ISSN: 1983 7402 ITA, 28 a 29 SET 2021

STPA Analysis over the earlier phases of military products life cycle

Guilherme M. B. Moreira[1], Willian Limonge[2], Carlos H. N. Lahoz[1], Christopher S. Cerqueira[1], Willer G. Santos[1]
[1]Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil
[2]Instituto de Fomento e Coordenação Industrial (IFI), São José dos Campos/SP – Brasil

***Abstract* – Airworthiness Certification is a globally accepted process to attest civil aircraft safety over the compliance with a set of requirements (certification basis) that aims to avoid the occurrence of aeronautical accidents due to design issues. Considering military airworthiness, in a similar way, the mission accomplishment verification process, in a product development contracted by the Brazilian Air Force (FAB), should seek to meet the needs and capacities to be acquired by FAB to support operational units. Therefore, clear mission requirements are key points for a good contract execution. This study has made use of a robust hazard analysis technique (STPA - System-Theoretic Accident Model and Processes) in order to investigate the causal factors which leads to negative impacts on the contract elaboration process for aeronautical military products in Brazil. STPA uses System Theory to model any process as a feedback-control structure. Focusing on losses we want to avoid, the method considers the hazards, safety constraints, unsafe control actions, causal factors and based on that, proposes requirements (which can be understood as recommendations), showing a path throughout the earlier phases of Brazilian military products life cycle to improve the contract elaboration process.**

***Keywords* – STPA, mission accomplishment verification, military products life cycle.**

I. INTRODUCTION

One of the biggest challenges on projects executed by the Brazilian Air Force is to ensure that all mission accomplishment requirements set on new development contracts will be fulfilled. In the early 50's the Brazilian Air Force has started its ambitious plan to develop an aerospace industrial park, starting with the creation of ITA (Instituto Tecnológico de Aeronáutica), a technological institute based on the same principles of the famous MIT (Massachusetts Institute of Technology). Later, the Brazilian Air Force has created the IPD (Instituto de Pesquisa e Desenvolvimento), an organization to develop aerospace projects, and has fostered the creation of Embraer, which now is settled as the third biggest commercial aircraft manufacturer in the world. To close this development loop and allow the Brazilian aircraft to get into other markets, especially the American and Europeans, the Air Force has founded IFI (Instituto de Fomento e Coordenação Industrial) on the early 70's, initially responsible for the aircraft airworthiness certification [1].

Over the years, the military aviation started to adopt the civil aviation best practices, such as certification, which had substantially contributed to the reduction of the number of accidents per million of aircraft departure [2]. Tracking the evolution of military certification at the Brazilian Air Force, the operational departments got more and more confidence that certification is a powerful process, that could regard the mission accomplishment requirements verification, resulting in the entry into service of more reliable systems.

G. Moreira, moreiragmbm@ita.br; W. Limonge, limongewl@ifi.cta.br; C. Lahoz, lahoz@ita.br; C. Cerqueira, chris@ita.br, W. Santos, willer@ita.br.

One specific development program brought a new paradigm for the Brazilian military aviation certification: the medium attack aircraft AMX (also known as A-1). Its development was executed in the early 80's within a partnership between Brazil and Italy [3] and has introduced a new way to perceive the application of certification over military projects.

Hence forward IFI started to consider mission accomplishment requirements as part of the aircraft certification basis, as the Italians were already used to do.

This mindset has driven IFI's certification strategies over time, without any substantial impact on its activities during the 90's since no significant new military aircraft development has occurred during those years.

Nevertheless, this scenario has changed with the A-29 Super-Tucano, a light attack aircraft, developed by Embraer and put into service in 2003 [4]. IFI's involvement on the verification stage was very opportune for the project success.

Clear evidence of such achievement is the fact Embraer has sold more than 200 units of such aircraft. Beyond the airworthiness matters, IFI was specifically concerned on the aircraft capabilities demonstration.

The verification of mission accomplishment requirements has demonstrated to be an efficacious way to ensure that Brazilian aeronautical products met the operators' expectations. However, this task is a winding road, and the verification can become a wicked challenge if the requirements are not clearly expressed. Sometimes, the requirement writing might jeopardize the certification duty, by simply stating something unverifiable.

During the certification of the Embraer KC-390 [5], IFI has faced tremendous difficulties on performing the project compliance verification with the certification basis, despite the issuance of the DCA 400-6 [6], a policy that deals with the systems and products life cycle inside the Brazilian Air Force.

Such regulation has well organized all the systems and products life cycle phases and made the involvement of the operational and maintenance Air Force departments mandatory on the conceptual and definition project phases.

However, this doesn't always actually happen, as we are going to see throughout this work.

To optimize the mission accomplishment requirements verification and avoiding the occurrence of some dangers in the path of users' needs fulfillment, the authors sought a robust hazards analysis technique that could identify specific areas to be improved, always aiming on the Air Force mission accomplishment requirements.

This document presents an overview on the hazard analysis technique chosen to drive this study. After, the authors followed the technique steps, applying them over the earlier phases of Brazilian military products life cycle, aiming to get better requirements for the development/acquisition phases.

II. STPA OVERVIEW

STPA (System Theoretic Process Analysis) 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 handle complex systems.

The main goal of STPA is to consider both component failure and unsafe interactions of system components on the hazard analysis [8], 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 very useful for software, due to their predictable characteristics, especially considering that software is present in almost all aircraft components nowadays. Therefore, STPA came to provide functional safety requirements for the system as a whole.

Also, 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. This 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 [9]. The Fig 1 shows a scheme to help STPA users in defining the purpose of the Analysis. Notice that hazards might be refined into sub-hazards after the identification of system-level (high level) constraints.

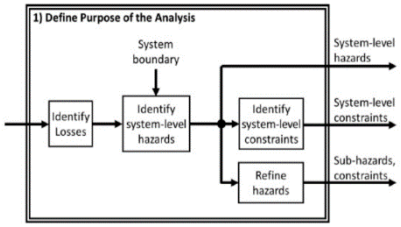


Fig. 1. Defining the purpose of the STPA Analysis

STPA is a very 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 [10], learning and applying STPA takes only 21% of the time spent in a generic industry project (Fig. 2).

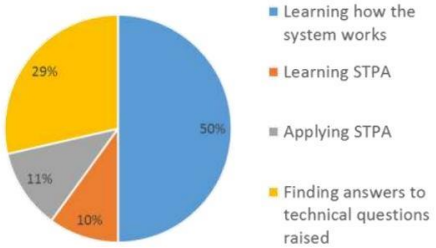


Fig. 2. Relative amount of time spent on different tasks during a recent industry STPA project [10].

The objective of this work is to raise some recommendations on the conceptual and definition phases of military aeronautical products, since those phases establish the projects' premises and, therefore, drive their success.

III. STPA HAZARD ANALYSIS

A. Losses

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

According to [11], requirements are the key to project success and projects' objective is to solve a problem experienced by users. Taking this into consideration for our case, the following unacceptable loss is stated:

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

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

B. Hazards

Following the STPA steps [8][11], we must identify human errors influenced by the system design. Some 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 not clearly reflect the user needs.*

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

C. Safety Constraints

For each identified recommendations (requirements) for a modeled system, i.e., the components considered on contract elaboration process for military aeronautical products and their relationships.

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

SC2.1: *The Acquisition Department must involve the system users on 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 3 shows how a basic control loop must be implemented.

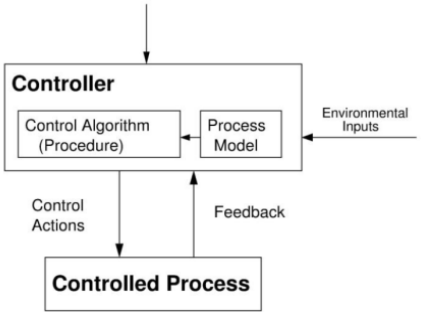
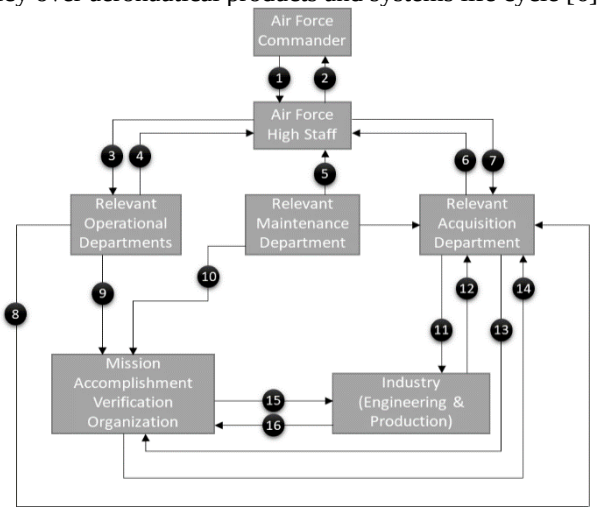


Fig. 3. Basic feedback-control loop used in functional control structures.

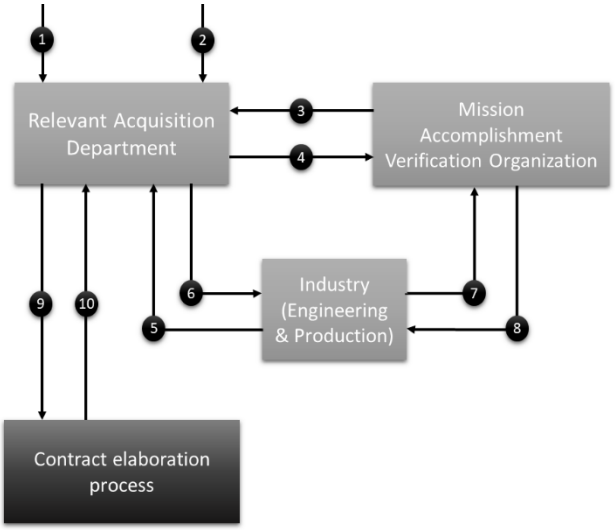
By adapting the basic control structure to the purpose of this work, the authors reached the hierarchical safety control structure shown on Fig. 4, based on the Brazilian Air Force policy over aeronautical products and systems life cycle [6].



#	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. 4. Adapted hierarchical safety control structure for conception, feasibility and definition phases according to [6].

This hierarchical structure embraces a dedicated contract follow-up structure which deals with this work aim. The Fig. 4 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. 4. Zoom in over the contract follow up control structure

We can now find the main controller connections of our relevant system, that is, the Relevant Acquisition Department, responsible for managing the contract follow-up process and, particularly, the contract elaboration. 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 on Fig. 5.

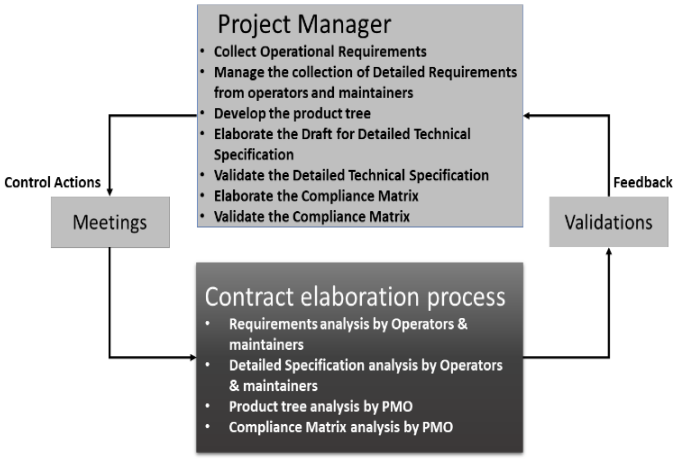


Fig. 5. Feedback-control loop on contract follow up control structure

To complete the first STPA implementation loop, we have raised some control actions to meet the safety constraints and avoid the elicited hazards. Tables 1 to 3 listed the respective Unsafe Control Actions (UCA) related to respective identified hazards (H1, H2 and H3), according to the technique.

Table 1: UCAs related to system users' involvement on the requirements validation process

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
The Acquisition Department involves the system users on the requirements validation process	**UCA 1.1**: The Acquisition Department does not involve one or more system users on the requirements validation process	**UCA 1.2**: The Acquisition Department involves unexperienced users of the system on the requirements validation process	**UCA 1.3**: Requirements become obsolete due a premature involvement of system users on 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 doesn't acquire enough feedback from the system users on the requirements validation process

Table 2: UCAs related to system users' involvement on the detailed specification process

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
The Acquisition Department involves the system users on the detailed specification process	**UCA 2.1**: The Acquisition Department does not involve one or more system users on the detailed specification process	**UCA 2.2:** The system users don't understand their task over the detailed specification process	**UCA 2.3**: Requirements become obsolete due a premature involvement of system users on 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 doesn't acquire enough feedback from the system users on the detailed specification process

Table 3: UCAs related to the establishment of a requirements writing policy

Control Action	Not providing causes hazard	Providing causes hazard	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 doesn't 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 3.5:** The Acquisition Department interrupt the application of a requirements writing policy before the involvement of system users

E. Loss Scenario

At this point of STPA analysis, it's 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's relevant to examine the following UCA provided by the controller:

UCA 2.2: *The Acquisition Department involves system users that don't understand their task over the detailed specification process.*

We should, therefore, 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 can help to raise some real reasons, on Table 4, to support a couple of scenarios where such UCA can find a propitious environment to happen.

Table 4: Loss scenarios related to UCA 2.2

Scenario	Associated Causal Factor	Requirement	Allocated to	Rationale
[Incorrect or no information is provided] The Acquisition Department doesn't brief the system users about what is expected from them.	Lack of an adequate time to perform the detailed specification process.	An adequate time to perform the definition phase (DCA 400-6) must be considered on the Project Plan.	Project Manager	The current Brazilian Air Force project guidelines doesn't 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) doesn't consider the involvement of the Mission Accomplishment Verification Organization on the detailed specification process	The lack of involvement of the Mission Accomplishment Verification Organization can lead some specifications to be impossible to verify.	The Mission Accomplishment 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 on the Brazilian Air Force. However, only after running its process over several years it was possible to understand the importance to engage the Mission Accomplishment Verification Organization as soon as possible.

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

SC: *The system users must be involved on 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 to be involved on the detailed specification process?" Again, the empirical authors' basis was used to set a reason that conducts to the control action disobedience, as shown on Table 5.

Table 5: Loss scenario related to system users' involvement on 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 don't have enough budget to participate on 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.

IV. CONCLUSIONS

After eight years of experience working on the Brazilian military aircraft certification at IFI and three years as Project Manager of a NSM IFF (National Secure Mode Identification Friend-or-Foe) system, aiming its integration on the SAAB new Gripen E/F, the main author has accumulated enough experience to comprehend the challenging scenario that is the development of aeronautical products in Brazil. The application of STPA over the contract elaboration process on aeronautical military Brazilian products has shown to be a powerful technique, which could raise new requirements for the earlier phases of FAB's products life cycle based on safety constraints that emerged to avoid the occurrence of real and relevant hazards, as demonstrated on Table 5. Such requirements (or recommendations) could be a useful tool to write a Handbook or Guidelines about the contract elaboration process of FAB or, by similarity, of any other Air Force.

The authors believe that the method can be helpful in modeling the initial phases of the Brazilian policy over systems and products life cycle, issued in 2007, and has brough to light some realistic and useful proposals to update such policy in order to assist the Brazilian Air Force to elaborate better development contracts.

Obviously, this work can be refined in several other layers, modeling the system of interest, and seeking a better description of the user needs throughout the STPA technique.

REFERENCES

[1] O. Silva, "Casimiro Montenegro Filho: A trajetória de um visionário. Vida e obra do criador do ITA", Bizz Editorial, 2006.

[2] Boeing, "Statistical Summary of Commercial Jet Airplane Accidents: Worldwide Operations | 1959 – 2016", July 2017. Available at: <https://www.skybrary.aero/bookshelf/books/4239.pdf>. Access in 15/06/2021.

[3] D. Donald et al, "The Encyclopedia of World Military Aircraft", NY: Barnes & Noble, 2000, p. 29-31.

[4] Embraer, "C-390 Millennium", 2021. Available at https://defense.embraer.com/br/pt/c-390. Access in 03/07/2021.

[5] Embraer, "Embraer entrega o primeiro ALX Super-tucano à Força Aérea Brasileira", December 2003. Availabe at <https://embraer.com/br/pt/noticias?slug=1746-embraer-entrega-oprimeiro-alx-super-tucano-a-orca-aerea-brasileira>. Access in: 15/06/2021.

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

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

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

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

[10] N. Leveson, J. Thomas, "STPA Handbook", MIT, Cambridge, March 2018.

[11] IBM, "Get it right for the first time: Writing better requirements", IBM Corporation, Massachusetts, 2011.