

# SpaceX Starship SN10 Prototype Safety Analysis: A Case Study on Organization's Needs Management

Joel Carlos Vieira Reinhardt<sup>1,2\*</sup> , Mariana de Freitas Dewes<sup>3</sup> , Odair Lelis Gonzalez<sup>4</sup> , Carlos Henrique Netto Lahoz<sup>5</sup> 

1. Departamento de Ciência e Tecnologia Aeroespacial  – Instituto Tecnológico de Aeronáutica – Programa de Pós-Graduação em Ciências e Tecnologias Espaciais, Área de Gestão Tecnológica – São José dos Campos/SP – Brazil.
2. Departamento de Ciência e Tecnologia Aeroespacial  – Instituto de Fomento e Coordenação Industrial – Divisão de Certificação de Produto Aeroespacial – São José dos Campos/SP – Brazil.
3. Universidade Federal de Ciências da Saúde de Porto Alegre  – Curso de Bacharelado em Gestão em Saúde – Porto Alegre/RS – Brazil.
4. Departamento de Ciência e Tecnologia Aeroespacial  – Instituto de Estudos Avançados – Divisão de Energia Nuclear – São José dos Campos/SP – Brazil.
5. Departamento de Ciência e Tecnologia Aeroespacial  – Instituto de Aeronáutica e Espaço – Divisão de Eletrônica – São José dos Campos/SP – Brazil.

\*Correspondence author: joel.reinhardt@gmail.com

## Abstract

This study addresses the inadequacy of conventional failure analyses, which, in addition to regulatory and customer requirements, often neglect organizational needs. It emphasizes the importance of a systemic approach to mitigating hazards in complex space program management. This article proposes a new approach to addressing security issues that adds the management of security-related organizational needs to systemic engineering analysis. The case study of the catastrophic event involving SpaceX's Starship SN10 prototype used publicly available information to build the system-theoretic accident model and processes (STAMP) model and identify organizational needs. The causal analysis based on systems theory (CAST) method was then applied to identify possible causes. Finally, the system-theoretic process analysis (STPA) method was used to determine design-related organizational needs and formulate recommendations for the design of the autogenous pressurization system. The presented method considered organizational needs to identify the key elements involved in the accident, the primary causes, and the actions to mitigate the associated hazards. This study proposed that managing organizational needs for system safety requires recognizing the current situation and constructing prospective scenarios to prevent failures, while emphasizing the importance of management's proactive measures, clear responsibilities, and active involvement of all members to ensure system reliability.

**Keywords:** System safety; Causal analysis; Accident modeling; Organizational requirements.

## INTRODUCTION

The complexity of space programs demands an approach to mitigate risks associated with unsafe decisions. Traditional models, such as the bow-tie model, assume that accidents are a linear chain of events, which is not applicable when multiple causes are complexly interconnected (Sultana and Haugen 2023). Conventional failure analysis in processes proves inadequate, as various factors such as contractual, economic, production, logistical aspects, and the complexity of long-term training significantly impact

**Received:** May 12, 2024 | **Accepted:** Oct. 14, 2024

**Section editor:** Alison Moraes 

**Peer Review History:** Single Blind Peer Review



costs, production halts, and the organization's revenue (Leveson 2017). While management systems guide strategic decisions, they are currently structured to meet clients' and normative requirements, neglecting the management of organizational needs. Since satisfying these needs is the organization's *raison d'être* (Seleme and Stadler 2012), it is crucial for the management system to be guided by the identification and prioritization of actions to meet such needs. By adopting a prospective scenario-based approach, management aligns its efforts to identify and meet the organization's needs, replacing managerial desires with formally established goals to build the strategically necessary future state. This realignment aims to transform the organization's current state into the required future state, promoting an active and adaptive managerial posture. Managing organizational needs provides a quality framework and organizational performance, adjusting strategies and minimizing risks associated with changes or management errors. In the aerospace sector, stakeholder polarization and aversion to high financial risk make it challenging to achieve satisfactory results through a strategy solely based on requirements established for the satisfaction of various stakeholders, many of whom are unknown to the end-user of aerospace technology. Therefore, the central problem is the need for a systemic approach that considers and prioritizes organizational needs to mitigate risks and ensure safe decisions in space programs.

This article proposes a new approach to addressing security issues by incorporating the management of security-related organizational needs into systemic engineering analysis. The research investigated how managing an organization's needs can enhance the systemic security analysis of space programs. It focused on analyzing organizational needs and managerial and technical factors that impact the security of space programs. The motivations and individual needs of employees involved in the studied organization were not included in this study, and implementation is not in scope; and it could be done in future research.

During a spacecraft failure, the initial stage of operational recovery procedures commonly involves system deactivation, activation of the self-check process, and the implementation of a subset of other monitoring processes to avoid conflicting recovery routines. The need to restore a spacecraft from a failure state to a functional operational state demands the execution of routines to isolate faulty components in the system and locate the mismatch node (or point) between the components or parts of the system. A common approach is the construction of the timed failure propagation graph (TFPG), a representation of a system's dynamics describing the occurrence of failures, their local effects, and the consequences over time in other system parts (Bittner *et al.* 2017). The TFPG integrates specific resources from failure mode and effects analysis (FMEA) or fault tree analysis (FTA), enriched with temporal information, assisting in the assessment and implementation of the fault detection, isolation, and recovery functions (FDIR). Bayesian networks and bow-tie models have been widely used as evaluative methods to show the connection between hazard, consequence, and risk-influencing factors. However, a shortcoming of the Bayesian model is that task or authority allocation is not easily visible (Sultana and Haugen 2023). Considering multiple factors and the complex interaction between factors, each barrier's required resources or controls create a complex structure. In these traditional analyses, systems are broken down and examined separately to find the root cause, either in components, or by separating the system's behavior into discrete events, and it is assumed that the parts can be safely separated and analyzed without affecting their functioning, a process that is subjective and vulnerable to bias (Barstow 2023).

Despite the widespread application of analytical methods such as the accident mapping model (AcciMap), system-theoretic accident model and processes (STAMP), causal analysis based on systems theory (CAST), functional resonance analysis model (FRAM), and the more recent accident network method (AcciNet), few formal studies have tested and compared these approaches (Hulme *et al.* 2024). According to Sultana and Haugen (2023), the functional resonance analysis method (FRAM) is employed to gain a deeper understanding and effectively manage variability in complex socio-technical systems, as well as to develop potential accident scenarios. FRAM decomposes the system into functions considering inputs, outputs, time, control, preconditions, and resources, and evaluates how interactions and variability impact performance and risk level. Although FRAM helps improve security by identifying functions and suggesting measures to control unexpected variability, its drawbacks include mathematical complexity and the time required to apply it. The method can also be extended to quantitatively assess the system state and predict actions needed by government agencies to prevent accidents. However, a more sophisticated model is required to identify specific gaps in organizations' actions.

STAMP-CAST aims to explain the actions of control structure elements within their constraints, communication, and process models, identifying missing or violated constraints and recommending changes to prevent future losses (Barstow 2023). The

STAMP and system-theoretic process analysis (STPA) method is effective for hazard assessment by treating safety as a dynamic control problem rather than just failure prevention, identifying and mitigating factors that may contribute to accidents, and requiring risk management due to high interactions in complex systems (Rodrigues *et al.* 2022). STAMP decomposes a system into controllers and their targets, analyzing inputs, outputs, control functions, and human or functional behavior, while STPA identifies unsafe control actions (UCA) and their causes, making it suitable for automated systems with its qualitative control structures (Sultana and Haugen 2023).

The trend of commercializing space activities, where multiple private companies around the world offer their services, demands various ways to reduce rocket launch costs, either by exploring new revolutionary technical opportunities or modernizing existing systems, with some system optimizations not requiring expensive testing and redesigns (Mitikov and Shynkarenko 2022). Beyond disruptive technologies, management, internal culture, budget constraints, and special interest groups, politics have significantly influenced the National Aeronautics and Space Administration's (NASA) decision-making, affecting its achievements and costs (Pessoa Filho 2021). The complexity of managing innovation in aerospace programs requires a proactive approach, with a high level of reflection on managerial practices and the business environment, to encourage cooperation among the various organizations involved in the program to mitigate managerial and technical risks of innovation (Brandão Neto *et al.* 2023). Although program requirements facilitate formal communication within the organization and with stakeholders like government agencies and other space-related companies, they do not explicitly highlight the importance of leadership and commitment to the need to identify, prioritize, and satisfy one's own organizational needs (Reinhardt *et al.* 2024).

To ensure the success of the Starship and promote safe and resilient space exploration, it is essential to continue advancing fault analysis methodologies. The scientific and engineering community should actively collaborate through research and development of new techniques tailored to the challenges of reusable rocket engines, promoting communication and collaboration between engineers and scientists, and investing in advanced infrastructure to improve engine reliability and reuse (Thomas 2024). According to Maslow (1981, p. 49), motivation is the path to satisfying the dominant need. Therefore, formulating a management system structure containing clear statements to define processes, indicators, and goals is an essential tool for motivating actions directed at satisfying organizational needs (Reinhardt *et al.* 2023). This structure generates contextualized consequences directly linked to the results of process management monitored through indicators in pursuit of challenging and necessary goals for achieving the key objectives that sustain the organization (Van Looy and Shafagatova 2016).

However, this analysis can be enhanced through a sociotechnical systemic approach, considering economic, political, social, technological, environmental, and logistical aspects influencing the entire life cycle of space systems (Aguilar 1967). This incorporates not only technical elements but also the business management of space programs (Zahari and Romli 2019). Applying models to prevent failures should consider not only the technology involved in spacecraft development but also the social and organizational systems, goals, and decision criteria used to design, build, and operate these systems (Leveson 2004). Thus, the cause of an accident should be viewed as the result of a complex process involving the entire sociotechnical system, including lawmakers, government agencies, industrial associations, clients, insurers, business administration, technical personnel, engineers, and operators (Rasmussen 1997).

The increasing complexity of space systems and intricate dynamics of the event chain emphasize that accidents are dynamic control challenges. They cannot be addressed through isolated analysis of component failures; instead, they require a comprehensive investigation through systemic analysis of interactions. In this approach, accidents result from UCA failures due to the absence of systemic constraints, driving the system's construction with constraints to prevent these UCA, rather than merely seeking measures to mitigate accident risks (Leveson 2016). In this way, to ensure safety, the system must achieve a required future state where all systemic safety restrictions are implemented. Identifying organizational needs is accomplished by determining the gap between the current and required future states to ensure the organization's safe operation. To satisfy organizational needs, satisfaction objects are identified that meet safety recommendations. This marks a paradigm shift in safety problem resolution, transitioning from basic reliability and redundancy analysis to safety organizational needs management via systems engineering.

The main challenge is to ensure a systemic analysis approach for managing critical processes effectively to ensure system reliability and increase operational value. This method is suggested for application across various sectors, including industry,

commerce, health, and services, to evaluate the potential of systemic analysis in identifying organizational needs and promoting social changes in different business environments and government organizations. These issues require a systemic approach that takes into account organizational needs in the safety analysis of space programs. The application of models such as STAMP and methods like CAST and STPA to generate relevant information helps in creating prospective scenarios, identifying organizational needs related to the program's safety, and formulating recommendations. These methods allow for a more comprehensive and detailed analysis of risks and needs to prevent loss, promoting better management of critical processes and increasing system reliability and safety. Integrating these systems engineering tools into safety analysis enables a more complete understanding of organizational needs and the implementation of effective preventive measures.

The Starship program case study is relevant due to its substantial impact on the space sector. SpaceX's goal is to use Starship for low Earth orbit, sun-synchronous orbit, geostationary transfer orbit, and interplanetary missions for both cargo and crew (FAA 2022). The proposal of a reusable spacecraft with a large payload capacity plays a crucial role in the future of the space economy, contributing to cost reduction, increased launch volume, mass, and frequency (Kulu 2023). SpaceX has emerged as a leader in this new era of space exploration, distinguishing itself with the ability to operate commercially at prices up to 30% lower than other space organizations (Cantu and Lunsford 2022, p. 79-92). The company aims to expand its presence in the satellite market with the introduction of the Starship rocket (Dias 2019). According to the Agence France-Presse (2019), SpaceX envisions launching the Starlink program, aiming to provide internet access through a satellite network. Operating rockets with reusable first stages allows for autonomous landings in designated areas or on ocean barges. Additionally, it transports astronauts and cargo to the International Space Station (ISS), demonstrating its ability to reduce the interval between launches (House 2021).

Starship's reusability introduces significant complexities and risks compared to expendable launch vehicles, as reusable engines endure multiple flights and extreme conditions, necessitating rigorous failure prevention to ensure mission success and a sustainable, cost-effective spacefaring future (Thomas 2024). The Starship program provides extensive audiovisual resources and detailed analysis opportunities despite the limited availability of official materials from SpaceX and government agencies. A comprehensive understanding of the Starship program is essential for grasping the complex phenomena associated with its development and operations. Thus, this study was conducted through an extensive search of publicly available content on the internet about the tests carried out and statements about the management of SpaceX's Starship program. The Starship program's audiovisual resources, including videos, interviews, and documentaries available online, enable a detailed analysis. Despite the limited availability of official material from SpaceX and government agencies like the Federal Aviation Administration (FAA) and NASA, the accessible content is sufficient to identify events, decisions, and actions relevant to Starship program development.

The case study research strategy employed for the Starship prototype utilized multiple information sources, making it suitable for comprehensively understanding the phenomenon under investigation (Yin 2009). The case study of the catastrophic event involving SpaceX's Starship SN10 prototype used publicly available information to build the STAMP model and identify organizational needs. The CAST methodology was then applied to identify possible causes. Finally, the STPA method was used to determine design-related organizational needs and formulate recommendations for the design of the autogenous pressurization system.

Given the complexity of the topic, this study was restricted to demonstrating the application of systems engineering tools and proposing possible solutions to meet organizational needs related to operational safety and the implementation of a new pressurization system in Starship prototypes. The extension of this study, analyzing potential hazard scenarios from its UCA, could provide a more comprehensive view of organizational needs related to other subsystems. It is important to emphasize that it is not the goal of this study to conduct a complete safety analysis of this project.

This article proposes that by identifying organizational needs, understanding the current situation, and performing systemic analyses to develop future scenarios, critical processes can be managed effectively to enhance system reliability and operational value. The results highlight the importance of managers being aware of the actual situation, the significance of proactive measures, clearly defined responsibilities, management commitment, and active involvement of all organization members in the analysis process. Applying systems engineering models and methods is recommended to identify and analyze organizational needs across different areas, processes, and equipment. This study's approach to managing organizational needs within prototype safety

analysis is comprehensive and particularly relevant for managers and researchers less familiar with the critical aspects of systems engineering necessary to avoid failures in complex prototypes. We provide a step-by-step guide on safety analysis methods and suggest opportunities for future studies in innovative strategic management methods.

The next section of this article presents the proposal to integrate organizational needs into the safety analysis approach through systems engineering. Then, the case study of SpaceX's Starship program is examined, detailing the application of the proposed method in STAMP-CAST and STAMP-STPA analyses, the main research findings, the construction of analytical models, and various aspects related to the challenges and benefits observed during the method's implementation. Finally, the results obtained with the proposed method are discussed. The study concludes with a summary of findings, suggestions for future research opportunities, and a description of the theoretical contribution's impact on the field of innovative management methods and safety analysis.

## ORGANIZATIONAL NEEDS IDENTIFICATION FOR SPACECRAFT SAFE OPERATION

According to the STAMP process, accidents result from complex processes operating with feedback control actions. In this context, losses arise not from component failures but from inadequate control of the system's behavior (Leveson 2016). Management can use the STAMP model to identify unsafe interactions and behaviors among components, identifying organizational needs to determine managerial strategies for building safe situations through the application of redundancies, interlocks, and barriers against failures in design, development, manufacturing, maintenance, and operation processes. From this perspective, accidents occur when disturbances are not properly controlled, either due to difficulty in detection or the appropriate response of actuators to avoid adverse consequences. Disturbances can also arise from dysfunctional behaviors resulting from interactions between components, such as in collaborative control systems where various commands act in parallel and can constitute an unsafe set (Kopeikin *et al.* 2024).

Therefore, accidents are not merely isolated events but a consequence of the absence of constraints preventing critical interactions for safety (Johnson and Almeida 2008). Hence, system safety is a control problem, requiring the implementation of constraints to prevent harmful interactions, not limited to the reliability of individual elements or the redundancy of functionalities (Fugivara *et al.* 2021). STAMP excels in generating recommendations at various system levels, describing the needs to avoid harmful future scenarios. In contrast, traditional approaches based on reliability analysis tend to focus on recommendations related to physical-human elements of the system. Considering the distinct characteristics of each method, their combined application has the potential to provide a deeper understanding of the mechanism and contributing factors during accident investigations (Goncalves Filho *et al.* 2019).

The construction of the STAMP control model identifies various elements comprising the system. This involves determining the roles of controllers, control algorithms, control actions, feedback, and controlled processes. Failures in the control algorithm, operator's mental model, and beliefs, which may result from misunderstandings or incomplete information, can trigger four types of UCA, leading to unsafe effects:

- No control command is provided.
- An unsafe action command is provided.
- A control command is provided too early or too late.
- A control command ends too early or too late.

Applying this model in the failure events study can assist in constructing lessons learned to guide projects and prevent the recurrence of similar accidents.

The CAST method is a structured technique designed to analyze accident causality from a systemic perspective, aiming to comprehend causes and develop more effective ways to prevent new accidents (Leveson 2019). The CAST method begins with the accident description, identification of real and potential hazards, and analysis of safety constraints (SC) that failed to prevent the accident. This method allows for reviewing the control structure construction of the STAMP model and gathering information to



identify involved components, constraints, safety requirements, decision contexts, failures in the mental control model, and UCA. This contributes to the formulation of a comprehensive explanation of what happened in the past and caused the loss and facilitates the creation of recommendations to avoid these losses in the future. The method was employed in this study to analyze the loss of the SN10 prototype in the Starship program, constructing the hierarchical control structure considering high-level SC, controlled processes, and their sensors and actuators. In conclusion, some unanswered questions and SC in Starship's operation were raised.

The STPA method was used to identify potential hazards associated with the design of a new autogenous pressurization system for Starship spacecraft, used to pressurize fuel and oxidizer tanks. This enabled the construction of a functional control structure at both high and low levels, identifying critical components. STPA is based on a systemic model that includes losses resulting from design errors, errors in requirement determination, engineering failures, and organizational and managerial deficiencies, going beyond the traditional model of failure event chain (Ishimatsu *et al.* 2014). This method helps identify potential UCA, both high and low-level functional requirements, and possible future causal loss scenarios.

The STPA analysis in early stages recognizes safety as an emergent property of complex systems. Thus, STPA encompasses not only simple failures but also emerging issues resulting from component interactions, software failures, human-machine interfaces, decision-making processes, organizational culture influence, and difficulties in management systems (Fugivara *et al.* 2021). Some of these causes may involve engineering errors, such as inadequate design of protection mechanisms and physical barriers, calculation errors, beliefs, incomplete information, or improper use of knowledge, which can create incorrect assumptions playing a significant role in hazard creation. A failure study in the Chinese space program highlights the predominance of failures caused by errors in spacecraft design and function detailing. This is mainly due to the lack of subsystem redundancy, failures in mitigating electromagnetic interference, component reliability failures, and the use of inappropriate technology (Ji *et al.* 2019). These failures could be avoided by employing systemic methods like STPA to identify organizational needs and adopt recommendations.

Management controls should also be considered, as the operation of the space program is influenced and partially controlled by the social and organizational context, along with various human factors and psychological issues contributing to causal scenarios (Leveson 2015). An advantage of this method is its application in the project conception phase, where limited information is available, generating recommendations to avoid harmful future states and assisting in detailed project design. This facilitates decision-making in project management, reduces development costs, avoids rework, and simplifies the product certification process through an analytical structure that allows clear tracking of all interactions among various elements of the designed system.

Comparison between different analysis techniques highlights how the STAMP model, CAST, and STPA methods differ from traditional approaches. STAMP develops a functional control model instead of a physical element model, analyzing interactions and failures among elements rather than focusing solely on component failures. The CAST method promotes accident analysis to understand the reasons and facts of unsuccessful events in a systemic context, aiming to strengthen control structures to prevent new accidents based on investigative learning (Leveson 2019). On the other hand, the results of the STPA method assist in designing system safety instead of adding safety elements later. This method generates safety requirements and constraints for the system and its components, as well as design changes that can eliminate or mitigate causal scenarios.

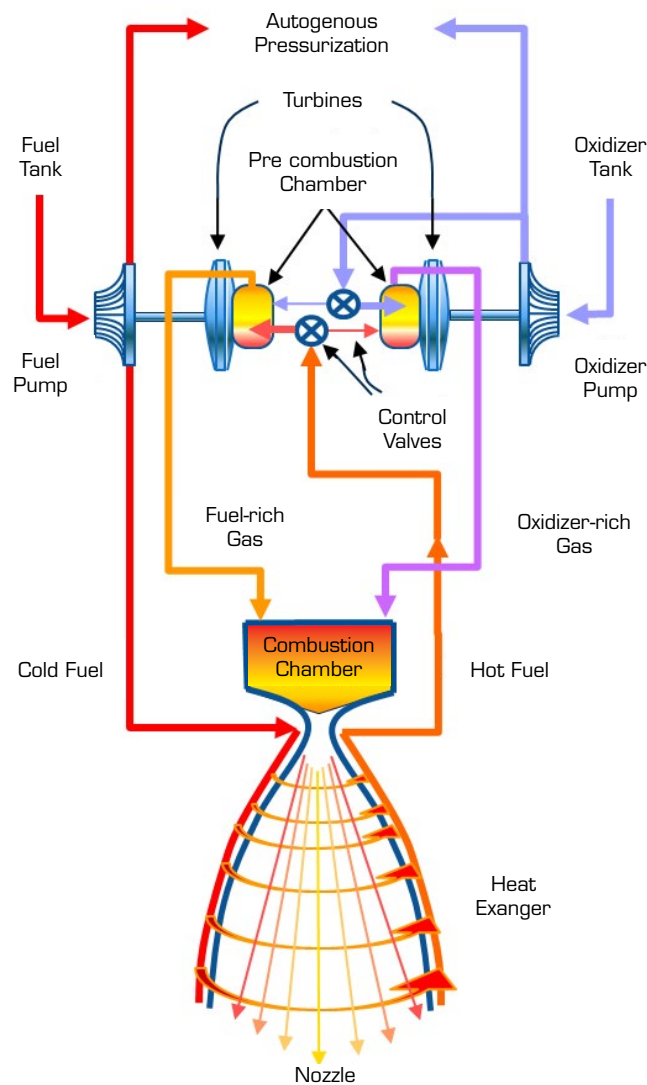
It is still not well understood how the management of organizational needs influences the safety analysis in space programs. There is a lack of formal studies that test and compare the effectiveness of different safety analysis approaches, such as AcciMap, STAMP-CAST, STAMP-STPA, FRAM, and AcciNet, in managing these needs. Furthermore, program requirements do not explicitly emphasize the importance of leadership and commitment in identifying, prioritizing, and satisfying organizational needs. The analysis can be enhanced by incorporating a sociotechnical systemic approach that considers operational and survival aspects of the organization, relationship management, self-development, and organizational leadership in the sector. There is a need for more comprehensive investigations into systemic interactions to better understand how the management of organizational needs impacts the effectiveness of safety analysis approaches in identifying and mitigating risks in space programs. It is also necessary to further explore the identification of gaps between the current state and the required future state for safe operation, as well as the impact of the process of satisfying these needs on accident prevention.

In the next section, the proposed approach is applied to build the STAMP control model for the SN10 prototype and identify high-level organizational needs, applying the CAST method to analyze the causes of the catastrophic event. Following this, the

STPA method was used to identify the organization's design needs related to the autogenous pressurization system for the Starship SN15 prototype, suggest design improvements, determine SC, and provide recommendations for the system's security.

## CASE STUDY OF SPACEX'S STARSHIP PROGRAM

The Starship program aims to reduce space access costs through the development of a reusable rocket after reentry into the atmosphere, using stainless steel structure technology pressurized by fuel tanks. It also stands out for developing a new high-efficiency engine operating in a full-flow staged combustion cycle, known as Raptor (Manley 2021). This engine represents an innovation with significant risks, as no engine with this configuration has been successfully taken into space. There is also no record of the use of an autogenous pressurization system use in space due to the risk of pipe freezing. In this engine configuration, the output gases from the pre-combustion chamber are directed to the combustion chamber after passing through the turbines of pressurization pumps, as illustrated in Fig. 1. The complete cycle increases efficiency, as each pressurization pump works in pre-combustion chambers rich in propellant or oxidizer. Part of the pumped fuel and oxidizer is used by the autogenous pressurization system. In this configuration, all parts are interdependent within the propulsion system.



Source: Elaborated by the authors.

**Figure 1.** Diagram of a full-flow staged combustion liquid rocket engine, featuring two gas generators.

The test conducted with the SN10 prototype aimed to gather telemetry data to validate essential systems for the spacecraft's reentry and landing procedures. The test involved liftoff, reaching an altitude of 12,000 meters, transitioning to a horizontal position, stabilizing the free-fall descent, returning to a vertical position, and executing landing in the designated area. This prototype utilized a helium pressurization system in tanks, as a new autogenous pressurization system was not available. The most critical test stage involved keeping the spacecraft in a horizontal position and restarting engines while avoiding the formation of helium gas bubbles used in pressurizing the fuel in auxiliary tanks, caused by propellant movement. The presence of bubbles in the fuel is cited as one of the causes of engine failures in the tests of prototypes SN8 and SN9. Analysis of various videos related to the SN10 prototype flight allowed for the identification of the following objectives (SpaceX 2021):

- Preparation and ignition of three engines for controlled liftoff.
- Validate attitude control and engine thrust and sequentially shut down the engines at defined altitudes.
- Validate the telemetry system for data and image collection.
- Execute the pitch change maneuver to horizontal position.
- Control free-fall descent through flaps.
- Cool engines and prepare for ignition before restart for landing.
- Validate the algorithm for ignition of three engines, confirm operation, and perform two engines shutdown before landing, keeping one engine on until touchdown.
- Execute the pitch change maneuver to vertical position.
- Perform horizontal translation of the rocket to the landing area.
- Extend and lock the landing legs.
- Execute final approach with thrust control until touching down in the landing area.
- Perform shutdown and open valves for tank venting.

Figure 2 depicts the SN10 preparation for launch and final phases of the flight test, from the landing approach to the catastrophic event at Boca Chica Launch Site in Cameron County, Texas (SpaceX 2021).



Source: Elaborated by the authors based on the video produced by SpaceX (2021).

**Figure 2.** Different phases of the SN10 prototype flight test.

The test stages proceeded as planned on March 3 2021, and despite all flight phases occurring without visible issues, the landing was at a very high speed, followed by the explosion of SN10 a few minutes after landing. The sequence of events for the flight test was as follows (SpaceX 2021):

February 23, 2021 – During the static fire test, a motor failure occurred.

February 24, 2021 – Replacement of the damaged motor.

February 25, 2021 – Successful new static fire test, setting a new record for motor replacement time.

February 28, 2021 – Installation of the flight termination system.

March 1, 2021 – Launch postponed.

March 3, 2021 – Launch preparation at 02:15 h on suborbital pad A.

On the day of launch, March 3, 2021, the following events occurred:

02:15 h – Launch aborted due to an indication of thrust exceeding specifications.



02:39 h – Technical team informs that the maximum thrust limit was set at a conservative value, and the maximum thrust limit is reprogrammed.

05:15 h – Liftoff of the SN10 prototype, marking the launch of prototypes SN8, SN9, and SN10 within last 90 days.

05:15:36 h – Dark smoke emitted from the exhaust gases, indicating incomplete methane combustion.

05:16:35 h – Camera image shows one engine with orange-colored exhaust gases, indicating a richer fuel mixture due to a command to reduce thrust of this engine.

05:17:15 h – Successful shutdown of first engine, with the beginning of yellowish exhaust gases in the third engine, indicating thrust control.

05:18:13 h – Successful shutdown of second engine. Start of transition from fuel flow from the main tanks to secondary tanks, indicated by the freezing of rocket's tip.

05:19:20 h – Start of transition from vertical to horizontal attitude through motor flow vectoring and control of rear flaps. Successful shutdown of the third engine at a 10 km altitude.

05:20:45 h – Reached a 2 km altitude for controlled horizontal free fall, starting the engine cooling phase and pumps pressurization with the gases exhaust from pressure vessels.

05:21:00 h – Restart of the three engines and rear flaps retraction, initiating the pendulum maneuver to reorient attitude to vertical.

05:21:06 h – Shutdown of two engines and start of horizontal translation to landing platform. Exhaust valves of the main tanks operate, controlling the pressure.

05:21:14 h – Activation of the landing gear legs, with failure to lock two legs. Propellant burn escapes in the engine skirt area.

05:21:20 h – Landing of SN10, with a strong impact on ground and onset of a fire at the bottom.

05:23:13 h – Failure to open the upper valves for tank venting maneuver. Only lower valves are opened. Increase in tank pressure due to cryogenic propellant heating.

05:23:18 h – Crushing of the legs causing contact of engine skirt with ground. Freezing of the tanks external surface may be gas leak evidence at the engines.

05:23:37 h – Start of the fire suppression system.

05:23:50 h – Opening of the exhaust valve of secondary oxygen tank.

05:24:08 h – Emission of hot black smoke in right rear flap.

05:27:47 h – End of the lower valves exhaust. Formation of a large area with gases on floor and freezing on the main oxygen tank surface and little freezing on the main methane tank upper area.

05:28:41 h – Shutdown of the fire suppression system.

05:29:32 h – Intense black smoke starts to emerge in the right rear flap area.

05:29:35 h – Tanks rupture and explosion of the lower oxygen tank dome.

Since the explosion occurred after landing, there was no investigation by the FAA.

## Analysis of the high-level control model of the Starship program

The design of the Starship prototype SN10 exemplifies a system characterized by extensive use of control software. Such a system demands an approach capable of identifying potential systemic failures, taking into account context, SC, and feedback from control actions. This goes beyond conventional analysis of failures in individual components (Ishimatsu *et al.* 2014). The STAMP model diagram was employed to build the control model, as depicted in Fig. 3.

In the high-level control structure analysis, the following control actions (CA) and feedback actions (FE) are identified:

CA1 – Authorization, cancellation, or postponement of launch.

FE1 – Information on current project status and its risks for launch.

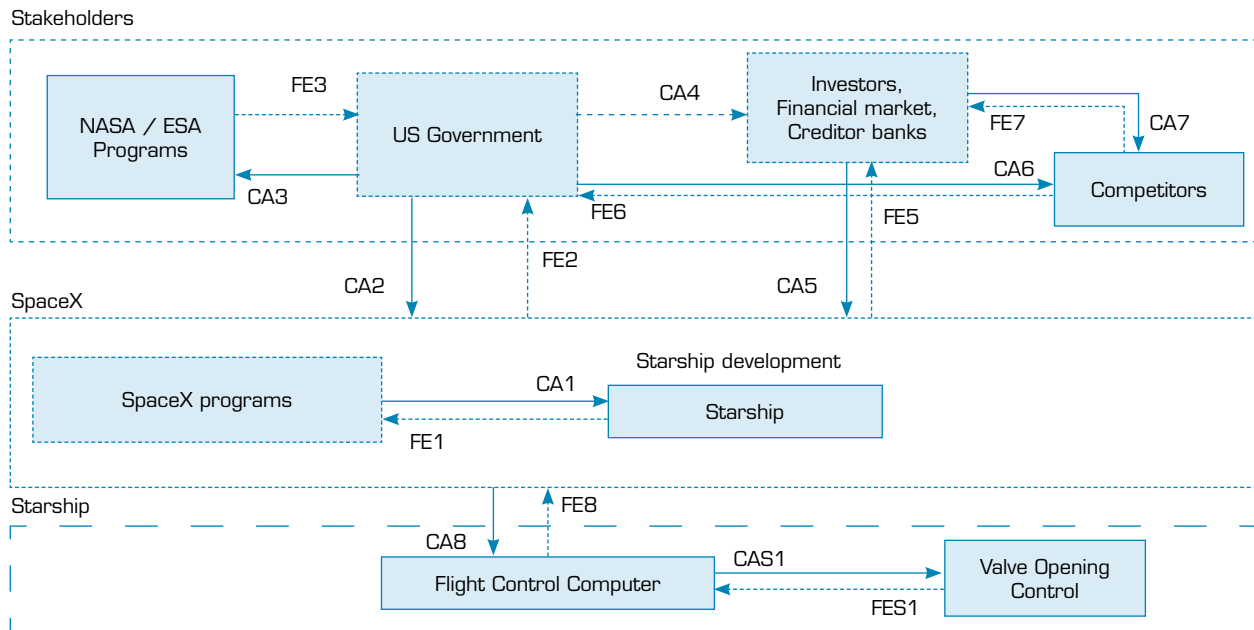
CA2 – Authorization of launch, monitoring, and evaluation of results.

FE2 – Information on launch decision and associated risks.

CA3 – Comparison of results and analysis of alternative options.

FE3 – Information on investment decisions in programs.





Source: Elaborated by the authors.

**Figure 3.** The high-level control structure of the Starship program.

CA4 – Information on government investment decisions.

CA5 – Provision of financial resources to SpaceX.

FE5 – Information on the application of investments in the Starship program.

CA6 – Authorization of launch, monitoring, and evaluation of results.

FE6 – Information on launch decision and associated risks.

CA7 – Provision of financial resources.

FE7 – Information on application of investments in competing programs.

CA8 – Start of the control algorithm for systems of the SN10 spacecraft.

FE8 – Telemetry information for the SN10 spacecraft systems.

CAS1 – Activation of actuators for the SN10 spacecraft systems.

FES1 – Information from sensors for the SN10 spacecraft systems.

Through the STAMP model, and the sequence of events for the flight test (SpaceX 2021), it is inferred that the following decisions were made, leading to UCA:

- The use of a helium pressurization system in secondary propellant and oxygen tanks without the implementation of a validated device to prevent the entry of helium bubbles into engines.
- Utilization of the flight control algorithm incapable of detecting an engine failure in time to activate a substitute engine.
- Acceptance of the risks associated with launching with an engine thrust exceeding specifications.

These decisions can be attributed to a highly competitive context to assure investments from the U.S. federal government and private investors interested in meeting schedules. In this way, it is possible to identify some prospective scenarios (Creech *et al.* 2022):

- SpaceX should demonstrate its technological capacity to comply with the NASA contracts for the Artemis program with the highest possible safety standard and the highest level of risk mitigation.
- SpaceX should develop the Human Landing System Starship, SpaceX Uncrewed Lunar Demo, SpaceX Uncrewed Lunar Demo-A – Artemis III, and SpaceX Uncrewed Lunar-Artemis IV within the contracted schedule to ensure U.S. government payments.
- SpaceX should ensure its position as the first provider of the Gateway Logistics Services contract.

Organizational needs are the gaps between the present state and the necessary future state that the organization must build (Reinhardt *et al.* 2024). Thus, through context analysis we can identify the current situation and the necessary future state that the Starship program should achieve, identifying the following organizational needs:

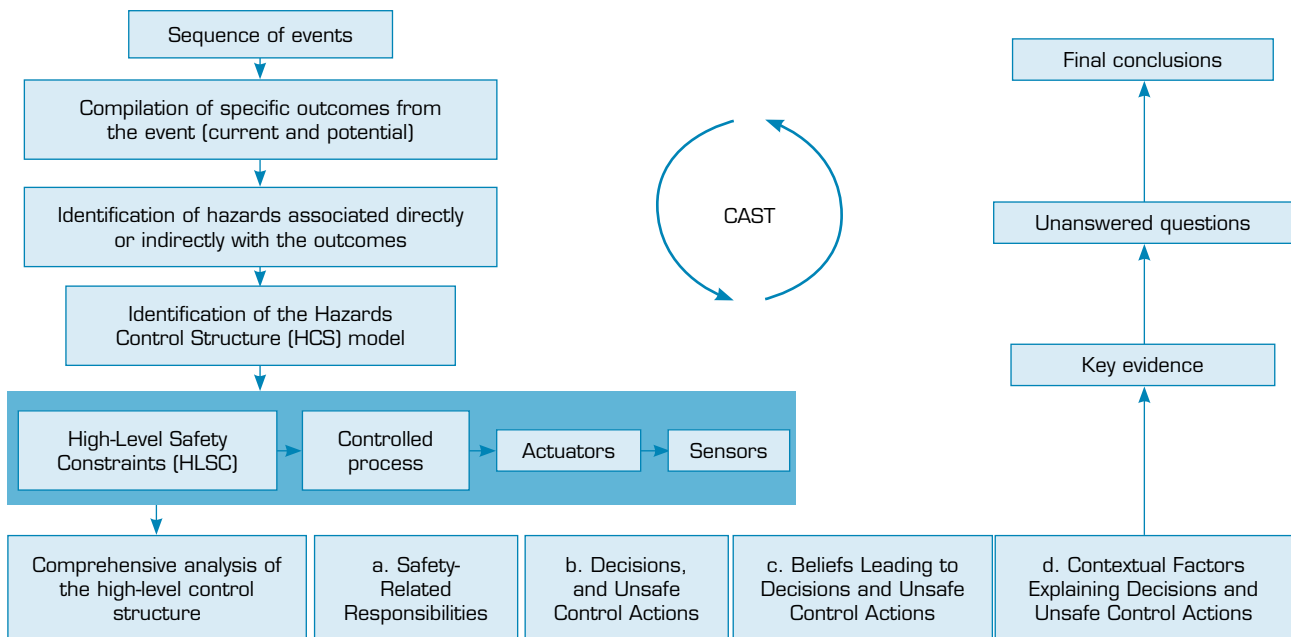
- SpaceX needs to develop Starship's safe operation.
- SpaceX needs to ensure the contract execution schedule.
- SpaceX needs to demonstrate the development of the ability to provide space logistics services.

The STAMP model analysis identified the following recommendations:

- The decision-making process leading to identified UCA should be critically analyzed in terms of organizational context, independence, and autonomy.
- The implementation of possible SC should be prioritized to avoid program schedule delays and prevent further accidents.

### CAST analysis of the SN10 prototype accident

The CAST method facilitates accident analysis to identify causes leading to losses that stakeholders aim to prevent in the future, following the phases outlined in Fig. 4.



Source: Elaborated by the authors.

**Figure 4.** Phases of the CAST.

With the analysis of videos available on the internet, current results (R), which actually occurred, and potential results (Rp), which could have occurred, were identified (Manley 2021):

#### *Current results (What actually happened?)*

- R1 – Destruction of the SN10 prototype.
- R2 – Destruction of project evidences and development outcomes.
- R3 – Cleanup and wreckage recovery costs.
- R4 – Decline in SpaceX stock value and private investments.
- R5 – Loss or delay of government contracts.

#### *Potential results (What could have happened?)*

- Rp1 – Destruction of fueling tanks infrastructure and launch structures.

Rp2 – Damage to private properties.

Rp3 – Delay in the Starship program due to technical issues or FAA investigation.

Rp4 – Delay in the Starlink program, with loss of investments and revenue.

Rp5 – Socioeconomic losses, damage to housing environment and loss of human lives.

Rp6 – Environmental degradation by cumulative effects on protected species habitat.

Rp7 – Damage to neighboring natural gas liquefaction facilities.

Rp8 – Restriction of public access in areas such as local roads and Boca Chica beach.

Rp9 – Impact on airspace.

Rp10 – Environmental impact caused by hazardous materials, solid waste and liquid or gas pollution.

The results analysis identifies the following hazards (H) and sub-hazards directly associated with hazardous behaviors in the event:

H01 – Engine thrust reduction.

H02 – Engine exceeding the maximum thrust limits.

H02a – Damage to internal engine components.

H03 – Landing gear operation without proper locking.

H03a – Structural damage.

H04 – Structural damage due to efforts during attitude change.

H04a – Leakage of propellant and oxidizer.

Associated hazards and indirectly associated sub-hazardous behaviors that directly affect the Starship program's operation can also be identified:

H01X – Delay in the Starship program.

H01Xa – Delay in the Starlink program.

H01Xb – Government contract cancellation (Artemis).

H01Xc – SpaceX revenue reduction.

H02X – Trajectory deviation due to wind gusts.

H03X – Lightning strikes.

H03Xa – Destruction of Starship telemetry and control system.

H04X – Sabotage and damage caused by third parties.

For each directly related hazard, an SC has been assigned to prevent or mitigate the hazard. The following high-level SC were identified:

SC01 – Decision control for the use of a specific pressurization system in the secondary tanks.

SC01b – Avoidance of inert gas and bubbles ingestion in the engine feed lines.

SC02 – Decision control for the alteration of engine operating parameters.

SC02a – Control of engine parameters to prevent damage to internal components.

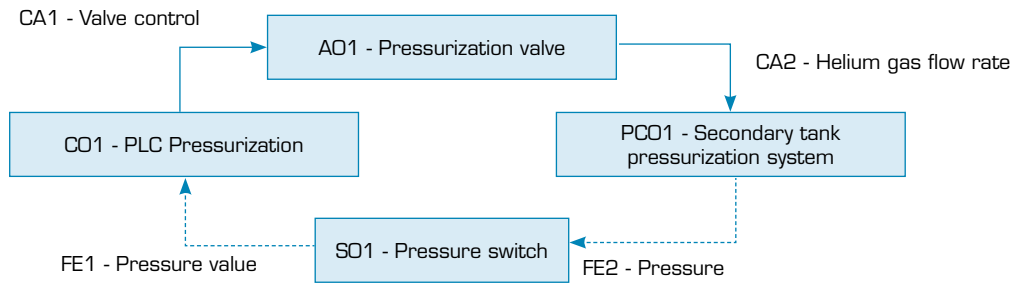
SC03 – Landing gear locking control.

SC03a – Landing gear damping control.

SC04 – Control of structural efforts during translation.

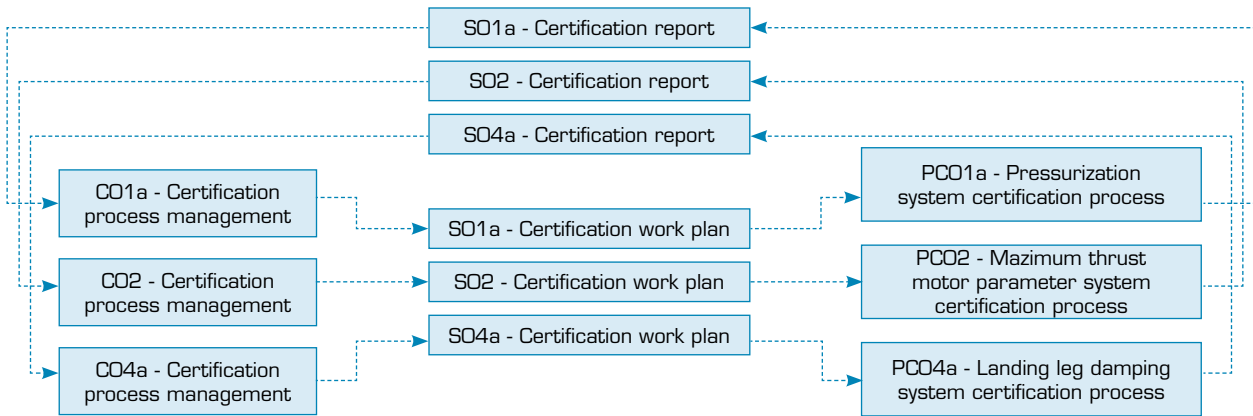
SC4a – Control of tank pressure drop rate.

Through the control loop analysis, we can verify that the predominant hazards were the engine thrust reduction during the final landing phase, probably caused by helium and gas ingestion into the propellant or oxygen pressurization system, and the internal engine components' failure due to thrust overload caused by the decision to change operating parameters after detecting overload in the first takeoff attempt. For each of these systems, hazard control structure (HCS) loops were constructed. Figure 5 presents the HCS model of the secondary tank pressurization system, while Fig. 6 describes the certification and flight envelope establishment system.



Source: Elaborated by the authors.

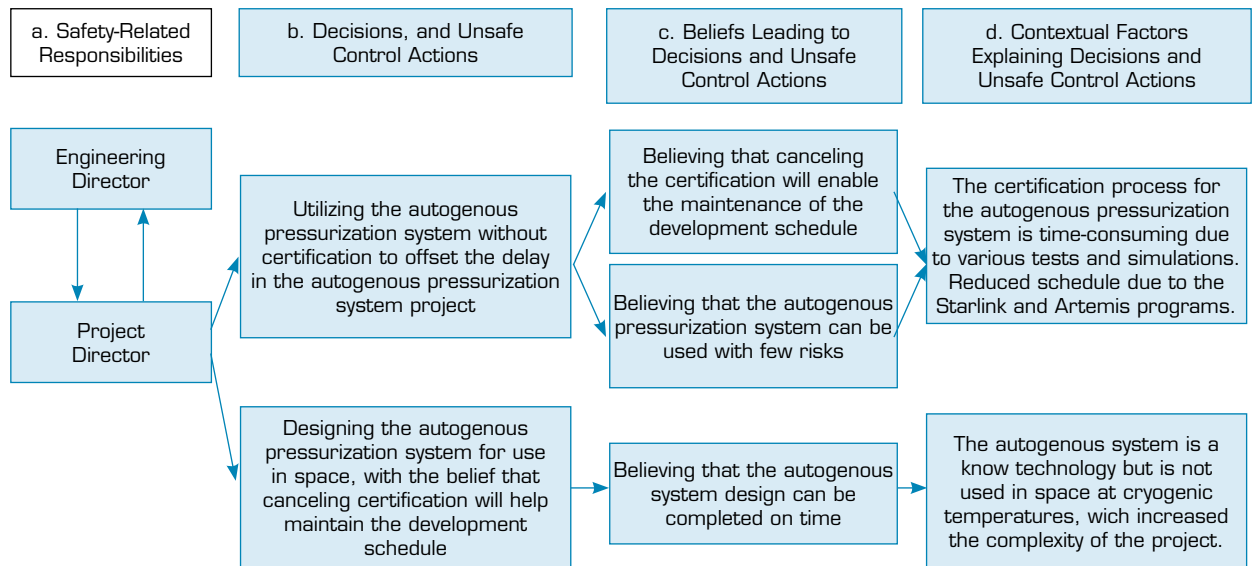
**Figure 5.** Secondary tanks pressurization system (PC01).



Source: Elaborated by the authors.

**Figure 6.** Certification system and flight envelope establishment.

Through the analysis of the high-level control structure, it was possible to identify certain responsible elements that made decisions regarding the pressurization system, leading to unsafe actions influenced by contextual factors, as described in Fig. 7.



Source: Elaborated by the authors.

**Figure 7.** Analysis of the high-level functional control structure of the SpaceX Starship autonomous pressurization system project.



After the accident, SpaceX made several statements regarding the operation and potential engine failure causes in the final moments of landing (Ricken 2021a):

March 05, 2021 – SpaceX reports that the accident cause was a thrust failure in the active engine, which was below the required value in the final moments of approach. Despite the command to increase thrust, it did not happen. The reasons for this are still unknown. The next test plans to keep two engines active during the approach and restart the third engine if either of the two engines shows inconsistent readings.

March 06, 2021 – SpaceX states that, as the landing speed of 10 m/s exceeded the landing leg absorption capacity, fixing the landing leg locking failure would not have prevented the accident.

March 09, 2021 – SpaceX suggests that the likely cause of thrust loss was the ingestion of pressurization gas helium from the secondary methane tank. Helium was introduced as a temporary solution after a pressurization failure in SN8.

According to SpaceX statements, a definitive solution proposed is the implementation of an autogenous pressurization system, which is still in the development phase. Another potential hypothesis is the ingestion of helium gas, used for tank pressurization, by the engines due to the movement of liquid methane within the secondary tank, leading to engine failure in a manner similar to a known issue in the early Falcon 1 prototypes (Ricken 2021a). The impact with the ground occurred at a speed of 24 km/h, resulting in damage to the main tank's lower structure in the engine skirt area, along with a fire due to propellant and oxygen leakage, followed by an explosion. Figure 8 illustrates the initial events of the explosion in the main oxygen tank's lower region, as viewed from the back of the Starship, with significant black smoke emission at 05:29:35 h (Manley 2021).



Source: Elaborated by the authors based on the video produced by Manley (2021).

**Figure 8.** Onset of the explosion in the main oxygen tank's lower region.

SpaceX statements indicate the need to demonstrate the capability of reducing the turnaround time between missions by improving booster inspection and reusability. Modifications were already planned for SN15, making SN10 a prototype solely intended for data collection to update control algorithms. This diminished the importance of the landing phase for SN10, as subsystem revalidation was required on SN15, including a new set of propellant ducts and a propulsion disc in the Raptor engine area. Consequently, SN10 flew with obsolete engines from two different versions. Operating the engine with higher thrust than specified might have led to a structural failure in the lower dome of the propellant tank, resulting in leaks in the engine skirt during flight and a potential failure in the secondary propellant tank pressurization.

The decision to use a helium pressurization system was a temporary corrective measure to address the pressure drop issue in the secondary tanks observed in SN8 and SN9 flights. This choice was motivated by flight schedule delays and the

need to gather telemetry data for upcoming prototypes with significant modifications already implemented. The autogenous pressurization system was not yet available for use on SN10. The program schedule delay could directly impact the Starlink system, projects funded by the U.S. federal government like the Artemis program, and the provision of material transport services for the U.S. military, directly affecting SpaceX's revenue. As a result of the CAST method analysis, some unanswered questions were raised:

- Why was a pressurization system used without a device preventing bubble formation and helium ingestion by engines, given that this issue was already known in SpaceX's Falcon 1 project?
- Why were not all engines ignited, with the subsequent shutdown of engines not in use, to prevent failure in the engine used during the landing phase?
- Why were thrust, vibration, and aerodynamic load tests not conducted on all prototypes to ensure the structural integrity of the tanks and the lower dome where the engines are installed?

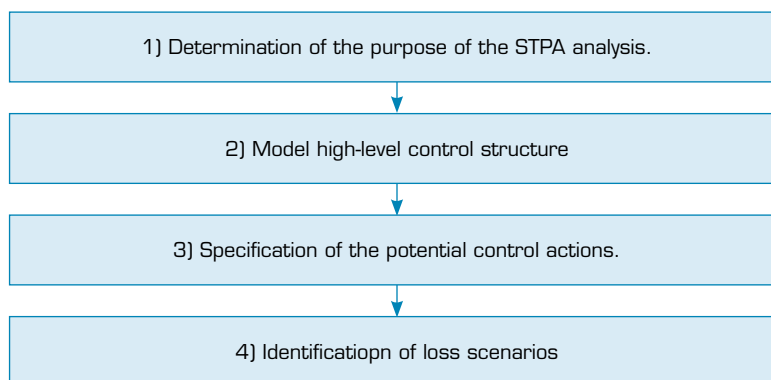
The CAST analysis of the accident emphasizes the organizational need to evaluate the criteria that led to the decision to employ a temporary pressurization system in auxiliary tanks without the implementation of motion restrictors or mechanisms to prevent helium bubble ingestion by engines. Additionally, a review of the engine assembly control algorithm is suggested to reduce unit failure risks. Another point is the development of a pressurization system for auxiliary tanks that prevents helium ingestion by engines. The autogenous pressurization system is suggested as a well-known option used in various liquid-propellant rocket projects. The criticality of analyzing the propulsion disc structure in the propellant tank's lower dome, where the engines are installed, considering aerodynamic forces during spacecraft translation, is also highlighted.

The propellant and oxygen tank pressurization system is identified as the most critical in the SN10 prototype, as other issues become relevant only if this system operates flawlessly. To date, rocket engines have not been used for the vertical landing of an orbital spacecraft on Earth with the aim of reuse. Typically, vertical landings of rocket engines are performed only in the initial stages, without exposing the engines to the cryogenic temperatures of space or the need for atmospheric re-entry.

### STPA analysis of the autogenous pressurization system design

The Starship program aims to innovate by introducing an autogenous pressurization system into the space environment, powered by a full-flow staged combustion rocket engine, enabling re-entry and a reusable spacecraft landing. This innovation promises a highly efficient spacecraft, with the lowest cost per kilogram for space access and the ability for rapid reuse.

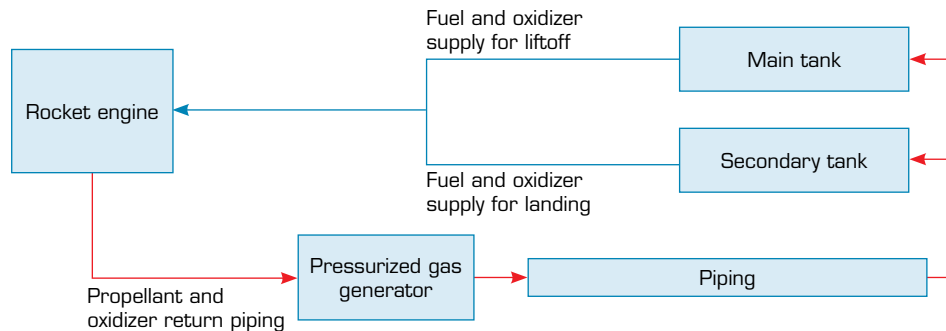
The STPA method was employed to analyze the design of an autogenous pressurization system for fuel and propellant tanks, as described in Fig. 9. This approach aims to identify safety organizational needs to ensure the system's operation under atmospheric conditions, in space, and during re-entry and landing maneuvers, and to determine the technical requirements to build objects that satisfy the identified needs.



Source: Elaborated by the authors.

**Figure 9.** Phases of the STPA analysis.

The STPA leads to the conclusion that the autogenous pressurization system with a full-flow staged combustion liquid propellant engine with two gas generators, as depicted in Fig. 10, is the configuration with the highest number of coupled elements.



Source: Elaborated by the authors.

**Figure 10.** Autogenous pressurization system diagram.

This structure poses a higher level of risk, as the failure or malfunction of one component impacts the entire system. The Raptor engines employ a full-flow staged combustion cycle with two rich pre-combustion gas chambers for both propellant and oxidizer. In this cycle, exhaust gases from the pre-combustion chambers are directed to the combustion chamber after passing through the turbopumps. A portion of these pressurized gases from the turbines is directed to the autogenous pressurization system. This approach reduces the risk of explosions due to leaks in the turbine shaft and allows for more efficient propellant usage, albeit making the system more complex. The autogenous pressurization system has the following main objectives:

- Maintain the structural integrity of the spacecraft by pressurizing tanks.
- Sustain the propellant and oxygen flow to engines by maintaining nominal pressure after liftoff.
- Increase the efficiency of the propellant and oxidizer pumping system by reducing cavitation in pressurization pumps through an initial pressure boost in tanks.
- Avoid the use of inert pressurization gas and potential propellant and oxidizer contamination.
- Increase pressure due to gas expansion after cooling in the combustion chambers and propellant and oxidizer heating upon return to tanks.

### *Hazards (H) and associated hazards (Ha)*

The H and Ha of the Starship autogenous pressurization system architecture that need to be addressed were identified as follows:

H1 – Overpressure pipe.

H2 – Pipe freezing.

Ha2 – Low pressure on tanks.

H3 – Insufficient tanks pressure.

Ha3 – Insufficient thrust

Hb3 – Significant engine vibration.

H4 – Operation with tanks overpressure.

H5 – Propellant and oxidizer leakage.

Ha5 – Fire in the propeller and oxidizing leakage area.

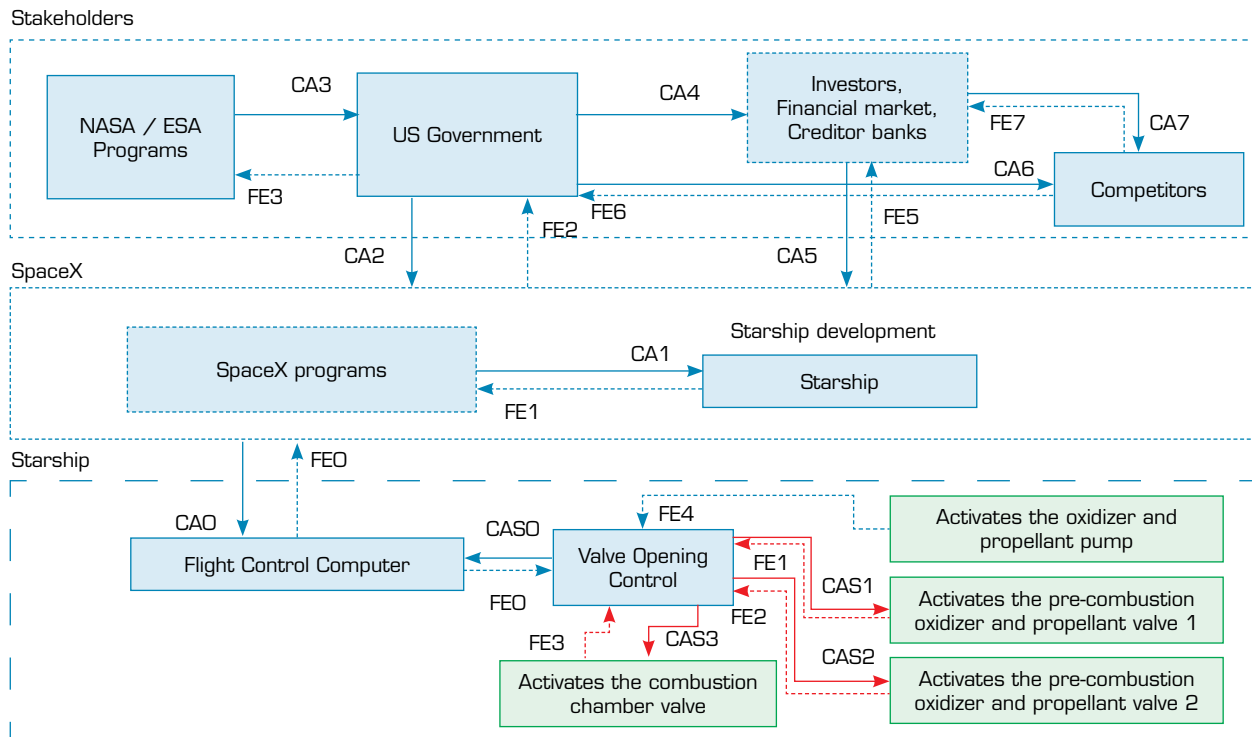
H6 – Delay in the Starship program.

Ha6 – Loss of revenue.

### *High-level functional control structure model*

After identifying the associated hazards and potential dangers, the high-level functional control structure model of the system was developed, as depicted in Fig. 11. This model takes into account the stakeholders influencing the development of the Starship autogenous pressurization project.





Source: Elaborated by the authors.

**Figure 11.** High-level functional control structure model of an autogenous pressurization system.

In the analysis of the high-level functional control structure involving an autogenous pressurization system, in addition to the previously described control actions and feedback, the following control actions and feedback are identified:

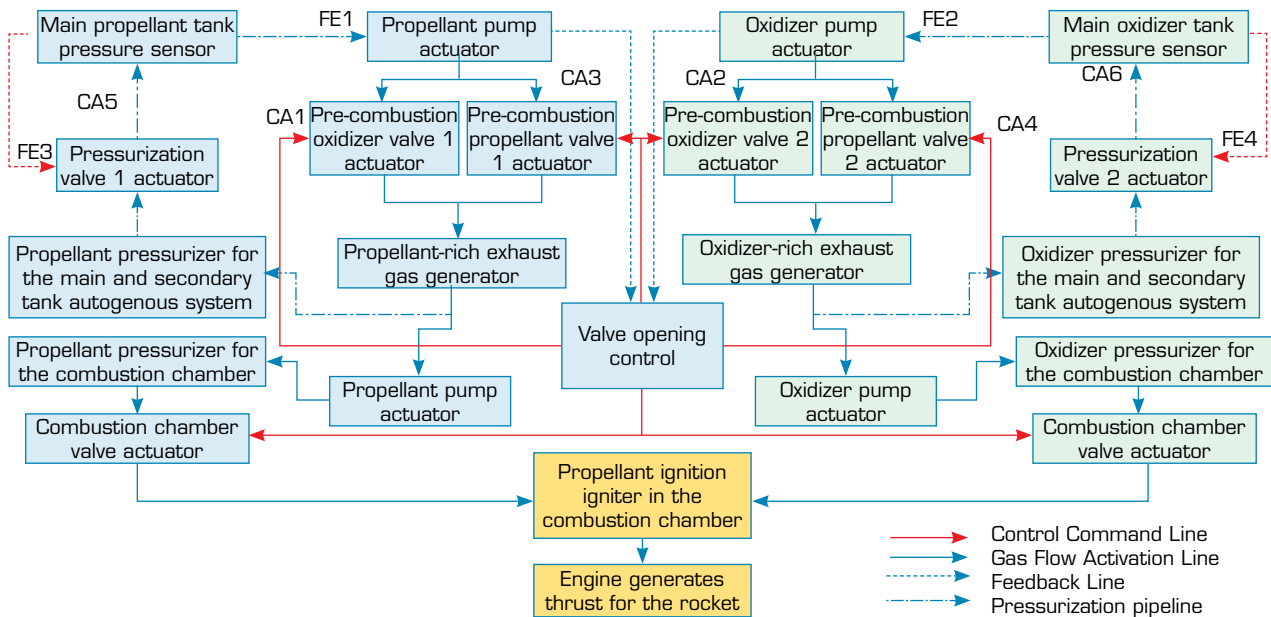
- CA8 – Start of the spacecraft systems control algorithm.
- FE8 – Telemetry information from spacecraft systems.
- CAS1 – Activation of spacecraft system actuators.
- FES1 – Sensor information from spacecraft systems.
- CAS2 – Activation of pre-combustion 1 propellant and oxidizer valves.
- FES2 – Sensor information from valve position sensors.
- CAS3 – Activation of pre-combustion 2 propellant and oxidizer valves.
- FES3 – Sensor information from valve position sensors.
- CAS4 – Activation of combustion chamber propellant and oxidizer valve.
- FES4 – Sensor information from valve position sensors.
- FES5 – Sensor information from propellant and oxidizer pump pressure sensors.

### *Low-level functional control structure model*

The low-level functional control structure model, as depicted in Fig. 12, takes into account the actuators and sensors that impact the operation of the autogenous pressurization system.

The analysis of the low-level functional control structure model of an autogenous pressurization system identifies some control actions and feedback in the system's operation:

- FE1 – Main propellant tank pressure.
- FE2 – Main oxidizer tank pressure.
- CA1 – Activates the pre-combustion 1 oxidizer valve.
- CA2 – Activates the pre-combustion 2 oxidizer valve.



Source: Elaborated by the authors.

**Figure 12.** Low-level functional control structure model of the Starship's autogenous pressurization system.

CA3 – Activates the pre-combustion 1 propellant valve.

CA4 – Activates the pre-combustion 2 propellant valve.

FE3 – Main propellant tank pressure.

FE4 – Main oxidizer tank pressure.

CA5 – Activates propellant pressurization tank 1 valve.

CA6 – Activates oxidizer pressurization tank 2 valve.

In this study, unsafe low-level control actions (UCAL) and unsafe high-level control actions (UCAH) were identified, which were studied to identify causal and loss scenarios (Sc). The relationship between low and high-level UCA lies in their potential to interact and influence each other. UCAL and UCAH refer to different types of control actions within a system that can potentially lead to adverse outcomes or safety hazards. UCAL usually involves a direct drive of components or parameter adjustments and system mechanism settings. However, high-level control actions involve broader strategic decisions that affect the general behavior of the system. These actions often involve setting policies, procedures, or making operational decisions. While UCAH may not directly involve operation of system components, they can still have significant implications for safety if they are not carefully considered or implemented.

The identified UCAL are as follows:

UCAL1 – Incorrect opening of propellant and oxidizer valves.

UCAL2 – Premature activation of propellant and oxidizer valves.

UCAL3 – Delayed activation of propellant and oxidizer valves.

UCAL4 – Prolonged activation of propellant and oxidizer valves.

UCAL5 – Short-term activation of propellant and oxidizer valves.

UCAL6 – Non-activation of propellant and oxidizer valves.

UCAL7 – Non-ignition of pre-combustion chambers 1 and 2.

UCAL8 – Non-ignition of the combustion chamber.

UCAL9 – Valve control with incorrect feedback information.

UCAL10 – Inadequate heating of the autogenous pressurization system piping.

The identified UCAH are as follows:

UCAH1 – Inadequate control over Starship development, compromising the certification process and ensuring safe Starship operation due to the organizational commercial context, economic pressures, and contract deadlines.

UCAH2 – Deploying the Starship flight control computer algorithm without completed certification may jeopardize engine and autogenous pressurization system operation during ignition and shutdown phases due to fuel flow and heat transients.

UCAH3 – Inadequate control over Starship valve openings may compromise engine and autogenous pressurization system operation during deceleration and landing phases due to fuel flow and heat transients.

The process of constructing Sc due to UCA and safety requirements allowed the identification of the following scenarios:

- ScUCAH1-3 and ScUCAL1-10 – Activation of pre-combustion chamber mixing valves resulted in complete burning, with pump melting during startup.
- ScUCAH1-3 and ScUCAL1-10 – Activation of pre-combustion chamber mixing valves caused combustion failure, with oscillation and pump breakage during startup.
- ScUCAH1-2 and ScUCAL1-9 – Late control command opening of valves due to delayed sensor signal processing, causing overpressure and pump breakage.
- ScUCAH1-2 and ScUCAL1-9 – Early control command opening of valves due to delayed sensor signal processing, causing overload and pump breakage.
- ScUCAH1-3 and ScUCAL1-9 – Oscillating control command opening of valves due to delayed sensor signal processing, causing stress leading to pump breakage.
- ScUCAH2-3 – SpaceX experienced a revenue reduction due to delays in the construction of the Starlink system caused by the integration of an autogenous pressurization system into Starship.
- ScUCAH2-3 – SpaceX experienced a revenue reduction due to delays in U.S. government projects, such as Artemis, caused by the integration of an autogenous pressurization system into Starship.
- ScUCAH3 – Engine thrust loss due to pressure loss for autogenous pressurization system feed during low-power engine landing operation.
- ScUCAH1-2 and ScUCAL10 – Insufficient pressurization of main and secondary tanks due to autogenous pressurization system piping freezing during space operation.
- ScUCAH1-2 and ScUCAL10 – Insufficient combustion chamber pressurization due to pressure loss for autogenous pressurization system feed, causing vibration and thrust loss.
- ScUCAH1-2 and ScUCAL10 – Structural collapse due to insufficient pressurization in main tanks.
- ScACIAH1-3 and ScACII-10 – Activation of pre-combustion chamber mixing valves resulting in complete combustion, leading to pump melting and subsequent pump failure due to low-speed actuation system.
- ScACIAH1-3 and ScACII-10 – Activation of pre-combustion chamber mixing valves resulting in complete combustion, leading to pump melting and subsequent pump failure due to loss of hydraulic system pressure.
- ScACIAH1 – Difficulty in obtaining FAA release authorization due to certification process not clearly demonstrating safety operation of Starship.
- ScACIAH1 – Delays in demonstrating safety operation of Starship may compromise service contracts to stakeholders.

With the construction of Sc due to UCA and safety requirements, it is possible to identify organizational needs and infer the following recommendations:

- The autogenous pressurization system, coupled with a full-flow staged combustion engine featuring two gas generators, represents a novel system in which multiple elements interact closely. The failure of any single element impacts the entire system, rendering it the architecture with the highest risk.
  - Organizational need – Mitigate failures by mandating the use of components subject to quality control in design and production processes.
  - Satisfaction object – System components that operate without failure within the operational envelope.
  - Recommendation – System components should be certified for operation at the various flight phases.



- The control of this system's operation can lead to an oscillatory state with little damping due to coupling of various elements involved in operation.
  - Organizational need – Mitigate oscillation during engine operation.
  - Satisfaction object – The valve control system must incorporate an algorithm capable of mitigating rocket engine thrust oscillation caused by feedback from the autogenous pressurization system pumps.
  - Recommendation – The valve control system should be certified to prevent this oscillatory state during operation at the various flight phases.
- The Starship project's development method, with the execution of interactive changes without complete equipment certification, has a high risk of new accidents, but it provides more precise information collection during flight tests.
  - Organizational need – Collect system operating information during the safe execution of a flight test.
  - Satisfaction object – System operational data collected in safety.
  - Recommendation – Critical components should be tested to mitigate the risk of flight test failure.

Critical high-level functional requirements (RUCAH) of the Starship autogenous pressurization system are identified.

RUCAH0&1 – The autogenous pressurization system should be certified according to operation requirements within the atmosphere and in space.

RUCAH2 – The pressurization system should have a secondary system to prevent pressure drop in main tanks and engine combustion chambers during various operation phases.

The analysis of UCALs, despite the importance of studying requirements and recommendations for each component's development, will not be addressed due to the extent of this work.

The Starship system's development and design method, with the execution of interactive changes without complete equipment certification, pose a new accident risk but provide precise information collection through flight tests and the rapid implementation of corrective actions. Despite being costly, this process demonstrates a reduction in development time. Through the analysis of the STPA method results, the following recommendations for the Starship program management are proposed:

- SpaceX's strategy for large-scale production development of this spacecraft type should align with an increase in the number of prototypes needed for flight tests without subsystem certification, simplifying the certification process.
- SpaceX management should promote the use of prospective scenarios for systems analysis and the identification of organizational needs, encompassing both the effects and systemic relationships produced by unsafe high and low-level control actions.

SpaceX management should balance the satisfaction of operational organizational needs with the need to maintain the economic survival of the SpaceX program.

## DISCUSSION OF RESULTS

In the Starship SN10 prototype case study, several critical issues and failures were identified related to the use of the helium pressurization system, the flight control algorithm, and engine thrust overload. The use of the helium pressurization system without a validated device to prevent helium bubbles from entering the engines and the flight control algorithm's inability to detect engine failures in time to activate a substitute were decisions that led to UCA. The analysis revealed that these failures were linked to the competitive context and how SpaceX's innovations are influenced by its relationships with governmental bodies, particularly regarding regulatory approvals and strategic timelines (Weinzierl *et al.* 2021). In terms of long-term relevance, the study highlights the importance of developing a safer autogenous pressurization system and improving decision-making to avoid UCA. The analysis suggests that implementing safety measures and critically reviewing decisions and control algorithms are crucial for preventing future accidents.

Systemic analysis must consider the failure scenario as well as contributions to the occurrence of unsafe actions. We can identify the following aspects that have affected SpaceX's management:

- Innovation in the method of building and testing space rockets (Vittori *et al.* 2024).
- Potential use of Starship for launching 12,000 satellites is planned to be deployed, with a possible later extension to an additional 30,000 communication satellites to build the Starlink global internet network (Shaengchart and Kraiwanit 2024).
- SpaceX is expected to generate approximately \$ 9 billion in revenue in 2023, combining its rocket launch and Starlink operations, with sales projected to increase to around \$ 15 billion in 2024 (Roy 2023).
- The NASA Commercial Lunar Payload Services (CLPS) program is set to initiate the delivery of scientific payloads to the Moon starting in 2024, facilitated through indefinite delivery, indefinite quantity contracts with a cumulative maximum value of \$ 2.6 billion through 2028 (Yost and Weston 2024).
- Pressure from various new private companies competing in the NewSpace market has led to the inclusion of a variety of high-energy launch vehicles from multiple vendors in the current NASA Launch Services Contract (NLS-II) (McNutt *et al.* 2024).

Although only one Starship service for lunar travel is currently contracted, there are projections to increase participation in space cargo transportation. This includes contracts with the U.S. Air Force for launches until 2023, valued at 260 million dollars, and exploration of the global provision of high-speed internet services through the Starlink program, generating 1.4 billion dollars in revenue in 2022 (Rubinstein 2023). A detailed analysis of the daily operating, development, and launch costs of the Starship program rockets, compared to the total cost of engines and prototypes at the Starbase, reveals that prototypes have a relatively small cost compared to the company's fixed costs (Wang 2019).

Considering the organizational needs in the economic context, the decision to launch the SN10 prototype, despite signs of accident risk in a controlled safety area, was justified. This decision aligns with the program's need to validate various subsystems, as it would be economically unfeasible to conduct repairs or new tests on engines or pressurization systems. Launch interruptions would delay Starship program activities, impacting investments and revenue opportunities with the Artemis and Starlink programs. The process of detecting and analyzing failures, along with subsequent modifications aimed at optimizing safe operations based on lessons learned, should proceed iteratively and sequentially to foster and bolster innovation within this space program (Vittori *et al.* 2024).

Financial losses and the potential loss of scientific advancements can be mitigated with systemic and safety assurance analyses. Organizational learning is crucial and requires a sophisticated analysis that includes organizational, social, and cultural factors to promote a constant process of change, not relying solely on previous experiences and specific scenarios (Marais *et al.* 2004). However, despite the proposed method being comprehensive, the depth of the analysis is contingent upon the team's experience and the available time for completion. The analysis process should be optimized with digital tools to reduce the time required for hazard and loss analysis and to assist in developing prospective scenarios for the program.

Adding the analysis of organizational needs to improve program safety, beyond technical aspects, provides a better understanding of the hazards and losses to be avoided. This approach goes beyond simple technical analysis by considering the socio-economic aspects of managerial decisions.

## CONCLUSION

This case study showed that organizational needs for system safety should be managed by recognizing the organization's current situation and constructing prospective scenarios through systemic analysis to prevent failures. The construction of the STAMP model, along with the application of the CAST and STPA methods, enabled the identification of program needs and recommendations for designing the safety requirements of an autogenous pressurization system to be used in the Starship SN15 prototype of the Starship program.

The STAMP model facilitated the identification of key stakeholders and UCA. Aspects of the organizational context influencing program management were identified, along with recommendations for evaluating the management process leading to identified unsafe actions and potential SC to be implemented promptly to prevent future accidents.

CAST effectively identified causes of the catastrophic event in SN10, highlighting UCA and providing a critical analysis of the structural integrity of the propulsion disk in the lower dome of the propellant tank, where the engines are installed.



Unanswered questions were raised, guiding potential changes in program management. The analysis confirmed that the pressurization system for propellant and oxygen tanks is the most critical system, with operational constraints in the space environment at cryogenic temperatures.

Subsequently, STPA was applied to determine key actions in the development of an autogenous pressurization system for Starship's propellant and oxygen tanks. In discussing the results within the current context of commercial opportunities in the space sector, it becomes evident that SpaceX's management focuses on promoting the sustainability of its operation, making rapid modifications to address issues encountered in technological innovation development. All recommendations from CAST and STPA analyses were later identified in web-available videos, showcasing practical changes made by SpaceX in the Starship SN15 prototype (Ricken 2021b). The SN15 flight and landing were successful, marking the first vertical landing by a Starship, and demonstrating that the recommendations produced by the proposed method are consistent. The actions implemented to address the recommendations from the systemic analysis are supported by identifying organizational needs through the aerospace context analysis. Unexpected results include the expansion of recommendations to managerial dimensions, extending beyond technical and operational analysis to encompass measures for sustaining the program over the long term. This includes considerations for relationships between the involved organizations, recommendations for continuous improvement and self-development, and strategies for achieving leadership in the aerospace sector.

As a future study proposal, the application of these methods in other areas, such as industry, commerce, and services, is suggested to assess the feasibility of identifying organizational needs and promoting social changes in different business environments and government organizations. Particularly, the development of digital techniques for identifying safety scenarios, organizational needs, and UCA is recommended to establish the necessary systemic requirements for managing operations. The adoption of systemic analysis for constructing prospective scenarios to guide organizational strategy enables the identification of a necessary future state grounded in the reality of the organizational context. This approach avoids purely technical or economic foundations that are blindly adopted to improve performance, instead considering the significant trends shaping the aerospace sector.

The findings of this study offer a theoretical contribution by advocating for a shift in managerial focus from traditional systemic safety analysis to an expanded approach that integrates organizational needs management. This represents a significant departure from historical managerial practices associated with conventional safety analysis methodologies.

## CONFLICT OF INTEREST

Nothing to declare.


## AUTHORS' CONTRIBUTION

**Conceptualization:** Reinhardt JCV and Lahoz CHN; **Methodology:** Reinhardt JCV; **Software:** Reinhardt JCV; **Validation:** Lahoz CHN and Dewes MF; **Formal analysis:** Reinhardt JCV and Lahoz CHN; **Investigation:** Reinhardt JCV; **Resources:** Reinhardt JCV; **Data Curation:** Reinhardt JCV and Dewes MF; **Writing - Original Draft:** Reinhardt JCV; **Writing - Review & Editing:** Reinhardt JCV and Lahoz CHN; **Visualization:** Reinhardt JCV; **Supervision:** González OL and Dewes MF; **Project administration:** González OL; **Funding acquisition:** Reinhardt JCV; **Final approval:** Reinhardt JCV.

## DATA AVAILABILITY STATEMENT

Data sharing is not applicable.

## FUNDING

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior   
Finance Code 001

## ACKNOWLEDGMENTS

Not applicable.

## REFERENCES

- Agence France-Presse (2019) SpaceX lança primeiros satélites para rede que vai prover internet do espaço. G1 Globo Economia. [accessed Aug 12 2019]. <https://g1.globo.com/economia/tecnologia/noticia/2019/05/24/spacex-lanca-primeiros-satelites-para-sua-rede-de-internet.ghtml>
- Aguilar FJ (1967) Scanning the business environment. New York: McGraw-Hill.
- Barstow J (2023) Application of systems-theoretic analysis to work movement in production systems (doctoral dissertation). Cambridge: Massachusetts Institute of Technology.
- Bittner B, Bozzano M, Cimatti A (2017) Timed failure propagation analysis for spacecraft engineering: the ESA solar orbiter case study. In model-based safety and assessment. Paper presented 2017 5th International Symposium on Model-Based Safety and Assessment. Springer; Trento, Italy.
- Brandão Neto N, Leite BRDA, Melo FCLD (2023) Model for strategic management of technological innovation in science and technology institutions in the Brazilian aerospace sector: a proposal. *J Aerosp Technol Manag* 15:e2123. <https://doi.org/10.1590/jatm.v15.1313>
- Cantu K, Lunsford RB (2022) Space travel privatization by SpaceX. *Review of Business and Finance Studies* 13(1):79-92.
- Creech S, Guidi J, Elburn D (2022) Artemis: an overview of NASA's activities to return humans to the moon. Paper presented 2022 IEEE Aerospace Conference. IEEE; Big Sky, USA. <https://doi.org/10.1109/AERO53065.2022.9843277>.
- Dias F (2019) O cenário atual e futuro do mercado de lançamentos de satélites, o engodo do governo Bolsonaro e as potencialidades da base de Alcântara. *Disparada*. [accessed Aug 11 2019]. <https://disparada.com.br/satelites-bolsonaro-base-de-alcantara/>
- [FAA] Federal Aviation Administration (2022) Final PEA for the SpaceX Starship/Super Heavy Launch Vehicle Program at the SpaceX Boca Chica Launch Site. FAA. [accessed Feb 02 2024]. [https://www.faa.gov/sites/faa.gov/files/2022-06/Final\\_PEA\\_Executive\\_Summary.pdf](https://www.faa.gov/sites/faa.gov/files/2022-06/Final_PEA_Executive_Summary.pdf)
- Fugivara S, Merladet AV, Lahoz CH (2021) STPA analysis of Brazilian sounding rockets launching operations. *Microgravity Sci Technol* 33(3):43. <https://doi.org/10.1007/s12217-021-09871-x>
- Goncalves Filho AP, Jun GT, Waterson P (2019) Four studies, two methods, one accident – An examination of the reliability and validity of AcciMap and STAMP for accident analysis. *Safety Sci* 113:310-317. <https://doi.org/10.1016/j.ssci.2018.12.002>
- House M (2021) SpaceX Starship kicked off the new space race – You haven't seen anything yet! YouTube. [accessed Jul 04 2021]. <https://www.youtube.com/watch?v=tbAqm6PCgq8>



- Hulme A, Stanton NA, Walker GH, Waterson P, Salmon PM (2024). Testing the reliability of accident analysis methods: a comparison of AcciMap, STAMP-CAST and AcciNet. *Ergonomics* 67(5):695-715. <https://doi.org/10.1080/00140139.2023.2240048>
- Ishimatsu T, Leveson NG, Thomas JP, Fleming CH, Katahira M, Miyamoto Y, Hoshino N (2014) Hazard analysis of complex spacecraft using systems-theoretic process analysis. *J Spacecraft Rockets* 51(2):509-522. <https://doi.org/10.2514/1.A32449>
- Ji XY, Li YZ, Liu GQ, Wang J, Xiang SH, Yang XN, Bi YQ (2019) A brief review of ground and flight failures of Chinese spacecraft. *Prog Aerosp Sci* 107:19-29. <https://doi.org/10.1016/j.paerosci.2019.04.002>
- Johnson CW, Almeida IM (2008). An investigation into the loss of the Brazilian space programme's launch vehicle VLS-1 V03. *Saf Sci* 46:38-53. <https://doi.org/10.1016/j.ssci.2006.05.007>
- Kopeikin A, Leveson N, Neogi NA (2024) System-theoretic analysis of unsafe collaborative control in teaming systems. Paper presented 2024 AIAA Science and Technology Forum and Exposition. AIAA; Orlando, USA.
- Kulu E (2023) In-space economy in 2023 – Statistical overview and trends. Paper presented 2023 74th International Astronautical Congress. Copernicus; Baku, Azerbaijan.
- Leveson NG (2004) A new accident model for engineering safer systems. *Safety Sci* 42(4):237-270. [https://doi.org/10.1016/S0925-7535\(03\)00047-X](https://doi.org/10.1016/S0925-7535(03)00047-X)
- Leveson NG (2015) A systems approach to risk management through leading safety indicators. *Reliab Eng Syst Saf* 136:17-34. <https://doi.org/10.1016/j.res.2014.10.008>
- Leveson NG (2016) *Engineering a safer world: systems thinking applied to safety*. Cambridge: USA. Massachusetts Institute of Technology. <http://library.oapen.org/handle/20.500.12657/26043>
- Leveson NG (2017) Rasmussen's legacy: a paradigm change in engineering for safety. *Appl Ergon* 59:581-591. <https://doi.org/10.1016/j.apergo.2016.01.015>
- Leveson NG (2019) CAST handbook: how to learn more from incidents and accident. [accessed Feb 06 2024]. <http://sunnyday.mit.edu/CAST-Handbook.pdf>
- Manley S (2021) SpaceX's Starship prototype takes to the skies and returns safely. YouTube. [accessed June 27 2021]. <https://www.youtube.com/watch?v=7IDMM63InLY>
- Marais K, Dulac N, Leveson NG (2004) Beyond normal accidents and high reliability organizations: the need for an alternative approach to safety in complex systems. Cambridge: USA. Massachusetts Institute of Technology. *Engineering Systems Division Symposium*; p. 1-16.
- Maslow AH (1981). *Introdução à psicologia do ser*. Rio de Janeiro: Eldorado.
- McNutt RL, Vernon SR, Brandt PC, Paul MV, Lusthaus RP (2024) High-speed scientific spacecraft launches with commercial launch vehicles. *Acta Astronautic* 217:18-26. <https://doi.org/10.1016/j.actaastro.2024.01.024>
- Mitikov Y, Shynkarenko O (2022) Reduction of the pressurization system final mass for a modern rocket launcher. *J Aerosp Technol Manag* 14:e0122. <https://doi.org/10.1590/jatm.v14.1238>
- Pessoa Filho JB (2021) Space age: past, present and possible futures. *J Aerosp Technol Manag* 13:e3421. <https://doi.org/10.1590/jatm.v13.1226>
- Rasmussen J (1997) Risk management in a dynamic society: a modelling problem. *Safety Sci* 27(2-3):183-213. [https://doi.org/10.1016/S0925-7535\(97\)00052-0](https://doi.org/10.1016/S0925-7535(97)00052-0)



Reinhardt JCV, Dewes MF, Gonzalez OL (2023) A new method for managing processes oriented towards satisfying the organization's needs. Paper presented 2023 27th International Congress of Mechanical Engineering. Associação Brasileira de Engenharia e Ciências Mecânicas; Florianópolis, Brazil. <https://doi.org/10.26678/ABCM.COBEM2023.COB2023-0542>

Reinhardt JCV, Dewes MF, Gonzalez OL (2024) Quality management systems' strategic structure oriented to organizational needs management. *J Aerosp Technol Manag* 16:e0924. <https://doi.org/10.1590/jatm.v16.1328>

Ricken MJ (2021a) #24: voo experimental de 10 km do SN10. Progresso da Starship. YouTube. [accessed Jul 04 2021]. <https://www.youtube.com/watch?v=beBI3ds GkRQt=477s>

Ricken MJ (2021b) #28: SN15 e a nova geração de protótipos da Starship. Progresso da Starship. YouTube. [accessed Jul 04 2021]. [https://www.youtube.com/watch?v=kS\\_cGqgOuUwt=756s](https://www.youtube.com/watch?v=kS_cGqgOuUwt=756s)

Rodrigues RG, Fulindi JB, Oliveira DBPD, Moraes ADO, Marini-Pereira L (2022) Safety analysis of GNSS parallel runway approach operation at Guarulhos International Airport. *J Aerosp Technol Manag* 14:e1622. <https://doi.org/10.1590/jatm.v14.1260>

Roy T (2023) Elon Musk's Starlink reaches cash-flow breakeven, eyes IPO and expansion. Alltech Magazine. [accessed Feb 27 2024]. <https://alltechmagazine.com/starlink-reaches-cash-flow-breakeven/>

Rubinstein L (2023) Starlink tem receita de US\$ 1,4 bilhão em 2022. Elon Musk erra projeção em mais de US\$ 10 bilhões. Blocktrends. [accessed Jan 27 2024]. <https://blocktrends.com.br/starlink-tem-receita-de-us-1-4-bilhao-em-2022-elon-musk-erra-projecao-em-mais-de-us-10-bilhoes/>

Seleme R, Stadler H (2012) Controle da qualidade: as ferramentas essenciais. Curitiba: Intersaberes.

Shaengchart Y, Kraiwanit T (2024) The SpaceX Starlink Satellite Project: business strategies and perspectives. *Corp Bus Strategy Rev* 5(1):30-37. <https://doi.org/10.22495/cbsrv5i1art3>

SpaceX (2021) Starship SN15 high-altitude flight test. YouTube. [accessed Aug 03 2021]. <https://www.youtube.com/watch?v=z9eoubnO-pE>

Sultana S, Haugen S (2023) An extended FRAM method to check the adequacy of safety barriers and to assess the safety of a socio-technical system. *Safety Sci* 157:105930, <https://doi.org/10.1016/j.ssci.2022.105930>

Thomas D (2024) SpaceX Starships reusability revolution: mitigating engine failure risks through advanced failure analysis. *J Fail Anal Prev* 1-3. <https://doi.org/10.1007/s11668-024-01943-5>

Van Looy A, Shafagatova A (2016) Business process performance measurement: a structured literature review of indicators, measures and metrics. *SpringerPlus* 5(1): 1-24. <https://doi.org/10.1186/s40064-016-3498-1>

Vittori D, Natalicchio A, Panniello U, Petruzzelli AM, Albino V, Cupertino F (2024) Failure is an option: how failure can lead to disruptive innovations. *Technovation* 129:102897, <https://doi.org/10.1016/j.technovation.2023.102897>

Wang B (2019) SpaceX Raptor engine will be best on cost and nearly best on ISP. Next big future. nestBIG Future. [accessed Jul 04 2021]. <https://www.nextbigfuture.com/2019/05/spacex-raptor-engine-will-be-best-on-cost-and-nearly-best-on-isp.html>

Weinzierl MC, Lucas K, Sarang M (2020) SpaceX, economies of scale, and a revolution in space access. Harvard Business School Case 720-027.

Yin RK (2009) Case study research: design and methods. Vol. 5. Thousand Oaks: Sage.



Yost B, Weston S (2024) State-of-the-art small spacecraft technology. No. NASA/TP-20240001462. [accessed Jul 20 2024]. [https://ntrs.nasa.gov/api/citations/20240001462/downloads/2023%20SOA\\_final.pdf](https://ntrs.nasa.gov/api/citations/20240001462/downloads/2023%20SOA_final.pdf)

Zahari AR, Romli FI (2019) Analysis of suborbital flight operation using PESTLE. J Atmos Sol-Terr Phy 192:104901. <https://doi.org/10.1016/j.jastp.2018.08.006>