Enhancing Brazilian Aerospace Systems Lifecycle Directive

Guilherme Moreira[1], Daniel Pleffken[1], Christopher Cerqueira[1] e Willer Santos[1]
[1]Instituto Tecnológico de Aeronáutica, São José dos Campos/São Paulo - Brazil

***Abstract*— This paper proposes an update to the Brazilian Air Force's directive DCA 400-6, incorporating principles from the Ministry of Defense's MD 40-M-01 and integrating System Theoretic Process Analysis (STPA) into the lifecycle management framework for aerospace systems. The comparative analysis reveals that the MD 40-M-01 emphasizes continuous improvement, risk management, and stakeholder involvement, which are less pronounced in the DCA 400-6. By aligning with international standards such as ISO/IEC/IEEE 15288, the revised directive aims to enhance operational efficiency, safety, and reliability. The proposed Vee-Model includes critical milestones and integrates STPA into requirement definition phases, ensuring comprehensive hazard analysis and robust safety measures from the earliest stages of system development. This paper outlines the necessary steps for these updates and provides a detailed rationale for the proposed changes, setting a foundation for future aerospace systems engineering and management advancements.**

***Keywords*— Lifecycle Management, System Theoretic Process Analysis (STPA), ISO 15288 Compliance**

I. Introduction

In the realm of defense and aerospace, the continuous evolution of standards and methodologies is paramount to maintaining operational efficiency, safety, and technological advancement [1]. The Brazilian Air Force's directive, DCA 400-6, entitled *Life Cycle of Brazilian Aeronautical Systems and Materials*, established in 2007, provides a comprehensive framework for the life cycle management of aeronautical systems and materials [2]. However, the rapidly changing landscape of defense technologies and methodologies necessitates an update to ensure alignment with contemporary best practices and higher hierarchical directives. This paper proposes an update to the DCA 400-6, incorporating insights and methodologies from the more recent MD 40-M-01 (2019), entitled *Manual of Good Practices for Life Cycle Management of Defense Systems*, of the Ministry of Defense [3], and introducing the System Theoretic Process Analysis (STPA), one of the most modern and robust risk analysis methods [4], as a standard method for eliciting system requirements.

The responsibility for issuing and updating the Manual MD 40-M-01 is the Brazilian Ministry of Defense, a institution hierarchically superior to the Air Force Command, which is the issuer of DCA 400-6. Also, this manual is a more modern document, offering an enhanced approach to life cycle management, emphasizing continuous improvement, risk management, and alignment with international standards such as ISO/IEC/IEEE 15288 [5]. This manual's comprehensive structure and up-to-date practices provide a robust foundation for modernizing the DCA 400-6. By integrating MD 40-M-01's principles, we can ensure that the lifecycle management processes are not only current but also superior in addressing the complexities and demands of contemporary defense systems.

G. Moreira, gui.moreira@gmail.com; D. Pleffken, rondon@ita.br; C. Cerqueira, chris@ita.br; W. Santos, willer@ita.br.

Furthermore, the incorporation of STPA into the DCA 400-6 presents a transformative approach to hazard analysis and requirements definition. Developed by Nancy Leveson at MIT, STPA extends traditional safety analysis methods by considering the complex interactions and controls within systems. This method is particularly advantageous for identifying and mitigating potential hazards early in the system development process, ensuring comprehensive and systemic risk management [6].

By updating the DCA 400-6 with the principles from MD 40-M-01 and incorporating STPA, the Brazilian Air Force may improve its capability to manage the lifecycle of its systems more effectively. This integration will not only align the DCA 400-6 with modern standards but also establish a proactive framework for hazard analysis and requirements definition, aiming for the improvement of the processes for development and acquisition of systems that must be safe, reliable, and operationally effective. This paper will delve into the specifics of these updates, providing a detailed rationale and methodology for the proposed changes.

To this end, Section II, Theoretical Framework, provides a basic foundation of the concepts explored in this study. In Section III, Related Documentation, this article presents and discusses other studies and guidelines that address the topic of this proposal. Section IV, Methods, depicts a comparative table describing the similarities and differences between DCA 400-6 and MD 40-M-01. Additionally, this section also introduces a Vee-Model that integrates the STPA method into the definition of requirements for DCA 400-6, as well as establishes the milestones that mark the transitions between the various stages according to best practices in Systems Engineering. Finally, Section V, Conclusions, presents the closing of the article, highlighting the key findings, important insights for the implementation of the ideas discussed herein, and proposals for future work that can contribute to the advancement of this study.

II. Theoretic Framework

The integration of modern methodologies and standards is critical for the effective lifecycle management of defense systems [7]. This theoretical framework explores the intersection of the Brazilian Air Force's directive DCA 400-6, the Ministry of Defense's MD 40-M-01, and the System Theoretic Process Analysis (STPA) method. By aligning DCA 400-6 with MD 40-M-01 and incorporating STPA, we aim to enhance the formulation of system requirements, ensuring they meet contemporary standards of safety and efficacy.

A. DCA 400-6

The DCA 400-6, published in 2007, provides a structured approach to managing the lifecycle of aeronautical systems within the Brazilian Air Force. It outlines the stages from conception, development, and acquisition to operation and disposal. This directive emphasizes thorough planning, execution, and continuous improvement to maintain operational readiness and efficiency [2].

However, as technological advancements and operational requirements evolve, so must the frameworks governing them. The DCA 400-6, while comprehensive, lacks integration with modern lifecycle management practices and the latest safety analysis methodologies.

The DCA 400-6 uniquely names some important concepts for the stages preceding the entry into service of Brazilian military aeronautical products, which are aligned with practices already adopted in Systems Engineering:

1) NOP (Operational Need): An identified deficiency or shortfall, formalized in a specific document of the same name, whose resolution, to fully achieve the mission of the Brazilian Air Force, depends on the provision of a new System or Material, or modifications to an existing one.
2) ROP (Operational Requirements): A document issued by the Brazilian Air Force High Staff, based on the NOP, that provides the initial description of the performance characteristics that the System or Material must exhibit, in both qualitative and quantitative terms, considering its mission or application and its safety in service.
3) RTLI (Technical, Logistics, and Industrial Requirements): A document derived from the ROP that establishes the technical, logistical, and industrial characteristics that the System or Material must have to meet the established operational requirements.
4) AVOP (Operational Evaluation): A mandatory contractual activity that must be conducted immediately after the conclusion of the System or Material development, and preferably before the start of its large-scale serial production. The objective is to verify whether the functional characteristics of each component of the System or Material comply with the operational and logistical requirements, as well as the technical specifications outlined in the contract, thereby preliminarily obtaining the parameters of Operational Reliability, Logistical Reliability, Maintainability, and Availability.

B. MD 40-M-01

The MD 40-M-01, published in 2019, is a more recent and superior hierarchical document that provides best practices for lifecycle management of defense systems. This manual emphasizes continuous improvement, risk management, and adherence to international standards such as ISO/IEC/IEEE 15288. It introduces a holistic approach, integrating technical, logistical, and operational aspects throughout the system's lifecycle [3]. The key elements of MD 40-M-01 are:

1) Continuous Improvement: Aligns with ISO 9001 standards, promoting ongoing enhancement of processes and systems.
2) Risk Management: Proactive identification and mitigation of risks, ensuring safety and reliability.
3) Integrated Lifecycle Management: Seamlessly connects various lifecycle phases, ensuring coherent transitions and sustained operational effectiveness.

The MD 40-M-01's emphasis on modern lifecycle management practices makes it a suitable foundation for updating the DCA 400-6. By adopting its principles, the Brazilian Air Force can align with international best practices and enhance its operational capabilities.

C. System Theoretic Process Analysis (STPA)

STPA is a cutting-edge methodology for hazard analysis and requirements generation. Unlike traditional safety analysis methods that focus on component failures, STPA addresses complex interactions and control issues within a system. This systems-theoretic approach is particularly effective for modern, highly integrated systems where traditional methods may fall short.

Utilizing STPA over traditional risk analysis methods such as Fault Tree Analysis (FTA) or Failure Modes and Effects Analysis (FMEA) is justified due to its ability to comprehensively address both component failures and unsafe interactions within complex systems [6]. Unlike traditional methods, which often focus on linear cause-effect relationships and component-specific failures, STPA employs a systems-theoretic approach that considers the entire system as a dynamic control structure. This enables the identification of hazards arising from interactions among system components, including software and human operators, which are critical in the context of modern, highly integrated systems.

Fundamentals of STPA [8]:

1) System-Level Hazards: Identifies hazards arising from system states and interactions rather than individual component failures.
2) Control Structures: Analyzes how control actions can lead to unsafe states, ensuring comprehensive hazard identification and mitigation.
3) Iterative Process: Allows for continuous refinement and improvement, adapting to new information and system changes.
4) Unsafe Control Actions (UCAs): Identifies the actions that could lead to the identified hazards.
5) Loss Scenarios: Elaborate the scenarios where the UCAs may happen.
6) Requirements: Generate the necessary requirements to avoid the Loss Scenarios occurrence.

Fig. 1 depicts the STPA phases. The first phase can be used to elicit high level requirements, and the fourth and last phase may generate detailed technical requirements.

By incorporating STPA into the DCA 400-6 framework, the Brazilian Air Force may have a useful tool to improve its hazard analysis capabilities, ensuring robust and comprehensive safety measures.

III. Related Documentation

There are several works, guidelines and case studies that discuss the application of STPA for improving internal standards in organizations that manage complex product

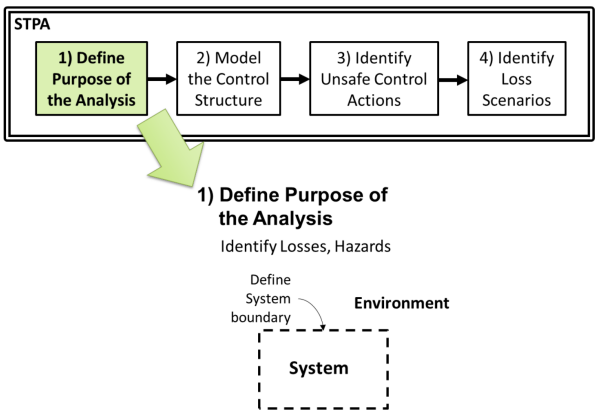

Fig. 1. STPA phases [8].

lifecycles. These studies span various industries, including aerospace, automotive, and energy sectors, emphasizing the versatility and effectiveness of STPA in enhancing safety and operational standards.

A study by Karatzas and Chassiakos (2020) explored the use of STPA for hazard analysis within demand response systems in smart grids. The implementation of STPA in this context provided insights into operational risks and helped in identifying and mitigating potential hazards in the system. The findings highlighted the utility of STPA in enhancing safety standards and operational efficiency in complex energy systems [9].

The SAE International document J3187_202305 outlines recommended practices for applying STPA to safety-critical systems across various industries, including automotive. This document provides a comprehensive framework for integrating STPA into the safety assessment processes, demonstrating its applicability in refining internal safety standards and improving hazard identification and mitigation strategies [10].

In another study, the authors, utilize Object Process Methodology (OPM) and STPA to model and analyze the earlier phases of aerospace products lifecycle [11]. The main goal is to enhance an acquisition and development policy by focusing on the conceptual and definition phases of the product lifecycle. The study models the conceptual feasibility and definition phases, highlighting the importance of these early stages in setting the foundation for successful project execution. The model is divided into five layers, covering various stages from initial concept to contract signing. STPA identifies hazards and unsafe control actions that could lead to unacceptable losses, such as requirements not meeting user needs. The study establishes safety constraints to address these hazards and improve the contract elaboration process. Their main findings are:

1) Involvement of Users: Emphasizes the need for involving system users in the requirements validation and detailed specification processes to ensure that the final product meets operational needs.
2) Requirements Writing Policy: Recommends establishing a standardized policy for writing requirements to avoid ambiguities and ensure clarity.

IV. Methods

This section details the methodologies employed in the comparative analysis of the DCA 400-6 and MD 40-M-01 regulations, as well as the development of a proposed Vee-Model integrating STPA into the DCA 400-6 framework. The aim is to enhance the lifecycle management of Brazilian aerospace defense systems by leveraging modern methodologies and aligning with superior regulatory standards.

A. Comparative Analysis of DCA 400-6 and MD 40-M-01

To systematically compare the DCA 400-6 (2007) and MD 40-M-01 (2019) regulations, a structured approach was employed, summarized at Table I. The process involved:

1) Document Analysis: A thorough review of both regulations was conducted to identify their scope, objectives, and specific directives regarding the lifecycle management of aerospace systems.
2) Criteria Definition: Key criteria for comparison were defined, including lifecycle phases, risk management, continuous improvement, stakeholder involvement, and alignment with international standards.
3) Comparison Table: Table I was created to highlight the similarities and differences between the two documents, providing a clear and concise overview of their respective approaches and requirements.

The comparative analysis revealed the following critical insights:

1) Lifecycle Management: Both regulations emphasize a structured approach to lifecycle management, but MD 40-M-01 incorporates more modern practices and international standards (ISO/IEC/IEEE 15288).
2) Risk Management: MD 40-M-01 provides a more proactive approach to risk management, integrating continuous risk assessment throughout the lifecycle. DCA 400-6 primarily focuses on traditional risk management techniques.
3) Continuous Improvement: MD 40-M-01 emphasizes continuous improvement and feedback mechanisms, aligning with ISO 9001 standards. DCA 400-6 lacks explicit directives on continuous improvement.
4) Stakeholder Involvement: MD 40-M-01 mandates extensive stakeholder involvement in all phases of the lifecycle, ensuring comprehensive requirements capture and validation. DCA 400-6 has less emphasis on stakeholder engagement.

In order to address Risk Management and Continuous Improvement compliance, the proposed DCA 400-6 modifications include the integration of STPA to its Decomposition and Definitions stages.

B. Integration of STPA to the DCA 400-6

The Vee-Model is a widely recognized systems engineering framework that emphasizes the decomposition and definition of requirements on the left side of the ”V” and integration and verification on the right side [12]. It ensures a structured approach to system development and verification, promoting traceability and alignment between requirements and final products.

TABLE I

COMPARISON BETWEEN DCA 400-6 AND MD40-M-01

Characteristics	Document	DCA 400-6	MD40-M-01
	Year of Publication	2007	2019
Similarities	Goal	Ensure efficiency and effectiveness in the management of systems and materials	Ensure efficiency and effectiveness in the management of systems and materials
	Lifecycle Framework	Uses process following specific phases	Uses process following specific phases
	Modernization and Improvement Phase	Highlights the importance of modernizing and improving systems and materials to maintain technological and operational relevance	Highlights the importance of modernizing and improving systems and materials to maintain technological and operational relevance
	Planning and Implementation	It emphasizes the need for detailed planning and structured implementation for each phase of the life cycle	It emphasizes the need for detailed planning and structured implementation for each phase of the life cycle
	Definition of Terms	Provides clear, detailed definitions of technical and operational terms	Provides clear, detailed definitions of technical and operational terms
Differences	Technological Update	Less emphasis on modern management concepts and continuous innovation	It includes more modern life cycle management practices, such as continuous improvement concepts, alignment with international standards (ISO/IEC/IEEE 15288), and a more integrated and updated approach to life cycle phases
	Continuous improvement approach	Focuses on revitalizations and modernizations as the need arises	It includes continuous improvement as a fundamental part of life cycle management, following standards such as ABNT NBR ISO 9000:2004, and emphasizes the identification of non-conformities and constant corrective/preventive actions
	Risk and Opportunity Management	Focuses more on traditional operational and logistical procedures	It adopts a proactive approach to managing risks and opportunities, integrating manufacturing readiness concepts (Manufacturing Readiness Level - MRL) and technological maturity assessment practices
	Hierarchy and Applicability	Specific to the Brazilian Air Force, with a clear hierarchy of responsibilities within the COMAER structure	More comprehensive and hierarchically superior document, applicable to all Brazilian Armed Forces, with a more integrated and multidisciplinary view of the life cycle management of defense systems

STPA is integrated into the Vee-Model to enhance hazard analysis and requirements definition, applying its first phase to the ROP (Operational Requirements elicitation phase), aiming the addressing of all Safety Constraints to avoid the identified hazards. Further into next stage of system's Decomposition and Definition of requirements, we integrate SPTA's phases 2 to 4, in order to generate technical requirements as RTLI.

The proposed Vee-Model for DCA 400-6, depicted in Fig. 2, also includes critical milestones that delineate transitions between various phases of a project's lifecycle. Most of these milestones are derived from ISO/IEC/IEEE 15288:2015, reinforcing the aim of this work to propose a more aligned version of DCA 400-6 with the corresponding manual of the Ministry of Defense. Those milestones' aims are:

1) MCR (Mission Concept Review): The MCR affirms the mission need and examines the proposed mission's objectives and the concept for meeting those objectives [13].
2) ASR (Alternative Systems Review): This review assesses alternative solutions and ensures that the selected system concept meets the operational needs and requirements. It evaluates the feasibility and risks associated with different options [14].
3) SRR (System Requirements Review): This milestone ensures that system requirements are complete, feasible, and verifiable. It confirms that the requirements are correctly defined and meet the needs of stakeholders [14].
4) SFR (System Functional Review): This review focuses on the system's functional baseline, verifying that all functional requirements are properly defined and allocated. It ensures that the system's functional architecture can meet the specified requirements [14].
5) PDR (Preliminary Design Review): This review assesses the preliminary design against the system requirements. It ensures that the design approach meets all functional and performance requirements and is ready to proceed to detailed design [14].
6) CDR (Critical Design Review): The CDR confirms that the detailed design meets all system requirements with acceptable risk and is ready for full-scale development. It evaluates the design maturity and completeness [14].
7) TRR (Test Readiness Review): This milestone ensures that the system and its components are ready for testing. It verifies that the test procedures, facilities, and configurations are prepared for execution [14].
8) SVR (System Verification Review): The SVR verifies that the system meets all specifications and requirements. It usually occurs together with the FCA (Functional Configuration Audit) to ensure that the final system configuration matches the documented specifications and requirements [14].
9) PRR (Production Readiness Review): This review assesses the readiness of the system for production. It ensures that the production processes, tools, and facilities are in place and capable of producing the system to the required specifications [14].
10) PCA (Physical Configuration Audit): The PCA verifies that the physical configuration of the system matches the documented design and requirements. It is typically performed before system delivery to ensure all configuration items are properly documented and controlled [14].

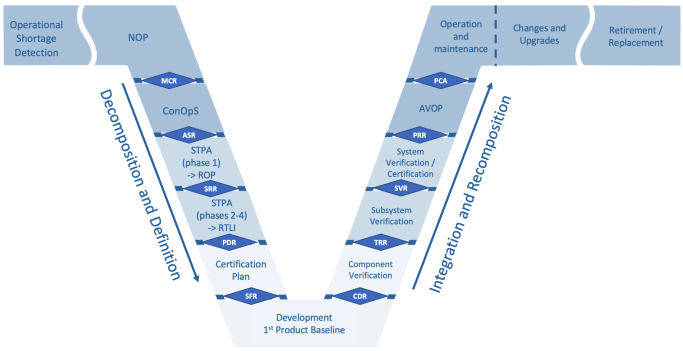

Fig. 2. Proposed Vee-Model for DCA 400-6

C. Implementation of the Proposed Model

The implementation of the proposed Vee-Model integrating STPA methods involves several critical steps to ensure its

effectiveness and applicability across projects. Initially, training and familiarization are essential, involving comprehensive training sessions for stakeholders and project teams on the Vee-Model and STPA methodologies. This foundational step ensures that all participants understand the concepts, processes, and objectives of the new model.

Following the training phase, pilot projects should be executed to validate the proposed model's effectiveness and identify areas for improvement. These projects serve as practical tests, allowing the model to be applied in real-world scenarios and providing valuable insights into its strengths and potential shortcomings.

Based on the feedback collected from the pilot projects, the model may be iteratively refined. This iterative process involves analyzing the feedback, making necessary adjustments, and continually improving the model to address any issues identified during this validation phase.

Once the model has been refined and validated through real projects, it cab be rolled out across all relevant projects. This full-scale implementation ensures consistent application of the refined model and incorporates continuous monitoring to maintain its effectiveness and adapt to any emerging challenges or changes in project requirements.

This structured approach to implementing the proposed V-Model ensures a thorough, practical, and adaptable integration of the new methodologies, ultimately enhancing the lifecycle management of aerospace systems.

V. Conclusions

This paper has presented a comprehensive approach to modernizing the DCA 400-6 directive of the Brazilian Air Force by updating its principles based on the more recent document MD 40-M-01 and incorporating System Theoretic Process Analysis (STPA) into the systems engineering framework. The proposed enhancements aim to align the lifecycle management of aerospace systems with contemporary best practices and international standards, thereby improving operational efficiency, safety, and reliability.

A. Key Findings

The comparative analysis between DCA 400-6 and MD 40-M-01 highlighted several areas where the older directive could benefit from updates. The MD 40-M-01 emphasizes continuous improvement, proactive risk management, and comprehensive stakeholder involvement, which are less pronounced in the DCA 400-6. By integrating these elements, the revised DCA 400-6 can ensure better alignment with international standards such as ISO/IEC/IEEE 15288, fostering a more robust and effective lifecycle management process.

The proposed V-Model, adapted for DCA 400-6, incorporates critical milestones and integrates STPA into the requirement definition and detailing phases. This integration facilitates a more thorough hazard analysis and ensures that safety constraints are considered from the earliest stages of system development. The inclusion of a Mission Concept Review (MCR) further strengthens the project validation process by ensuring strategic alignment and feasibility before advancing to more detailed phases.

B. Implementation Insights

The structured implementation approach, beginning with training and familiarization, followed by pilot projects, iterative refinement, and full-scale rollout, ensures that the proposed model is both practical and adaptable. This phased implementation strategy allows for the collection of feedback and continuous improvement, thereby increasing the likelihood of successful adoption across relevant projects.

C. Future Work

Future research should focus on further refining the integration of STPA within the V-Model to enhance its applicability and effectiveness. Specific areas of interest include developing detailed guidelines for conducting STPA in various phases of the lifecycle and exploring the use of advanced tools and technologies to support STPA implementation.

Additionally, scientific work implementing the model proposed in this article in pilot projects, and establishing metrics for evaluating its effectiveness, can significantly contribute to demonstrating the concepts explored here.

References

[1] M. R. Guldal and J. Andersson, "Integrating process standards for system safety analysis to enhance efficiency in initial airworthiness certification of military aircraft: A systems engineering perspective," in *INCOSE International Symposium*, vol. 30, no. 1. Wiley Online Library, 2020, pp. 589–603.

[2] C. d. A. Ministério da Defesa, *Ciclo de Vida de Sistemas e Materiais da Aeronáutica*, Comando da Aeronáutica, Brasília, Brasil, Mar. 2007, portaria Nº129/GC4, de 5 de março de 2007.

[3] E.-M. C. d. F. A. Ministério da Defesa, *Manual de Boas Práticas para a Gestão do Ciclo de Vida de Sistemas de Defesa*, Ministério da Defesa do Brasil, Brasília, Brasil, 2019, instrução Normativa Nº1/EMCFA-MD, de 10 de janeiro de 2020.

[4] R. Hegde, S. Yako, K. Post, and S. Nuesch, "Systems theoretic process analysis for layers of system safety," in *INCOSE International Symposium*, vol. 29, no. 1. Wiley Online Library, 2019, pp. 895–909.

[5] K. Collyer, L. Wright, and A. Hill, "The iso-15288 technical processes, system maturity, and conceptual gaps," in *INCOSE International Symposium*, vol. 32, no. 1. Wiley Online Library, 2022, pp. 636–647.

[6] N. G. Leveson, "Safety analysis in early concept development and requirements generation," in *INCOSE International Symposium*, vol. 28, no. 1. Wiley Online Library, 2018, pp. 441–455.

[7] P. Crowe, A. Mostashari, M. Mansouri, and R. Cloutier, "9.2. 1 reference framework and model for integration of risk management in agile systems engineering lifecycle of the defense acquisition management framework," in *INCOSE International Symposium*, vol. 19, no. 1. Wiley Online Library, 2009, pp. 1391–1405.

[8] N. G. Leveson and J. P. Thomas, *STPA Handbook*, MIT, Cambridge, Massachusetts, Mar. 2018. [Online]. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[9] S. Karatzas and A. Chassiakos, "System-theoretic process analysis (stpa) for hazard analysis in complex systems: the case of "demand-side management in a smart grid"," *Systems*, vol. 8, no. 3, p. 33, 2020.

[10] *System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry*, SAE International Std. J3187_202 305, May 2023, recommended practices regarding how STPA may be applied to safety-critical systems. [Online]. Available: https://www.sae.org/standards/content/j3187_202305/

[11] G. Moreira, D. R. Pleffken, C. Cerqueira, and W. Santos, "Stpa analysis over the earlier phases of brazilian aerospace products life cycle using opm," in *2022 13th International Conference on Mechanical and Aerospace Engineering (ICMAE)*. IEEE, 2022, pp. 465–471.

[12] C. S. Wasson, *System engineering analysis, design, and development: Concepts, principles, and practices*. John Wiley & Sons, 2015.

[13] NASA, "Nid 7123.69: Nasa interim directive for systems engineering," NASA Office of the Chief Engineer, Tech. Rep., Jun. 2023, accessed: 2024-06-15. [Online]. Available: https://nodis3.gsfc.nasa.gov/OPD_docs/NID_7123_69_.pdf

[14] International Organization for Standardization, “Iso/iec 81702:2023 information technology — systems and software engineering — systems and software assurance — part 1: Concepts and vocabulary,” ISO, Tech. Rep., 2023, accessed: 2024-06-15. [Online]. Available: https://www.iso.org/standard/81702.html