisition of equipment; Acquisition of materials; Teaching and safety procedures.

Figure 3 Control structure (see online version for colours)



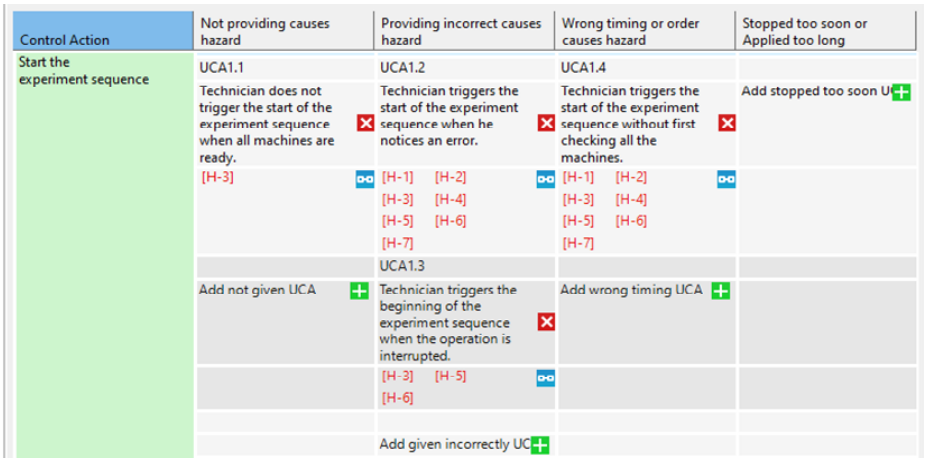
Source: Elaborated in software XSTAMP

The assembly of the control structure and list of hazards and accidents were inserted in the XSTAMP software. For example (Figure 4), in the control action ‘follow procedures’, in the influence loop between technicians and the combustion chamber, the following UCAs were listed:

- UCA1.1 “Technicians do not follow the procedures during an experiment”
- UCA1.2 “Technicians followed incorrect procedures during an experiment”
- UCA1.3 “Technicians do not fully follow the procedures established during activities”

- UCA1.4 “Technicians do not check equipment and materials before experiments”.

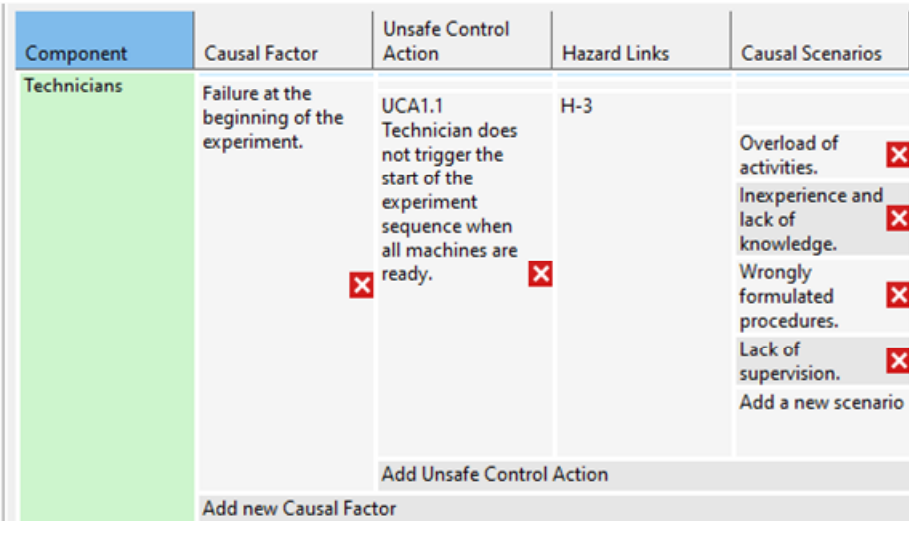
Figure 4 UCAs of the control action ‘follow procedures’ (see online version for colours)



Source: Elaborated in software XSTAMP

Subsequently, causal scenarios are identified for each UCA. As shown in Figure 5, referring to UCA1.1.

Figure 5 Causal scenarios for UCA1.1 (see online version for colours)



Source: Elaborated in software XSTAMP)

Following, the TOPSIS fuzzy method was applied to the 4 (four) UCAs of the STPA model, seen as more harmful. In fuzzy theory, conversion scales are used to transform linguistic terms into numbers. In this way, the criteria and alternatives can be classified on a scale, 1 to 9 for example, sorting out the intervals to have a uniform representation in the fuzzy triangular numbers. Table 1 presents these fuzzy numbers and the five

linguistic classifications associated with the criteria (probability, impact, and detectability).

Table 1 Linguistic variables based on fuzzy theory

Fuzzy numbers	*Rating of alternatives*			*Weights*
	Probability	*Impact*	*Detectability*	
1, 1, 3	Very low (E)	Very low (E)	Very high (A)	Very low (MB)
1, 3, 5	Low (D)	Low (D)	High (B)	Low (BB)
3, 5, 7	Average (C)	Average (C)	Average (C)	Average (C)
5, 7, 9	High (B)	High (B)	Low (D)	High (AA)
7, 9, 9	Very high (A)	Very high (A)	Very low (E)	Very high (MA)

Since there are two decision-makers, principally responsible for the CEPROS Laboratory, represents a fuzzy multi-criteria group decision making (GDM) problem which could be expressed in matrix format [equation (2)] (Borges, 2019; Kore et al., 2017).

$$\begin{matrix} & C_1 & C_2 & \ldots & C_n \end{matrix}$$
$$\tilde{D}^k = \begin{Bmatrix} \tilde{x}_{11}^k & \tilde{x}_{12}^k & \ldots & \tilde{x}_{1n}^k \\ \tilde{x}_{21}^k & \tilde{x}_{22}^k & \ldots & \tilde{x}_{2n}^k \\ \ldots & \ldots & \tilde{x}_{ij}^k & \ldots \\ \tilde{x}_{m1}^k & \tilde{x}_{m2}^k & \ldots & \tilde{x}_{mn}^k \end{Bmatrix} \quad (2)$$

The next step is to define the weight vector [equation (3)], which is formed of the weights for each criterion C_j respectively (Borges, 2019; Kore et al., 2017):

$$\tilde{W}_j = \tilde{w}_1, \tilde{w}_2, ..., \tilde{w}_n \quad (3)$$

Besides, professors were interviewed to define the fuzzy classification and the weight of the importance of each decision-maker k, on alternative i and criterion j (as shown in Tables 2 and 3).

In this analysis, the alternatives A_i are the UCAs, the criteria C_j are probability, impact, and detectability. This concept is similar to the FMEA method, which establishes three indexes to score the risk: occurrence (defines the frequency of failure); severity (refers to the severity of the failure effect); detection (ability to detect the fault before it occurs) (Amaral et al., 2010).

Table 2 Decision maker 1

UCA	*Probability*	*Impact*	*Detectability*
UCA1.1	B	A	D
UCA1.2	D	B	A
UCA1.3	D	B	D
UCA1.4	B	B	D
Weight W	MA	MA	AA

For example, for Decision 1 at UCA1.1 "Technicians do not follow the procedures during an experiment", the probability was assessed as high (B), impact as very high (A), and detectability as low (D).

Table 3 Decision maker 2

UCA	*Probability*	*Impact*	*Detectability*
UCA1.1	E	A	C
UCA1.2	D	A	C
UCA1.3	D	A	D
UCA1.4	C	A	D
Weight W	M	MA	MA

Then, the aggregated fuzzy ratings $\tilde{x}_{ij}$ of alternatives (i) for each criterion (j) [equation (4)] result in an aggregated matrix [equation (5)] (Borges, 2019; Kore et al., 2017):

$$a_{ij} = \min_{k}\left\{\tilde{x}_{ij}^{k}\right\}, b_{ij} = \frac{1}{k}\sum_{k=1}^{k}\tilde{x}_{ij}^{k}, c_{ij} = \max_{k}\left\{\tilde{x}_{ij}^{k}\right\} \tag{4}$$

$$\tilde{D} = \left(a_{ij}, b_{ij}, c_{ij}\right) \tag{5}$$

Thereby is necessary to calculate the aggregated fuzzy weights of each criterion [equation (6)] (Borges, 2019; Kore et al., 2017):

$$a_{j}' = \min_{i}\left\{a_{ij}'\right\}, b_{j}' = \frac{1}{n}\sum_{i=1}^{n}b_{j}', c_{j}' = \max_{i}\left\{c_{j}'\right\} \tag{6}$$

Table 4 presents for each a_{ij}, b_{ij}, c_{ij} the minimum, average, and maximum general values of each UCA by criterion, from the values in Tables 2 and 3. The linear scale transformation is used in the criteria scales to have a comparable scale, resulting in an aggregated fuzzy decision matrix (Sodhi and Tadinada, 2012), as shown in Table 4.

Table 4 Aggregate matrix (D)

UCA	*Probability*			*Impact*			*Detectability*		
UCA1.1	1	4	9	7	9	9	3	6	9
UCA1.2	1	3	5	5	8	9	1	3	7
UCA1.3	1	3	5	5	8	9	5	7	9
UCA1.4	3	6	9	5	8	9	5	7	9

In this step, from the aggregate matrix $\tilde{D}$, normalisation is performed, finding the elements $\tilde{r}_{ij}$. The probability and impact in Table 4 are cost criteria, therefore, their values are divided by c_j^* (general maximum value of the entire table), because the higher of probability and impact, needs a greater degree of prioritisation [equation (7)]. Already, the detectability criterion is a benefit criterion, therefore each of its values will be divided by a_j^- (general minimum value of the entire table), and the lower detectability needs a

greater degree of prioritisation [equation (8)]. The results of this analysis are shown in Table 5 (Borges, 2019; Kore et al., 2017).

$$\tilde{r}_{ij} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*} \right), c_j^* = \max_i \{c_{ij}\} \tag{7}$$

$$\tilde{r}_{ij} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}} \right), a_j^- = \min_i \{a_{ij}\} \tag{8}$$

Table 5 Normalisation (R)

UCA	*Probability*			*Impact*			*Detectability*		
UCA 1.1	0.11	0.44	1.00	0.78	1.00	1.00	0.11	0.17	0.33
UCA 1.2	0.11	0.33	0.56	0.56	0.89	100	0.14	0.33	1.00
UCA 1.3	0.11	0.33	0.56	0.56	0.89	1.00	0.11	0.14	0.20
UCA 1.4	0.33	0.67	1.00	0.56	0.89	1.00	0.11	0.14	0.20
Weight W	3	5	7	7	9	9	3	5	7
	Cost criterion			Cost criterion			Benefit criterion		

The weighted normalised fuzzy decision matrix $\tilde{v}_{ij}$ is calculated by multiplying the weights $(\tilde{w}_j)$ of criteria with the normalised fuzzy decision matrix $\tilde{r}_{ij}$ [equation (9)] (Borges, 2019; Kore et al., 2017), shown in Table 6.

$$\tilde{v}_{ij} = \tilde{r}_{ij}(.)\tilde{w}_j = \left(a_{ij}'', b_{ij}'', c_{ij}'' \right) \tag{9}$$

Table 6 Normalised and weighted matrix (V)

UCA	*Probability*			*Impact*			*Detectability*		
UCA 1.1	0.33	2.22	7.00	5.44	9.00	9.00	0.33	0.83	2.33
UCA 1.2	0.33	1.67	3.89	3.89	8.00	9.00	0.43	1.67	7.00
UCA 1.3	0.33	1.67	3.89	3.89	8.00	9.00	0.33	0.71	1.40
UCA 1.4	1.00	3.33	7.00	3.89	8.00	9.00	0.33	0.71	1.40
	Cost criterion			Cost criterion			Benefit criterion		

The FPIS and FNIS of the alternatives need to be defined [equations (10) to (11)] (Borges, 2019; Kore et al., 2017).

$$\begin{aligned} &A^+ = \left(\tilde{v}_1^+, \tilde{v}_2^+, ..., \tilde{v}_n^+ \right), \text{where:} \\ &\tilde{v}_j^+ = (c, c, c), \text{and,} \\ &c = \max_i \{c_{ij}'\}; i = 1, 2, ..., m;\ j = 1, 2, ..., n \end{aligned} \tag{10}$$

$$A^{-} = \left(\tilde{v}_1^{-}, \tilde{v}_2^{-}, ..., \tilde{v}_n^{-}\right), \text{ where:}$$
$$\tilde{v}_j^{-} = (a, a, a), \text{ and,} \tag{11}$$
$$a = \min_i \left\{a'_{ij}\right\}; i = 1, 2, ..., m; j = 1, 2, ..., n$$

Among the alternatives (UCAs) for each criterion, in the column with the maximum values is selected the highest value (C_j) and in the column with the minimum values is select the lowest value (A_i), in this way, the minimum and maximum values are established.

Looking for the fuzzy triangular distance, whether $\tilde{p}_{ij} = (a, b, c)$ and $\tilde{q}_{ij} = (a', b', c')$ are two triangular fuzzy numbers, the distance between them is found [equation (12)] (Borges, 2019; Kore et al., 2017), being:

$$d_v = \sqrt{\frac{1}{3}\left[\{a - a'\}^2 + \{b - b'\}^2 + \{c - c'\}^2\right]} \tag{12}$$

For the FPIS and the FNIS, the distance (d_i^+ and d_i^-) of each weight alternative i = 1,2,…,m is computed [equation (13)], for ideal positive fuzzy value and for ideal negative fuzzy value [equation (14)] (Borges, 2019; Kore et al., 2017).

$$d_i^+ = \sum_{j=1}^{n} d_v\left(\tilde{v}_{ij}, \tilde{v}_j^+\right), i = 1, 2, ..., m \tag{13}$$

$$d_i^- = \sum_{j=1}^{n} d_v\left(\tilde{v}_{ij}, \tilde{v}_j^-\right), i = 1, 2, ..., m \tag{14}$$

The results are shown in Table 7, and for each UCA the FPIS and FNIS are found.

Table 7 Results of FPIS and FNIS distances

	FPIS				*FNIS*			
Criterion/UCA	1.1	1.2	1.3	1.4	1.1	1.2	1.3	1.4
Probability	4.74	5.25	5.25	4.06	4.00	2.19	2.19	4.24
Impact	2.05	3.01	3.01	3.01	4.27	3.79	3.79	3.79
Detectability	5.89	4.89	6.20	6.20	1.19	3.93	0.65	0.65
Sum =	12.68	13.14	14.45	13.27	9.46	9.91	6.63	8.68

In the end, the proximity coefficient Cp_i is calculated, which represents the distances to the positive fuzzy ideal solution A^+, and the negative ideal solution A^- simultaneously. Then, the result of the proximity coefficient for each alternative is found by the next function [equation (15)] (Borges, 2019; Kore et al., 2017).

$$Cp_i = \frac{d_i^-}{d_i^- + d_i^+}, i = 1, 2, ..., m \tag{15}$$

Table 8 shows the order of the UCAs. The closeness coefficient scores for alternatives have numeric values and can be used to designate the degree of inferiority or superiority of the alternatives to each other.

Table 8 Calculation of FPIS and FNIS distances

UCA	CC_i	*Classification*
1.1	0.427	2
1.3	0.315	4
1.4	0.395	3
1.2	0.430	1

Thus, when identifying a UCA, its causes and control actions are also identified, with this proposal it is possible to order the UCAs that indicate where to start executing the mitigating actions.

4 Conclusions

The STPA method provides a structure for the system analyst to identify accidents, hazards, UCAs, more causal scenarios with respective control or mitigating actions, and requirements. It stands out that the biggest gain seen with the STPA was that, once scenarios are identified, they could be used to create additional requirements, identify mitigations, propose a modification in the architecture, make design recommendations and make safer decisions. Although, it does not present the prioritisation of results at the end. Thus, the integration with the TOPSIS Fuzzy method was proposed and tested, based on the list of UCAs, considering the criteria of probability, impact, and detectability.

Then, the priority will be on unsafe action (UCA), in which the respective causal scenarios and mitigating actions are already mapped.

For activity planning and risk mitigation, this previous process proved to be viable and resulted in the following classification: UCA1.2 “Technicians followed incorrect procedures during an experiment”; UCA1.1 “Technicians do not follow the procedures during an experiment”; UCA1.4 “Technicians do not check equipment and materials before experiments” and UCA1.3 “Technicians do not fully follow the procedures established during activities”.

For UCA1.1, for example, the following causes for the elaborated causal scenarios were:

1 attention overload during activities

2 lack of specific knowledge due to inexperience

3 poorly formulated procedures

4 lack of supervision.

Additionally, the following defences or security actions were determined for each respective causal scenario:

1 notify the person in charge when there is an attention overload

2 check if the technicians are ready to operate unsupervised

3 reinforce the need to notify the manager if there is no understanding of the procedures

4 the manager must carry out constant or periodic supervision of operations.

It is also worth noting that this study focused on the integration of methods, considering the need for systemic analysis of the problem and later the prioritisation of results for adequate treatment by the decision-maker. Therefore, there is still the possibility of new applications with these proposed methods (STPA and TOPSIS fuzzy) and other combinations of methods in the area of security and risk analysis to complement their results.

References

Abdulkhaleq, A. and Wagner, S. (2015) 'XSTAMPP: An eXtensible STAMP platform as tool support for safety engineering', *4th STAMP Workshop*, *Proceedings*, Boston, Massachusetts, USA, Vol. 1.

Amaral, É.H., Amaral, M.M. and Nunes, R.C. (2010) 'Metodologia para Cálculo do Risco por Composição de Métodos', *10th Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, *Proceedings*, Porto Alegre, Rio Grande do Sul, Brazil, Vol. 1.

Bjerga, T., Aven, T. and Zio, E. (2016) 'Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM', *Reliability Engineering and System Safety*, Vol. 156, pp.203–209.

Borges, S.F.S. (2019) *Integração de métodos para análise de riscos em projetos de pesquisa aeroespaciais*, MSc Thesis, Aeronautics Institute of Technology, São José dos Campos, Brazil.

Castilho, D.S. (2019) *Active STPA: Integration of Hazard Analysis into a Safety Management System Framework*, Doctoral Thesis, Massachusetts Institute of Technology, Massachusetts, USA.

Castilho, D.S., Urbina, L.M.S. and Andrade, D. (2018) 'STPA for continuous controls: a flight testing study of aircraft crosswind takeoffs', *Safety Science*, Vol. 108, No. 1, pp.129–139.

Chen, C.T. (2000) 'Extensions of the TOPSIS for group decision-making under fuzzy environment', *Fuzzy Sets and Systems*, Vol. 114, No. 1, pp.1–9.

Chenci, G.P., Rignel, D.G. and Lucas, C.A. (2011) 'Uma introdução a lógica fuzzy', *Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica*, Vol. 1, No. 1, pp.1–12.

Hata, A., Araki, K., Kusakabe, S., Omori, Y. and Lin, H.H. (2015) 'Using hazard analysis STAMP/STPA in developing model-oriented formal specification toward reliable cloud service', *1st International Conference on Platform Technology and Service*, *Proceedings*, Jeju, South Korea, Vol. 1.

Hwang, C.L. and Yoon, K. (1981) *Multiple Attribute Decision Making*, Ed. Group, Taylor & Francis, Springer, Berlin, Heidelberg.

Kore, M.N.B., Ravi, K. and Patil, S.B. (2017) 'A simplified description of FUZZY TOPSIS method for multi criteria decision making', *International Research Journal of Engineering and Technology*, Vol. 4, No. 5, pp.2047–2050.

Leveson, N.G. (2011) *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge.

Leveson, N.G. and Thomas J.P. (2018) *STPA Handbook*, Massachusetts Institute of Technology [online] https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf (accessed 20 July 2020).

Leveson, N.G., Daouk, M., Dulac, N. and Marais K. (2003) 'Applying STAMP in accident analysis', *2nd Workshop Investigation Reporting Incidents Accidents (IRIA)*, *Proceedings*, Radisson Fort Magruder Hotel & Conference Center in Williamsburg, Virginia, USA, Vol. 1.

Lima-Junior, F.R. and Carpinetti, L.C.R. (2015) 'Uma comparação entre os métodos TOPSIS e Fuzzy-TOPSIS no apoio à tomada de decisão multicritério para seleção de fornecedores', *Gestão & Produção*, Vol. 22, No. 1, pp.17–34.

Nouri, J., Arjmandi, R., Riazi, B., Aleshekh, A.A. and Motahari, S. (2016) 'Comparing multi-criteria decision-making (MCDM) tool and huff model to determine the most appropriate method for selecting mountain tourism sites', *Environmental Engineering and Management Journal*, Vol. 15, No. 1, pp.41–52.

Panda, M. and Jagadev, A.K. (2018) 'TOPSIS in multi-criteria decision making: a survey', *2nd International Conference on Data Science and Business Analytics (ICDSBA)*, *Proceedings*, Changsha, China, Vol. 1.

PMI (2013),*Project Management Body of Knowledge (PMBOK)*, 5th ed., Project Management Institute, Philadelphia.

Rahim, R., Siahaan, A.P.U., Wijaya, R.F., Hantono, H., Aswan, N., Thamrin, S., Sari, D., Agustina, S., Santosa, R.B., Muttaqin, W., Sujito, S., Yulia, Y., Fatmasari, R., Ikhwan, A., Sugiarto, I., Purnomo, A., Kulsum, N.M., Diawati, P. and Sujarwo, S. (2018) 'Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method for decision support system in top management', *International Journal of Engineering and Technology (UAE)*, Vol. **7**, pp.290–293.

Sodhi, B. and Tadinada, P. (2012) 'A simplified description of fuzzy TOPSIS', *Computing Research Repository*, Vol. 1, No. 1, pp.1–4.

Stanton, N.A., Harvey, C. and Allison, C.K. (2019) 'Systems theoretic accident model and process (STAMP) applied to a royal navy hawk jet missile simulation exercise', *Safety Science*, Vol. 113, pp.461–471.

Underwood, P. and Waterson P. (2012) 'A critical review of the stamp, fram and accimap systemic accident analysis models', in Stanton N.A. (Ed.): *Advances in Human Aspects of Road and Rail Transportation*, CRC Press, Boca Raton, pp.385–-394.

Wróbel, K., Montewka, J. and Kujala, P. (2018) 'Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels', *Reliability Engineering and System Safety*, Vol. 178, No. 1, pp.209–224.

Yousefi, A., Hernandez, M.R. and Peña, V.L. (2018) 'Systemic accident analysis models: a comparison study between AcciMap, FRAM, and STAMP', *Process Safety Progress*, Vol. 37, No. 2, pp.1–16.

Zyoud, S.H. and Fuchs-Hanusch, D. (2017) 'A bibliometric-based survey on AHP and TOPSIS techniques', *Expert Systems with Applications*, Vol. 78, No. 1, pp.158–181.