Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27775-cd

SYSTEMIC FAILURE IN THE VLS-1 LAUNCH ACCIDENT: A CAST PERSPECTIVE

Henri von Buren
Technological Institute of Aeronautics, Brazil. E-mail: henriburen@ita.br

Bruno Nunes Vaz
Technological Institute of Aeronautics, Brazil. E-mail: brunovaz@ita.br

Moacyr Machado Cardoso Junior
Technological Institute of Aeronautics, Brazil. E-mail: moacyr@ita.br

This study applied the Causal Analysis based on System Theory (CAST) methodology to investigate the systemic causes of the 2003 VLS-1 rocket launch pad accident in Brazil. Following the five CAST steps, the analysis models the hierarchical safety control structure, formulates six explicit safety constraints, identifies four unsafe control actions with documentary evidence mapping, and grades each finding by confidence level (High/Medium) based on multi-source triangulation. The findings demonstrate that the tragedy resulted not from a single failure but from a cascade of systemic control flaws distributed across institutional, organizational, and technical layers that reinforce the utility of systems-theoretic methods, such as CAST, in complex environments, including space operations. CAST offers both explanatory and prescriptive value for improving safety culture and resilience in emerging space programs.

Keywords: CAST, space operations, rocket accidents, systems theory, complex systems.

1. Introduction

The increasing complexity of socio-technical systems, particularly in the aerospace domain, underscores the limitations of traditional accident investigation methods based on linear causality and component failure. In response, system theoretic approaches have emerged to better account for dynamic interactions, organizational factors, and feedback failures that characterize accidents in modern high-risk environments (Leveson, 2009, 2019). One such approach is CAST (Causal Analysis based on Systems Theory), which integrates principles from control theory and systems thinking to examine how safety constraints are violated across organizational levels (Zarei, Rafiee, & Leveson, 2024).

This article employs CAST to analyze the fatal accident that impacted the third prototype of Brazil's Satellite Launch Vehicle (VLS-1 V03) in 2003. The unintentional ignition of the first-stage booster during final prelaunch procedures at the Alcântara Launch Center (CLA) resulted in 21 fatalities and the destruction of critical national aerospace infrastructure (Brasil, 2004; Johnson & de Almeida, 2008). Rather than attributing causality to individual error or technical malfunction (Bôas, 2005; Moltz, 2015), this study reconstructs the socio-technical control structure and identifies systemic failures in communication, coordination and feedback mechanisms (Rollemberg, Coelho, & Veloso, 2010; Vaz, 2024).

Several systemic methods could be applied to this case. AcciMap (Rasmussen, 1997; Rasmussen & Svedung, 2000) supports multi-level mapping of decision-making, goal conflicts, and pressure-driven migration to safe operating limits, but is less explicit in modeling control actions, feedback adequacy, and enforceable safety constraints as a closed-loop problem (Branford, Hopkins, & Naikar, 2009). FRAM - the Functional Resonance Analysis Method (Hollnagel, 2012) excels at analyzing everyday performance variability and functional couplings, but is less direct at representing hierarchical accountability. Hopkins' frame-

work (2005, 2006) explains how safety is shaped by organizational priorities, learning, and cultural patterns, though through qualitative interpretive strategies rather than control-theoretic representations.

Therefore, in this article, CAST is adopted as the primary analytical backbone to reconstruct hierarchical control structures, safety constraints, and feedback paths, and to derive redesign recommendations grounded in the structure of control and assurance (Leveson, 2004, 2012). Hopkins' concepts serve as a complementary interpretive lens to strengthen the discussion of organizational culture, learning, and systemic drift.

The primary documentary source is the 130-page official investigation report issued by the Brazilian Air Force's Technical Investigation Commission (Brasil, 2004). The report comprises four analytical sub-commissions: Meteorological Factor, Material Factor, Operational Factor, and Human Factor. Secondary sources include Johnson and de Almeida's (2008) independent safety-science analysis, Bôas's (2005) technical description of VLS-1, and institutional records from AEB and the Brazilian Congress (Brasil, 2009; Rollemberg et al., 2010; Vaz, 2024). The use of multiple independent sources covering the same event allows systematic cross-validation: claims supported by two or more sources are graded as HIGH confidence, while those resting primarily on a single source are graded MEDIUM (see Table 2).

1.1. *Research Questions*

RQ1: What were the key breaches of safety constraints and where were they documented (or absent)?

RQ2: Where did control and feedback break down across hierarchical levels (government– agency– operations– hardware)?

RQ3: What control structure redesigns would have prevented ignition-with-personnel-present?

2. Background

2.1. *The Brazilian Space Program*

The Brazilian Space Program developed over three phases. The institutional consolidation (1940-1999), including the creation of the Ministry of Aeronautics (1941), the Aerospace Technical Center (CTA, 1946) and the Aeronautics Institute of Technology (ITA, 1950); the Comprehensive Brazilian Space Mission (MECB, 1979–1994), which pursued indigenous satellite and launch-vehicle capabilities; and the current AEB-led phase (1994 to present) under the governance framework of the National System for the Development of Space Activities, SINDAE (Rollemberg et al., 2010; Vaz, 2024). This institutional context is essential to understand the organizational environment in which the VLS-1 program operated.

2.2. *The VLS-1 V03 Accident*

The VLS-1 was a four-stage solid-propellant vehicle, approximately 19 m high and 50 tons at liftoff, designed for payloads of 100-350 kg to low Earth orbit (Johnson & de Almeida, 2008; Bôas, 2005). Structurally, it employed a clustered first-stage configuration with strap-on boosters around a central core, enabling sequential staging toward orbital insertion (Bôas, 2005). The first prototype (V01, 1997) failed due to a malfunctioning mechanical safety device (DMS); the second (V02, 1999) was destroyed after a second-stage propellant failure.

On 22 August 2003, an explosion in the CLA Mobile Integration Tower (TMI) killed 21 professionals. The incident occurred during the final preparation phase for the launch of the VLS-1 V03. At that time, the rocket was fully assembled and vertically positioned within the TMI, with integration procedures at an advanced stage, including electrical testing of the ignition and safety systems. Several civilian technicians and engineers were inside the tower performing verification activities when the explosion occurred. Most of the personnel were in the propellant preparation building, the bunker, and the support house, while others were moving between facilities within the preparation and launch sector.

The official investigation established that Booster A fired nominally for approximately 40 seconds, initiated by the inadvertent activation of one of its detonators (Brasil, 2004, Ch. 3.2). The inves-

tigation commission constructed a 26-event fault tree and retained two plausible hypotheses: (a) electrical current through the 'line of fire', and (b) electrostatic discharge (ESD) inside the detonator. The commission assessed hypothesis (b) as more probable, because the original shielded wires in the fire line had been replaced with unshielded twisted-pair following a 1998 technical memorandum (nº 011/GES-VLS/98), and because a non-conductive plastic cap inflated with dry, cold air may have facilitated static charge accumulation (Brasil, 2004, Ch. 3.2). No active failure—i.e., an immediate human error that directly initiated the accident—was identified. The commission concluded that the accident was rooted in latent failures: decisions and conditions established well before the event whose consequences remained dormant until they combined under operational stress (Brasil, 2004, Chap. 4, Conclusions 4-6).

3. CAST analysis

The following sections present each of the five CAST steps (Zarei et al., 2024) applied to the VLS-1 V03 accident.

3.1. *Step 1: Assemble Basic Information*

The first step is to gather all relevant information about the incident. This includes collecting technical documentation, procedural records, organizational charts, communication logs, and contextual factors such as regulatory constraints, resource limitations, or political pressures. The goal is to develop a comprehensive understanding of the system and the environment in which the loss occurred. Data sources were mapped to specific report chapters:

Material Factor (Ch. 3.2) — fault tree, physical evidence from recovered ignition assemblies, X-ray radiographs, and laboratory tests;

Operational Factor (Ch. 3.3) — CLA infrastructure, access control, planning and coordination, quality management, and configuration control;

Human Factor (Ch. 3.4) — 90 structured and semi-structured interviews in CTA/IAE, CLA, and CLBI, covering psychosocial climate, staff shortages, and safety culture indicators;

Meteorological Factor (Ch. 3.1) — confirming benign weather on 22 August. Cross-validation was based on Johnson and de Almeida (2008) and congressional records (Brasil, 2009).

3.2. *Step 2: Model the Safety Control Structure*

Then a control structure is modeled to represent the hierarchical organization of the actors and subsystems involved in the operation. This structure identifies the various levels of control—typically ranging from strategic decision-making bodies to operational teams and technical components—along with the control actions and feedback loops that link them. The purpose is to visualize how commands, responses, and information flow throughout the system and to expose potential points of failure in coordination and oversight.

Four hierarchical levels were modeled from the operational plan issued by the Department of Research and Development (DEPED) of the Brazilian Air Force (Operations Plan 006/2002), the CLA's *Síntese da Qualidade dos Meios Operacionais*, and the SINDAE structure. DEPED is the first-level organ of the Air Force Command to which both CTA and CLA are subordinate; it was responsible for authorizing and coordinating launch operations (Brasil, 2004, Chap. 3.3).

Strategic level: Ministry of Defense and Ministry of Science, Technology and Innovation. Control actions: define national space policy, allocate budgets, and set program priorities. Feedback observed: limited—resource allocation decisions were disconnected from operational safety indicators, as evidenced by the widening gap between required and available human and financial resources documented in the official report (Brasil, 2004, Ch. 3.4, Figs. 97–102).

Coordination level: FAB (through DEPED) and AEB. FAB approved and managed launch operations; AEB nominally coordinated SINDAE. Feedback observed: AEB lacked operational authority and had no mechanisms to intervene in military-managed activities. FAB concentrated both operational execution and oversight within the same institutional chain (Vaz, 2024; Johnson & de Almeida, 2008).

Operational level: CTA/IAE (Institute of Aeronautics and Space) and CLA (Alcântara Launch Center). IAE planned and executed vehicle integration and testing; CLA provided infrastructure, logistics, and launch security. Feedback observed: risk assessment was subjective; The access of TMI was controlled informally through team leaders without nominal log; no independent indicator confirmed the status of the ignition-circuit (Brasil, 2004, Chap. 3.3, pp. 66–69).

Technical level: Test and integration teams, fireline circuitry, relay box, detonators, and solid-propellant boosters. Control actions: execute assembly procedures, connect and disconnect pyrotechnic circuits. Feedback observed: no automated feedback; operational safety relied on procedural assumptions and manual checklists, with no real-time diagnostic systems monitoring circuit state (Brasil, 2004, Ch. 3.2).

3.3. *Step 3: Analyze Controller Behavior and Safety Constraints*

The third step consists of analyzing the behavior of each controller within the structure, human and automated. The investigators evaluated the information available to the controllers at the time of the event, the decisions made based on that information, and whether the relevant safety constraints were adequately enforced or monitored. This analysis clarifies the extent to which each controller's mental model aligned with the actual state of the system and identified gaps in situational awareness or decision support. Safety constraints were derived from explicit normative requirements (MIL-STD-1576; NBR 14882) and from the necessary conditions for safe operation that were absent.

Table 1 presents six main constraints, their expected enforcement, their actual status, and supporting evidence. Based on these constraints, four unsafe control actions (UCA) are identified:

UCA-1 (CTA/IAE Test Teams): Connected detonators to the fire line (task VLS-60.40), while integration tasks were still ongoing in the TMI, creating a live-armed condition with personnel present. Violated SC-2; enabled by the absence of a task-interlock mechanism that prevents the pyrotechnic connection until tower clearance was confirmed.

Table 1. *Safety constraints, enforcement status, and evidence sources.*

ID	Safety Constraint	Expected Mechanism	Actual Status	Evidence
SC-1	No current in detonator circuits prior to launch authorization	Mechanical safety devices (DMS) + relay box short-circuit	DMS removed after V01 failure; relay box provided only electrical, not physical, isolation	Brasil 2004, Ch. 3.3, pp. 69–70; MIL-STD-1576
SC-2	Pyrotechnic connection to fire line only after all integration tasks complete	Task sequencing per Assembly Plan Doc. 590-000000/B5005	Detonators of Boosters A and D connected on morning of 22 Aug while integration tasks continued in TMI	Brasil 2004, Ch. 3.3, p. 69; task VLS-60.40
SC-3	Safety organization operationally independent from hazardous-operations executor	Independent safety authority per NBR 14882, §4.5.2	CTA/IAE teams performed both execution and verification; CLA lacked qualified safety staff	Brasil 2004, Ch. 3.3, pp. 66–67; NBR 14882
SC-4	Minimize personnel in TMI during hazardous operations	Formal access control; risk-graded scheduling	21 persons present; access controlled informally without nominal logging	Brasil 2004, Ch. 3.3, pp. 66–67; Ch. 3.4, p. 97
SC-5	Safety-critical electrical changes via formal configuration management	Configuration Commission per Doc. 590-0000/A4201	Shielded wire replaced via informal memo without project management sign-off	Brasil 2004, Ch. 3.3, pp. 70–71; Memo 011/GES-VLS/98
SC-6	AEB effective oversight over military-managed operations	SINDAE governance mandate	AEB lacked operational authority to intervene in FAB-managed activities	Vaz 2024; Rollemberg et al. 2010; Johnson & de Almeida 2008

UCA-2 (CTA/IAE Engineering): Authorized the substitution of shielded wiring with unshielded twisted-pair via an informal technical memorandum, without a system-level impact assessment or project management notification. Violated SC-5; removed a critical electromagnetic protection layer.

UCA-3 (CLA Safety Organization): Failed to enforce independent access control and formal risk assessment for TMI operations, allowing 21 persons inside the tower during a phase when pyrotechnic circuits were energized. Violated SC-3 and SC-4.

UCA-4 (AEB): Did not exercise operational oversight or intervene in military-managed safety-critical operations, despite its formal SINDAE mandate. Violated SC-6; left safety assurance concentrated entirely within FAB/CTA structures.

3.4. *Step 4: Identify Control Structure Flaws*

The fourth step focuses on identifying the flaws in the control structure that contributed to the loss. These may include missing or delayed feedback, inadequate sensor information, lack of functional independence, or concentration of control responsibilities in a single actor. Institutional fragmentation, communication asymmetries, or the absence of independent validation mechanisms can also be highlighted as structural weaknesses that compromise the integrity of safety-related decisions.

Five systemic flaws are identified in the control structure:

Flaw 1 – Missing physical safety barrier: mechanical safety devices (DMS), which provided a

physical interruption between the detonator and the ignition chain, were removed after the V01 failure. The replacement relay box offered only electrical isolation, without mechanical backing. The existence of a DMS could have prevented the accident even if the detonator had been accidentally energized (Brasil, 2004, Chap. 3.3, pp. 69–70).

Flaw 2 – Absent circuit-state feedback: No automated or independent indicator confirmed to personnel in the TMI, or to the control bunker, whether the fire-line relay box was in a safe (short-circuited) or armed state. Relay logic was assumed to maintain safety interlocks, but no diagnostic system monitored its actual condition in real time (Brasil, 2004, Chap. 3.2).

Flaw 3 – Consolidated execution and verification: The teams responsible for executing test procedures were also tasked with interpreting the results, merging the control and verification functions within a single operational layer. No independent body verified critical safety configurations. This violated NBR 14882, §4.5.2, which requires operational independence of the safety organization (Brasil, 2004, Chap. 3.3).

Flaw 4 – Contradictory safety hierarchy: The CLA's own document (*Síntese da Qualidade dos Meios Operacionais*) placed the Safety Coordinator subordinate to the Launch Coordinator, whereas the DEPED Operations Plan 006/2002 placed them at the same hierarchical level (Brasil, 2004, Chap. 3.3, p. 64). This structural contradiction created an ambiguity about who had authority to stop operations for safety reasons.

Flaw 5 – Degraded strategic feedback: Quantitative data in the official report show that the gap between required and allocated human resources widened steadily from 1987 onward (Brasil, 2004, Ch. 3.4, Figs. 97–99), and financial resources followed a similar trajectory (Figs. 100–102). The commission concluded that the prolonged coexistence with resource scarcity may have led to a growing inability to perceive the degradation of working conditions and safety (Brasil, 2004, Ch. 4, Conclusion 6). Decision-makers at the Ministerial and AEB levels did not translate these resource gaps into safety risk indicators.

3.5. *Step 5: Generate Recommendations*

Finally, the last step focuses on generating recommendations to enhance the system's resilience and prevent recurrence. These recommendations may span technical, procedural, and organizational domains, such as redesigning feedback loops, implementing automated safety interlocks, separating roles to ensure independent verification, or reforming governance structures to reduce ambiguity in safety responsibilities. The CAST approach thus facilitates a comprehensive and constructive examination of system-level contributors to accidents, offering prescriptive insights grounded in systems thinking. Upon analyzing the control structure, several flaws became evident. Feedback from the ignition system was either non-existent or insufficiently monitored. The technicians responsible for executing the procedures were also tasked with interpreting the results, thereby consolidating control and verification functions within a single operational layer. An independent body was not present to verify critical safety configurations. Furthermore, the institutional division between military and civilian organizations created blurred accountability and fragmented governance, preventing a comprehensive assessment and mitigation of risk.

Based on these insights, CAST enabled the formulation of system-level recommendations to improve safety and resilience. Six system-level recommendations are derived from the identified flaws:

R1 (Flaw 1, SC-1): Reinstate or redesign mechanical safety devices that provide physical interruption of the ignition chain, compliant with MIL-STD-1576.

R2 (Flaw 2): Implement real-time automated feedback that confirms the safe state of all ignition circuits, visible to both tower personnel and the control bunker.

R3 (Flaw 3, SC-3): Establish an independent safety authority, structurally separated from operational command, with veto power over launch operations.

R4 (Flaw 4, SC-2, SC-4): Implement procedural interlocks that prevent pyrotechnic connection

while personnel are in the TMI, and resolve organizational ambiguity by establishing a single unambiguous safety command chain.

R5 (SC-5): Mandate formal configuration management for all safety-critical electrical modifications, requiring system-level impact assessment, independent review, and project management approval prior to implementation.

R6 (SC-6, Flaw 5): Empower AEB with operational oversight resources, audit mechanisms, and the authority to mandate corrective actions. Establish a resource-adequacy feedback loop that requires periodic independent assessment of whether human and financial resources are sufficient to maintain safety margins. Through this structured and systems-oriented approach, CAST provided not only a deeper understanding of the accident but also practical guidance for reforming Brazil's space governance and engineering practices to prevent future failures.

4. Discussion

The CAST analysis (Fig. 1) reveals a system operating in a degraded resilience state. This systemic fragility resulted from a combination of institutional fragmentation, unverified safety constraints, and ineffective governance mechanisms. At the technical level, the absent feedback on ignition-circuit status (Flaw 2) is the most consequential gap: the relay box assumed a safe short-circuit but provided no independent confirmation to operators. This exemplifies Leveson's (2012) principle that unmonitored control actions and weak feedback are critical vulnerabilities in socio-technical systems. At the operational level, the concurrent execution of integration tasks and pyrotechnic connection on the morning of 22 August illustrates a fundamental task-sequencing failure. While the electronics team connected Boosters A and D to the fire line, the propulsion team was pressurizing actuator systems at levels 1 and 3, the integration team was fixing cable trays at levels 4 and 5, and an imaging team was adjusting cameras at level 5 (Brasil, 2004, Chap. 3.2). Interviews conducted by the Human Factor subcommission revealed a pervasive sense of security, reinforced by the successful second launch rehearsal (Brasil, 2004, Ch. 3.3, p. 69). This is consistent with Hopkins's (2005) analysis of how normalized risk perception erodes safety culture over time. At the coordination level, contradictory organizational charts (Flaw 4) created ambiguity about the safety authority. The operational impotence of AEB (UCA-4) concentrated all safety assurance within FAB/CTA, which simultaneously executed the operations it was supposed to supervise. Similar patterns have been documented in other CAST applications in aerospace and industrial contexts, often allowing unsafe practices to persist unchecked (Leveson & Thomas, 2009; Vert, Sharpanskykh & Curran, 2021). At the strategic level, the progressive erosion of resources documented in the official report (Brasil, 2004, Chap. 3.4, Figs. 97–102) was not translated into safety risk indicators at the Ministerial level, which constitutes degraded strategic feedback (Flaw 5). As CAST emphasizes, safety constraints must not only be documented, but actively enforced through technological and organizational mechanisms (Leveson, 2012). In the VLS-1 system, the failure to incorporate constraints in automated interlocks or diagnostic systems prevented the timely detection and mitigation of unsafe conditions. This resonates with observations from other CAST analyses, which highlight that systems that rely heavily on procedural compliance and tacit knowledge are inherently fragile under stress (Leveson & Thomas, 2009). The findings also reinforce the utility of CAST not only as a diagnostic tool but also as a guide for designing robust socio-technical systems that integrate independent oversight, redundant safety functions, and real-time feedback.

4.1. *Alternative Hypotheses*

A linear event-chain account focusing on wire shielding alone would fail to explain why shielding was removed in the first place (inadequate configuration management, SC-5), why personnel were present when the pyrotechnics were armed (failures of SC-2, SC-3, SC-4), and why no independent body questioned these conditions (failure of SC-6). The added value of CAST lies in revealing how multiple individually insufficient control

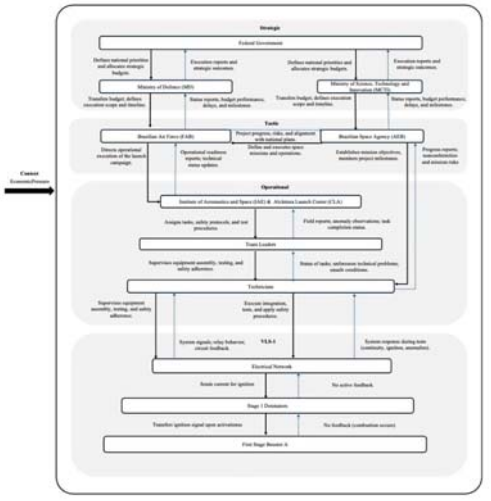

Fig. 1. CAST analysis

failures combined to produce a lethal outcome. Sabotage was investigated by the commission and was considered low probability, given the comprehensive electromagnetic monitoring by FAB and Army units, military patrols, and the two-hour gap between the electrical connection of Booster A and the ignition event.

4.2. *Confidence Grading*

Table 2 summarizes the confidence level assigned to each key finding.

Table 2. *Confidence grading of key CAST findings.*

Finding	Level	Supporting Sources
Inadvertent detonator activation initiated Booster A	HIGH	X-ray radiographs, video surveillance, 26-event fault tree (Brasil 2004, Ch. 3.2); corroborated by Russian specialists; confirmed by Johnson & de Almeida (2008)
DMS removal increased ignition vulnerability	HIGH	Brasil 2004, Ch. 3.3, pp. 69–70; MIL-STD-1576 prescribes mechanical devices; Johnson & de Almeida (2008) independently identify this decision
Fire-line shielding removal contributed to ESD vulnerability	HIGH	Memo 011/GES-VLS/98 documented in Brasil 2004, Ch. 3.3, p. 71; laboratory tests confirmed static induction risk (Ch. 3.2)
Consolidated execution and verification	HIGH	Brasil 2004, Ch. 3.3; NBR 14882, §4.5.2; Johnson & de Almeida (2008)
Resource degradation as latent systemic factor	HIGH	Quantitative HR and financial data (Brasil 2004, Ch. 3.4, Figs. 97–102, Tables 2–4); 90 interviews; Moltz (2015); congressional review (Brasil, 2009)
AEB lacked operational oversight authority	MEDIUM	Implied in Brasil (2004); corroborated by Vaz (2024), Rollemberg et al. (2010), Johnson & de Almeida (2008)
ESD inside detonator as most probable proximal cause	MEDIUM	Commission assessment by elimination; acknowledged that this hypothesis was analysed less exhaustively than the electrical-current hypothesis (Brasil 2004, Ch. 3.2, p. 62)

4.3. *Limitations*

Reconstruction relies on the available documentary record; informal coordination practices, time-critical sensemaking, and undocumented decision rationales are only partially observable, necessitating interpretive assumptions when modeling controller objectives, control actions, and feedback paths (Leveson, 2019). The control structure model encompasses four hierarchical levels based on entities documented in the DEPED Operations Plan and the SINDAE structure. Entities outside this boundary (e.g., component suppliers, foreign governments imposing embargoes) are acknowledged as contextual factors but are not modeled as controllers, because they did not exercise direct control actions during the operation. Finally, the conclusions are derived from a single case study and offer analytically generalizable insights rather than statistically generalizable claims.

5. Conclusion

This study applied the CAST methodology to analyze the systemic causes underlying the 2003 VLS-1 launch pad accident in Brazil. The investigation revealed that the tragedy was not attributable to a single failure point or an isolated human error, but rather to a cascade of systemic control flaws embedded across institutional, organizational, and technical layers. The absence of automated safety feedback, the fragmentation of governance between civil and military entities, and the lack of independent verification mechanisms combined to create a socio-technical environment inherently vulnerable to failure under operational stress. Regarding RQ1, six safety constraints (SC-1 through SC-6) were identified, each of which was violated or not enforced properly at the time of the accident (Table 1). These constraints span the technical domain (SC-1: circuit isolation; SC-2: task sequencing; SC-5: configuration management), the operational domain (SC-3: safety independence; SC-4: personnel exposure), and the strategic domain (SC-6: civilian oversight authority). Regarding RQ2, control and feedback breakdowns occurred at all four hierarchical levels: absent physical barriers and missing circuit-state feedback at the technical level (Flaws 1–2); consolidated execution and verification with informal access control at the operational level (Flaws 3–4); The operational impotence of AEB at the coordination level (UCA-4, SC-6); and the disconnect between resource decisions and safety indicators at the strategic level (Flaw 5).

Regarding RQ3, recommendations R1–R6 (Section 3.5) specify control-structure redesigns: mechanical interlocks (R1), automated circuit-state feedback (R2), an independent safety authority with veto power (R3), procedural lockouts and an unambiguous safety command chain (R4), formal configuration management (R5), and empowered civilian oversight with resource-adequacy feedback (R6). The majority of findings are supported with HIGH confidence from multiple independent sources (Table 2).

These findings underscore the value of systems-theoretic approaches such as CAST in the context of complex aerospace operations. Future Brazilian aerospace initiatives and comparable emerging space programs must institutionalize system safety engineering from the outset. CAST serves not only as a retrospective analytical framework, but also as a forward-looking toolkit to strengthen safety culture and resilience. The lessons from the VLS-1 accident should inform both national policy and organizational redesign of Brazil's space governance structures, paving the way for a safer and more sustainable space program.

Acknowledgment

This work was supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES) - Finance Code 001.

References

Bôas, D. J. F. V. (2005). O veículo lançador de satélites VLS-1. Anais da 1ª Jornada Espacial Brasileira, São José dos Campos, SP.

Branford, K., Hopkins, A., & Naikar, N. (2009). Guidelines for AcciMap analysis. In A. Hopkins (Ed.), Learning from high reliability organisations (pp. 193–212). CCH Australia Ltd.

Brasil. Comando da Aeronáutica. (2004, February 10). VLS-1 V03: Relatório da investigação do acidente [Final report]. São José dos Campos: Instituto de Aeronáutica e Espaço.

Brasil. Congresso Nacional. Câmara dos Deputados. (2009). Caderno de Altos Estudos – A política espacial brasileira. Brasília, DF: Conselho de Altos Estudos e Avaliação Tecnológica.

Hollnagel, E. (2012). FRAM, the Functional Resonance Analysis Method: Modelling complex socio-technical systems. Ashgate.

Hopkins, A. (2005). Safety, culture and risk: The organisational causes of disasters. CCH Australia.

Hopkins, A. (2006). Studying organisational cultures and their effects on safety. Safety Science, 44(10), 875–889.

Johnson, C. W., & de Almeida, I. M. (2008). An investigation into the loss of the Brazilian space programme´s launch vehicle VLS-1 V03. Safety Science, 46(1), 38-53.

Leveson, N. G. (2004). A new accident model for engineering safer systems. Safety Science, 42(4), 237–270.

Leveson, N. G., & Thomas, J. P. (2009). STAMP handbook: system-theoretic accident model and processes. MIT.

Leveson, N. G. (2012). Engineering a safer world: Systems thinking applied to safety. MIT.

Leveson, N. G. (2019). CAST handbook: How to learn more from accidents and incidents. MIT.

Moltz, J. C. (2015). Brazil's space program: Dreaming with its feet on the ground. Space Policy, 33, 13–19.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2–3), 183–213.

Rasmussen, J., & Svedung, I. (2000). Proactive risk management in a dynamic society. Swedish Rescue Services Agency.

Rollemberg, R., Coelho, D. A. S., & Veloso, M. M. (2010). A política espacial brasileira: 50 anos de história. Brasília, DF: Câmara dos Deputados.

Vaz, B. N. (2024). Um panorama do ecossistema espacial brasileiro no New Space (Master's thesis). ITA, São José dos Campos.

Vert, M., Sharpanskykh, A., & Curran, R. (2021). Adaptive resilience of complex safety-critical socio-technical systems: Toward a unified conceptual framework and its formalization. Sustainability, 13(24), 13915.

Zarei, E., Rafiee, A., & Leveson, N. G. (2024). Causal analysis based on systems theory (CAST) in complex systems. In A. Rafiee & E. Zarei (Eds.), Systems engineering approaches for complex safety-critical systems (pp. 277–284). Springer.