STPA Analysis over the Earlier Phases of Brazilian Aerospace Products Life Cycle Using OPM

2022 13th International Conference on Mechanical and Aerospace Engineering (ICMAE) | 978-1-6654-7235-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICMAE56000.2022.9852838

Guilherme Moreira
PPGAO (Postgraduate Program in Operational Applications)
ITA (Aeronautics Institute of Technology)
São José dos Campos, Brazil
moreira@ita.br

Daniel Rondon Pleffken
PPGAO (Postgraduate Program in Operational Applications)
ITA (Aeronautics Institute of Technology)
São José dos Campos, Brazil
rondon@ita.br

Christopher Cerqueira
Aerospace Systems Department
ITA (Aeronautics Institute of Technology)
São José dos Campos, Brazil
chris@ita.br

Willer Santos
Aerospace Systems Department
ITA (Aeronautics Institute of Technology)
São José dos Campos, Brazil
willer@ita.br

***Abstract*—The earlier phases of any product development greatly influence its life cycle, especially in the aerospace field. Therefore, precise requirements are critical for good acquisition/development contract execution. Firstly, this study has made use of OPM (Object Process Methodology) to model the current Brazilian Air Force Policy for aerospace products' life cycle and a robust hazard analysis technique (STPA - System-Theoretic Accident Model and Processes) to investigate the causal factors which lead to negative impacts on the contract elaboration process for military aerospace products in Brazil. STPA uses System Theory to model any process as a feedback control structure. Focusing on the minimization of losses, the method considers the hazards, safety constraints, unsafe control actions, and causal factors. Based on that, it proposes requirements (which can be understood as recommendations), showing a path throughout the earlier phases of the Brazilian military aerospace products life cycle to improve the contract elaboration process.**

Keywords—STPA, OPM, contract elaboration process

I. INTRODUCTION

Aerospace Project/Operation Organizations usually rely on their acquisition/development policies and directives. Such organizations are careful in setting the terms that will invariably impose a considerable influence on how those systems under acquisition/development will work, be verified, and, more importantly, how they will fulfill the organizations' needs [1].

The Brazilian Air Force is a large and complex organization with significant responsibilities over the Brazilian aerospace environment. The Brazilian National Defense Strategy [2] splits three major strategic fields among the three-component Forces: The Army is responsible for cyberspace; the Navy for nuclear matters; and the Air Force oversees aerospace issues.

With more than 70,000 employees, approximately 800 units of 30 different aircraft, hundreds of defense products (such as bombs, missiles, electronic warfare intelligent PODs, etc.), and dozens of space products under operation (launched from inside borders and abroad), it is absolutely crucial for the Brazilian Air Force to have a robust systems and products life cycle policy. Such a set of information is found in [3].

The conceptual phase of product development is where the stakeholder needs are detailed in statements, defining functionalities and conducting multidisciplinary analysis [4]. Due to the importance of such a development stage, this work focuses on the conceptual and definition phases of Brazilian aerospace systems and products life cycle established on [3], which finalize with the contract celebration.

After stating this work objective in section II, this paper presents a brief overview of the methodologies and techniques used to improve the current Brazilian Air Force acquisition/development policy for aerospace products and systems in sections III and IV. Subsequently, section V presents the hazard analysis performed by the authors and its output: constraints and requirements (that might be taken as recommendations) for the earlier phases of the Brazilian Air Force products life cycle.

Similarly, other Aerospace Project/Operation Organizations, whether private or public, may take lessons learned by this work as reference.

II. WORK AIM

This work aims to raise recommendations on the conceptual and definition phases of Brazilian Military Aerospace products, aiming at the contract elaboration process, since those phases establish the projects' premises and, therefore, drive their success.

The authors believe that the challenges faced by many organizations, private and public, are close to the ones faced by the Brazilian Air Force over this matter.

The methodologies, tools, and techniques used in this work are accessible to any Aerospace Project/Operation Organization.

III. OBJECT PROCESS METHODOLOGY

A. Overview

One of the biggest challenges in understanding any system (or process) is the emergence of complexity that may surround various components and subsystems (or subprocesses) and how they interact.

Traditionally, System Engineering processes are based on a robust body of documentation and stakeholders' requirements. On the other hand, such a large amount of technical and management information may make synchronizing all those elements challenging to fulfill [5].

OPM (Object Process Methodology), ISO 19450:2015, is a Model-Based System Engineering methodology, and it is based on a minimal modeling ontology of stateful objects as things that exist or can exist and processes as things that transform objects by creating or consuming them or by changing their state [5]. Therefore, OPM is an outstanding tool to model any system or process, providing a comprehensive approach that integrates structural, functional, and behavioral aspects of the modeled object of study.

In addition, OPM has already been used together with STPA, and both techniques could be easily made as a theory and laboratory exercise to define system functionality and architecture [6].

For that reason, the authors have selected OPM to design a model of the Conceptual, Feasibility, and Definition phases of the Brazilian Air Force aerospace products life cycle [3]. The model increases the understanding of this process and yields a better situation awareness, easing the identification of improvements.

B. Model

To cover all the relevant procedures defined in the earlier phases of the Brazilian aerospace products life cycle Policy, we have split the model into five layers, as shown in Fig. 1 to 5.

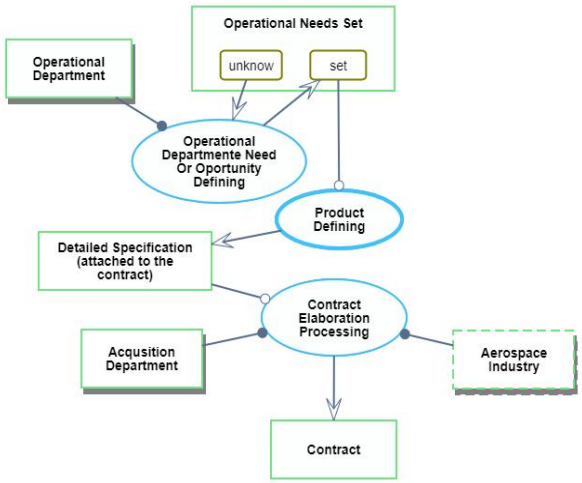


Fig. 1. Contract elaboration process of Brazilian aerospace products at its higher level

Once modeled this process, from its very beginning up to the contract signing, whether a supply or development commitment, we can better design its hierarchical control structure, which was used to guide the next steps of this work.

To optimize the aerospace systems requirements and avoid the occurrence of dangers in the path of users' needs fulfillment, the authors sought a robust hazards analysis technique that could identify specific areas to improve: the STPA (System Theoretic Process Analysis). The technique overview, application, and results are presented in sections IV and V.

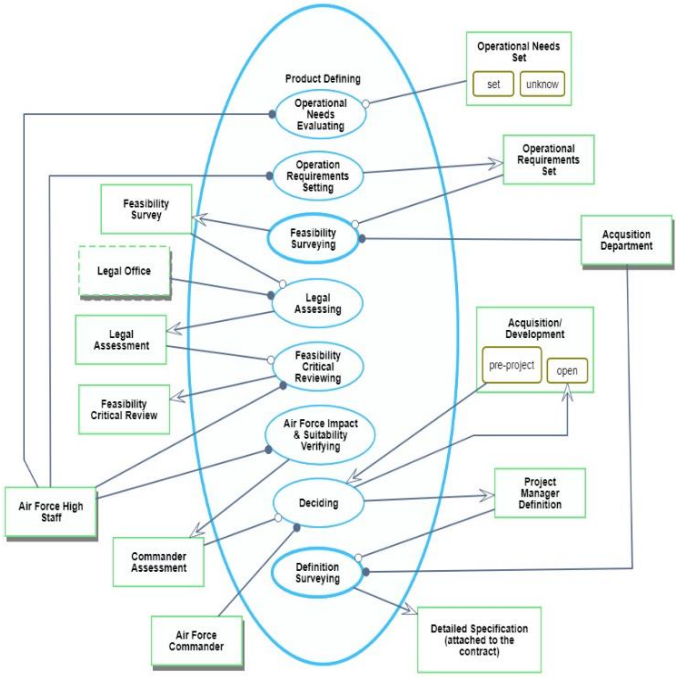


Fig. 2. Product Defining process in-zoomed

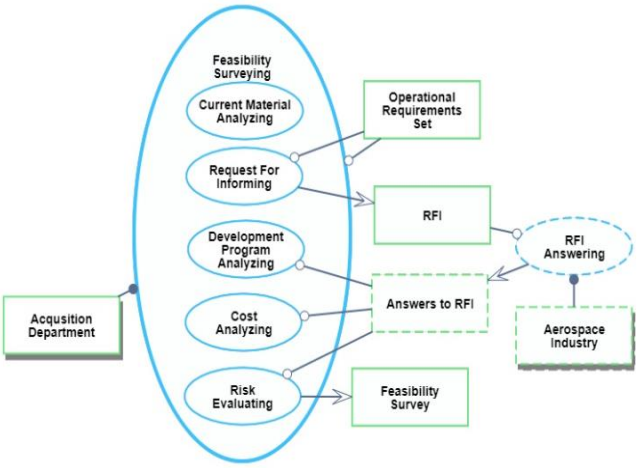


Fig. 3. Feasibility Surveying process in-zoomed

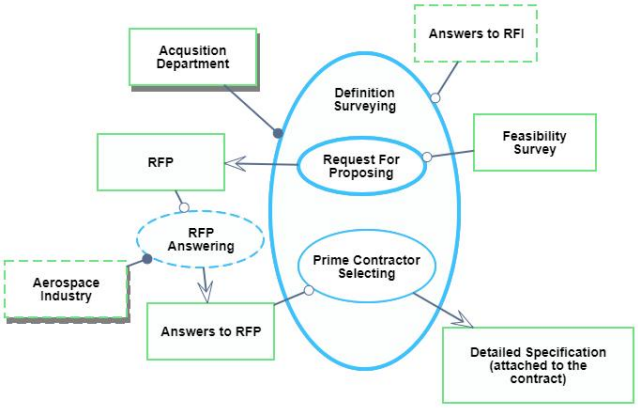


Fig. 4. Definition Surveying process in-zoomed

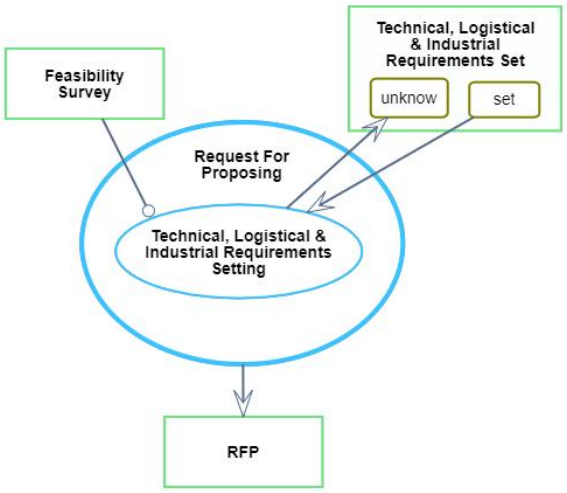


Fig. 5. Request for proposing process in-zoomed

IV. System Theoretic Process Analysis

A. Overview

STPA is a technique to perform hazard analysis based on an extended model of accident causation developed by Dr. Nancy Leveson in 2002 called STAMP (System-Theoretic Accident Model and Processes), which is based on System Theory [7] created to manage complex systems.

Compared to the traditional risk analysis FTA (Fault Tree Analysis), STPA provides a more detailed analysis and better functionality, which is crucial to safety-critical systems [8].

The main goal of STPA is to consider both component failure and unsafe interactions of system components on the hazard analysis [9], including the human component and its behavior with the designed system.

In aviation, probabilistic requirements are created based on previous similar systems' operational experience. However, such class of requirements are not helpful for software, due to their predictable characteristics, especially considering that software is present in practically all aircraft components nowadays. Therefore, STPA came to provide functional safety requirements for the system as a whole.

In addition, STPA is an iterative process and might be refined according to the design through the generation of more detailed requirements, which address the Unsafe Control Actions (UCA) raised by the method application. Such an iterative process allows the analyst to refine the STPA analysis as far as it seems applicable for the design. The method creator encourages their users to apply STPA in the early concept development stage [10]. Fig. 6 shows a scheme to help STPA users to define the purpose of the analysis. Notice that hazards might be refined into sub-hazards after identifying system-level (high-level) constraints.

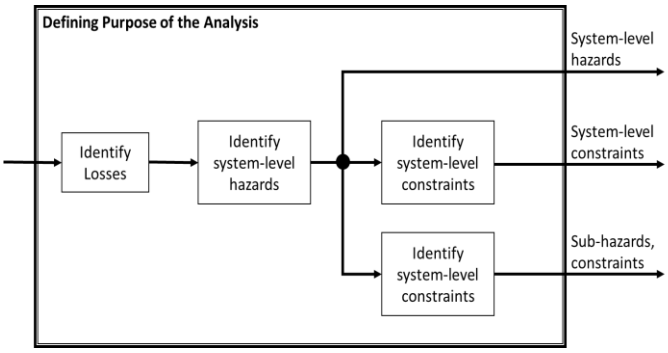


Fig. 6. Defining the purpose of the STPA analysis

STPA is an adjustable technique. This means that we may use its results to improve anything that can be modeled according to System Theory [7] in a hierarchical control structure. In addition, the application of STPA raises more holistic system requirements with a high benefit-cost ratio. According to [11], learning and applying STPA takes only 21% of the time spent in a generic industry project (Fig. 7).

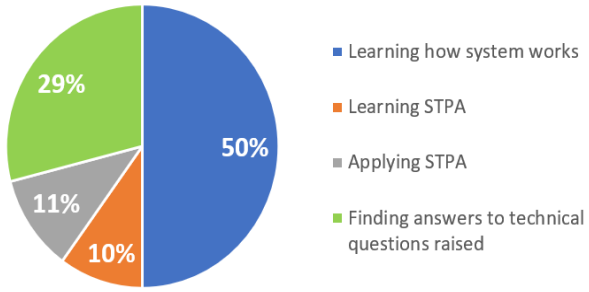


Fig. 7. Relative amount of time spent on different tasks during a recent industry STPA project [11]

V. STPA Hazard Analysis

A. Losses

STPA starts with the specification of unacceptable losses. For this study magnitude, it is enough to consider one main concern that the implementation of the method must address.

According to [1], **requirements are the key to project success,** and projects' objective is to solve a problem experienced by users. Considering this for our case, we state the following unacceptable loss:

L1: *A system requirement does not fit the users' needs.*

The unwanted event L1 reflects something that could undermine the whole project's purpose, which could deliver an unacceptable system in terms of desired results.

B. Hazards

Following the STPA steps [11], we must identify human errors influenced by the system design. A list of associated hazards might be enumerated:

H1: *The requirement does not reflect the system user's needs.*

H2: *The requirement does not reflect what the system must do.*

H3: *The Detailed Specification document does not clearly reflect the user's needs.*

With the hazard statements, we can establish Safety Constraints that will address the elaboration of needs.

C. Safety Constraints

For each identified hazard we set a high level safety constraint.

SC1.1: *The Acquisition Department must involve the system users in the requirements validation process.*

SC2.1: *The Acquisition Department must involve the system users in the detailed specification validation process.*

SC3.1: *The Acquisition Department must follow or establish a requirement writing policy.*

D. Building a Model of the Functional Control Structure

The next step in STPA is to create a system functional control model. Fig. 7 shows how a basic control loop must be implemented.

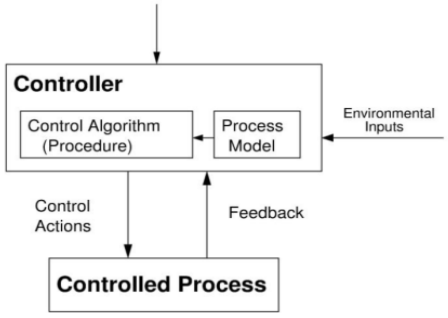
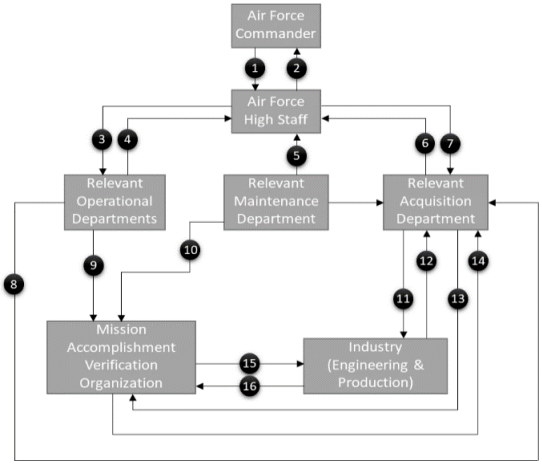


Fig. 7. Basic feedback-control loop for functional control structures

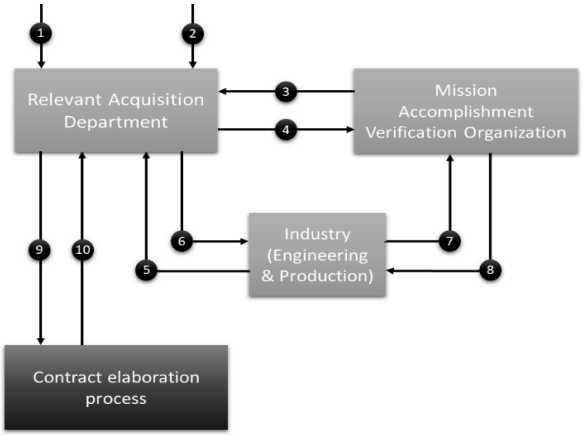
By adapting the basic control structure to the purpose of this work, the authors reached the hierarchical safety control structure shown in Fig. 8, based on the Brazilian Air Force policy over aerospace products and systems life cycle [3].



#	Control Actions	#	Control Actions
1	Project opening decision Decision on the continuation of the definition phase Contract Draft Approval	9	Specification validation
2	Feasibility survey review Definition phase review Contract draft	10	Specification validation
3	Strategic doctrine Mission triggering Operational Needs approval	11	RFI RFP WBE approval
4	Operational Needs Contract draft accord Cost forecast accord	12	Commercial offer Commercial proposal BAFO Detailed specification assessment Offset plan WBE
5	Cost forecast accord	13	Verification request
6	Feasibility survey Detailed specification proposal Cost estimate Contract draft proposal Contract formalization	14	Compliance verification
7	Operational Requirements Project order Detailed specification approval Contract formalization order	15	Verification basis approval
8	Detailed Specification assessment Contract draft support	16	Verification basis proposal Compliance demonstration

Fig. 8. Zoom in over the contract follow up control structure

This hierarchical structure embraces a dedicated contract follow-up structure, which deals with this work aim. Fig. 9 gives a zoom into this structure.



#	Control Actions	#	Control Actions
1	Detailed specification assessment	6	RFI RFP WBE approval
2	Operational Requirements	7	Verification basis proposal Compliance demonstration
3	Compliance verification	8	Verification basis approval
4	Verification request	9	Control Actions
5	Commercial offer Commercial proposal BAFO Detailed specification assessment Offset plan WBE	10	Feedback

Fig. 9. Zoom in over the contract follow up control structure

Considering the hazards and safety constraints acquired by the STPA first stages, it was possible to develop a more detailed feedback-control loop for this control structure, as shown in Fig. 10.

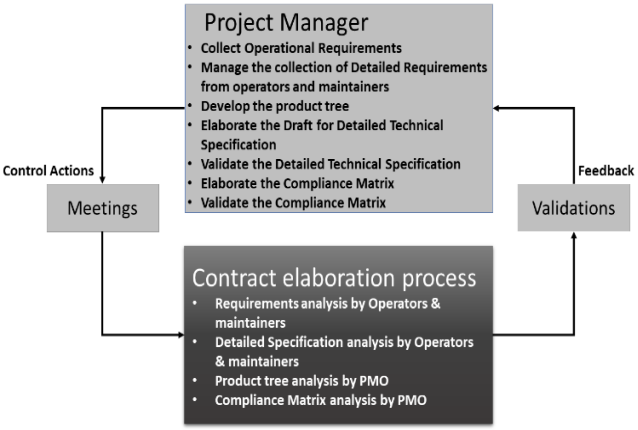


Fig. 10. Feedback-control loop: contract follow up control structure

To complete the first STPA implementation loop, we have raised control actions to meet the safety constraints and avoid the elicited hazards. Tables I to III listed the respective Unsafe Control Actions (UCA) related to the respectively identified hazards (H1, H2 and H3), according to the technique [11].

TABLE I. UCAS RELATED TO SYSTEM USERS' INVOLVEMENT IN THE REQUIREMENTS VALIDATION PROCESS

Control Action	Not providing causes hazards	Providing causes hazards	Too early, too late, out of order	Stopped too soon applied too long
The Acquisition Department involves the system users in the requirements validation process	**UCA 1.1**: The Acquisition Department does not involve one or more system users in the requirements validation process	**UCA 1.2**: The Acquisition Department involves inexperienced users of the system in the requirements validation process	**UCA 1.3**: Requirements become obsolete due to a premature involvement of system users in the requirements validation process **UCA 1.4**: Insufficient time for the requirements validation process is provided to system users	**UCA 1.5**: The Acquisition Department does not acquire enough feedback from the system users on the requirements validation process

TABLE II. UCAS RELATED TO SYSTEM USERS' INVOLVEMENT IN THE DETAILED SPECIFICATION PROCESS

Control Action	Not providing causes hazards	Providing causes hazards	Too early, too late, out of order	Stopped too soon applied too long
The Acquisition Department involves the system users in the detailed specification process	**UCA 2.1:** The Acquisition Department does not involve one or more system users in the detailed specification process	**UCA 2.2:** The system users do not understand their task over the detailed specification process	**UCA 2.3**: Requirements become obsolete due to a premature involvement of system users in the detailed specification process **UCA 2.4**: Insufficient time for the detailed specification process is provided to system users	**UCA 2.5**: The Acquisition Department does not acquire enough feedback from the system users on the detailed specification process

TABLE III. UCAS RELATED TO THE ESTABLISHMENT OF A REQUIREMENTS WRITING POLICY

Control Action	Not providing causes hazards	Providing causes hazards	Too early, too late, out of order	Stopped too soon applied too long
The Acquisition Department follows internationally recognized standards for requirements writing	**UCA 3.1:** The Acquisition Department does not follow internationally recognized standards for requirements writing	**UCA 3.2**: The Acquisition Department establishes a bad policy for requirements writing	**UCA 3.3:** The Acquisition Department adopts a method for requirements writing before the Involvement of system users **UCA 3.4:** The Acquisition Department adopts a method for requirements writing after the involvement of system users	**UCA 1.5**: The Acquisition Department does not acquire enough feedback from the system users on the requirements validation process

E. Loss Scenario

At this point of STPA analysis, it is necessary to identify the two kinds of scenarios: 1) that could lead to Unsafe Control Actions or 2) in which control actions are improperly executed or not executed at all. For the first type, it is relevant to examine the following UCA provided by the controller:

UCA 2.2: The Acquisition Department involves system users that do not understand their task over the detailed specification process.

Therefore, we should raise a relevant question in order to understand what could cause such UCA: "What are the causal factors that make the system users to not properly understand their task over the detailed specification analysis?"

The authors' experience on systems development and certification were helpful to propose some genuine reasons, shown in Table IV, to support a couple of scenarios where such UCA can find a favorable environment to happen.

Taking into consideration the scenarios that lead to the absence or improper control actions execution, the following Safety Constraints (SC) should be put under discussion:

SC: The system users must be involved in the detailed specification process.

A pertinent question that can be made about such SC is: "What are the causal factors that make the system users not being involved in the detailed specification process?" Again, the empirical authors' basis was used to set a reason for the control action disobedience, as shown in Table V.

TABLE IV. LOSS SCENARIOS RELATED TO UCA 2.2

Scenario	Associated causal factor	Requirement	Allocated to	Rationale
[Incorrect or no information is provided] The Acquisition Department does not brief the system users about what is expected from them.	Lack of adequate time to perform the detailed specification process.	An adequate time to perform the definition phase (DCA 400-6) must be considered in the Project Plan.	Project Manager	The current Brazilian Air Force project guidelines does not make clear the importance of this activity.
[Process model inconsistent, incomplete or incorrect] The current model (DCA 400-6 - (Brazilian Air Force policy for systems and products life cycle) does not consider the involvement of the Mission Accomplish-ment Verification Organization on the detailed specification process	The lack of involvement of the Mission Accomplish-ment Verification Organization can lead some specifications to be impossible to verify.	The Mission Accomplish-ment Verification Organization must be requested to assess the detailed specification validation.	Project Manager	The DCA 400-6 was issued in 2007 and has revolutionized the systems and products' development in the Brazilian Air Force. However, only after running its process over several years, it was possible to understand the importance of engaging the Mission Accomplish-ment Verification Organization as soon as possible.

TABLE V. LOSS SCENARIO RELATED TO SYSTEM USERS' INVOLVEMENT IN THE DETAILED SPECIFICATION PROCESS

Scenario	Associated causal factor	Requirement	Allocated to	Rationale
[Inadequate operation] The Acquisition Department request the detailed specification validation by the system users, but they do not have enough budget to participate in the events	Lack of financial resources to support the detailed specification validation activities.	The project plan must contemplate the specification validation phase and its expenses to finance the system users' participation on relevant events (meetings).	Project Manager	Typically, neither system users nor project managers include this activity in their budget planning.

VI. CONCLUSION

A. *Summary*

The authors' background in military aircraft certification and in the development of a NSM IFF (National Secure Mode Identification Friend-or-Foe) system, allow us to comprehend the challenging scenario of aerospace products' development in Brazil. The application of STPA over the contract elaboration process of aerospace Brazilian products has shown to be a powerful technique. It was useful to raise new requirements for aerospace products' earlier life cycle phases based on safety constraints that emerged to avoid the occurrence of genuine and relevant hazards, as demonstrated in Table 5. Such requirements (or recommendations) might be a valuable tool for writing a Handbook or Guidelines for the Brazilian Air Force contract elaboration process or, by similarity, for any other Air Force.

STPA may be deepened in several layers, depending on the detailing level the technique applier wants to reach. As it is shown in Figure 7, you can identify the system's sub-hazards (or process' sub-hazards) and subsystems hazards (or sub-process hazards) to develop the analysis. This deepening was not part of this paper scope and may be the target of future works on this topic. Nonetheless, a Brazilian Air Force Workgroup responsible for updating the policy for aerospace systems and products' life cycle is currently using the results of this effort.

B. *Work Outcome*

Based on the models developed by this work and the analysis performed by the authors, it was possible to conclude the following:

1) OPM can and should be used to model organizations' processes, providing a systemic and holistic view of its steps and the relationships between them and the involved players.

2) Using OPM to model the Brazilian Air Force Policy for Aerospace products life cycle on its earlier phases increased the understanding of the system engineering first steps of such products, easing the application of other methodologies capable of its improvement.

3) STPA can and should be used to analyze the hazards of organizations' processes, since they fit into a hierarchical control structure.

4) When applied over the Brazilian Air Force Policy for Aerospace products life cycle in its earlier phases, STPA technique has raised constraints and requirements that might be used as recommendations to improve the contract elaboration process for new acquisitions/developments.

ACKNOWLEDGMENT

The Authors thank the support of PPGAO (*Programa de Pós-Graduação em Aplicações Operacionais* - Postgraduate Program in Operational Applications) from the Aeronautics Institute of Technology, and CAPES (*Coordenação de Aperfeiçoamento de Pessoal de Nível Superior*).

REFERENCES

[1] IBM, "Get it right for the first time: Writing better requirements", *IBM Corporation, Massachusetts*, 2011, pp 9-13.

[2] Brazilian Ministry of Defense, "Estratégia Nacional de Defesa (National Defense Strategy)", 2012. Available at: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf>. Access in May 12th 2022.

[3] COMAER, "Diretriz do Comando da Aeronáutica DCA 400-6: Ciclo de vida de Sistemas e Produtos Aeronáuticos", Brasília, 2007, pp 28-38.

[4] D. Pereira, C. Hirata, and N. Tehrani, "A STAMP-based ontology approach to support safety and security analyses", *Journal of Information Security and Applications*, vol. 47, Aug. 2019, pp. 302-319.

[5] L. Li, N. Soskin, A. Jbara, M. Karpel, D. Dori, "Model-Based Systems Engineering for Aircraft Design with Dynamic Landing Constraints Using Object-Process Methodology", *AIAA SciTech Forum*, San Diego, 2019.

[6] S. Chokkadi, Y. Jeppu, "Teaching STPA and OPM to Engineering Students – Industry Academia Experiences", *Asia Oceania Systems Engineering Conference*, Bangalore, 2019.

[7] P. Checkland, "Systems Thinking, Systems Practice", *John Wiley*, Chichester, November 2000.

[8] S. Basnet, O. Banda, P. Kujala, "Review of the safety engineering techniques for a complex ship system", *7th Asia Conference on Earthquake Engineering*, 2018.

[9] N. Leveson, "Engineering a Safer World: Systems Thinking Applied to Safety", *MIT Press*, Massachusetts, 2012.

[10] N. Leveson, "Safety Analysis in Early Concept Development and Requirements Generation", *28th annual INCOSE international symposium*, Washington, July 2018.

[11] N. Leveson, J. Thomas, "STPA Handbook", *MIT Press*, 2018.