



# Comparison of CAST and FTA results in the Investigation of a Suborbital Rocket Launch Accident

Capt. Diniz - Dra. Chiara Manfletti - Dr. Carlos Lahoz  
Col. Clovis – Dr. Ricard González Cinca

2025 MIT STAMP Workshop





## Objective

This research applies CAST to determine the causal factors of a VSB-30 suborbital rocket accident that occurred during a launch operation at Alcântara Launch Center (CLA), Brazil, in 2016.

The results from CAST are then compared with the official accident investigation report, which primarily relied on Fault Tree Analysis (FTA) to identify component failures and determine the root cause of the accident.

# Headlines:

- 1) Accident Overview
- 2) CAST for the VSB-30 accident
- 3) Fault Tree Analysis (FTA) of the accident
- 4) Criteria and results of the comparison



# Launcher System Overview

**VSB-30:** A suborbital two-stage rocket designed for microgravity experiments.

**Launch Platform:** A Mobile Launcher (LM) with the rail adapted for this mission.

**RESTRICTED**



# Payload System Overview

**Payload:** MICROG2 experiments involving multiple institutions, including the INPE, IEAV and universities.

**RESTRICTED**

# Accident Overview

On December 7, 2016, the VSB-30 V11 (Rio Verde Operation) was launched from the CLA - Maranhão, Brazil. The mission involved carrying out scientific experiments requiring microgravity conditions and aimed to demonstrate the reliability of the VSB-30 system.

## VSB-30 V11 Flight

- **First-stage success:** The S31 motor ignited and burned as expected, successfully separating from the rocket.
- **Second-stage anomaly:** During the S30 motor burn, the payload separated prematurely, deviating from the nominal trajectory.
- **Trajectory deviation:** The payload reached a lower apogee, not achieving microgravity requirements.
- **Payload recovery:** Despite the anomaly, the payload was successfully recovered from the sea.





# Accident Overview

## Losses and Consequences

- **Mission Loss:** The impossibility of microgravity conditions for the onboard experiments.
- **Safety Breach:** The payload landed outside the designated safety area.
- **Operational Setback:** The incident affects the reliability of the VSB-30 system and required an extensive investigation.

## Key anomalies:

- **Ground system interactions.**
- **Empennage Deformation.**
- **Telemetry Data loss.**
- **Premature Separation.**

## Payload Trajectory

**RESTRICTED**



# Accident Overview

## Ground system:

- Ground **Tracking** Systems were configured to follow payload transponder.
- Design, setup, or calibration of the launch platform **flame deflector**, generating flame backflow.

**RESTRICTED**

# Accident Overview

## Empennage Deformation:

- An **updated** and flight-validated **fin project** was available for production.
- Indications of **storage damages** that demanded the necessity of restorations.
- **Deformation of the S30 stage fins** >> unbalanced forces.
  - Comparative evidence: Similar deformation was observed in a previous launch operation (VSB-30 V07).

**RESTRICTED**



DEPARTMENT OF AEROSPACE SCIENCE AND TECHNOLOGY  
Sovereignty in the form of Science and Technology



INDUSTRIAL FOSTERING AND COORDINATION INSTITUTE  
*Wings for a strong industry*



# Accident Overview

**RESTRICTED**

# Accident Overview

## Premature Separation:

- Integration procedures have been designed for vertical assembly. Adjustment torque release tasks were performed in the past but have never been inserted into the procedures.
- Separation mechanism could not resist unusual flight mechanical load.

**RESTRICTED**

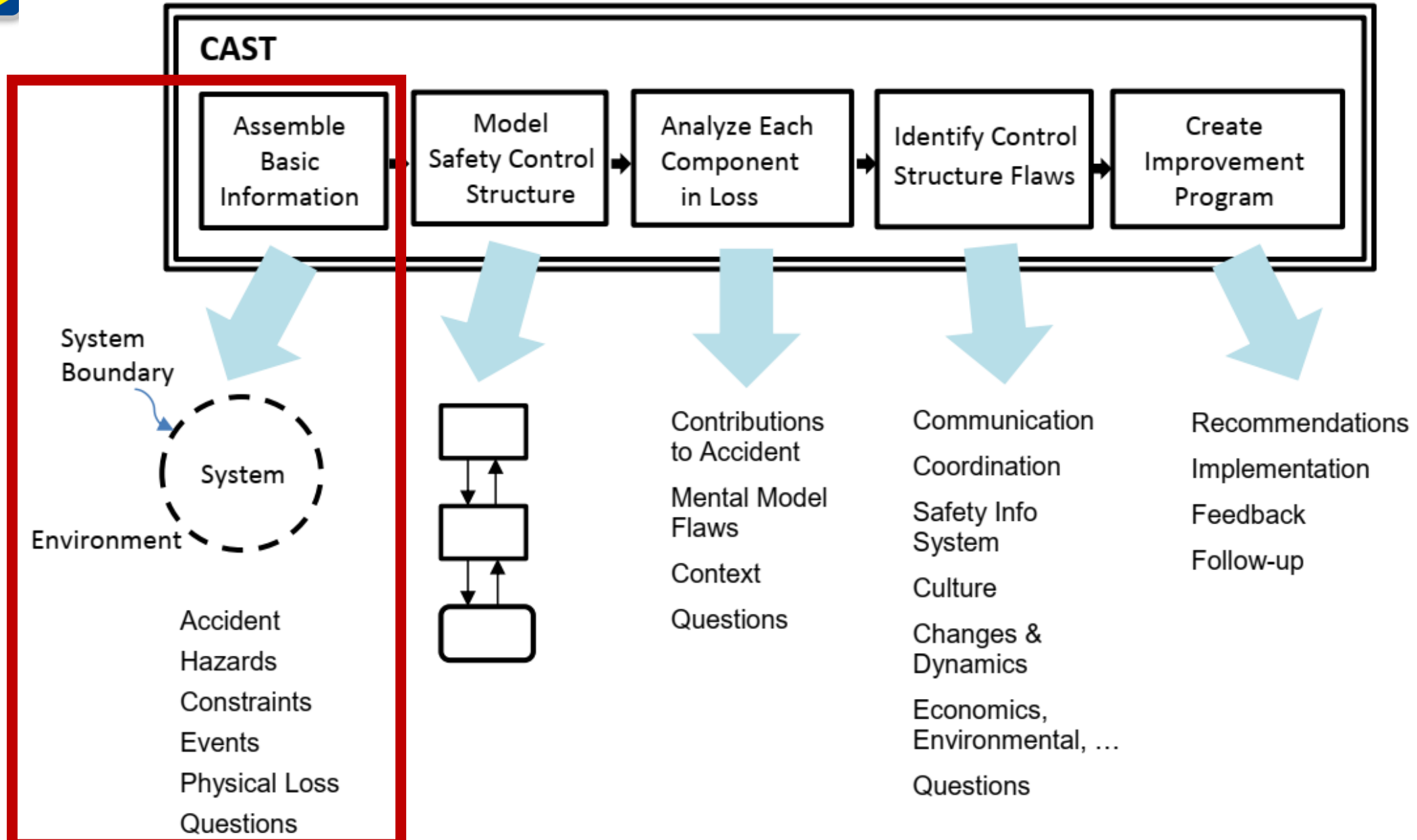


# Accident Overview

## Telemetry Data Loss:

- Onboard cameras were not working properly (discovered during pre-launch tests).
- Part of the telemetry data was not transmitted due to damage to one of the pins from cable connectors. (recovered parts)

**RESTRICTED**



# System-level Hazards

## **SH-1: Uncontrolled separation of the payload during flight**

**System State/Condition:** The payload separates previously from the rocket or remains attached to the rocket under conditions outside the intended timing or parameters.

## **SH-2: Aerodynamic instability during flight**

**System State/Condition:** The rocket experiences excessive roll, pitch, or yaw, deviating from its intended aerodynamic trajectory.

## **SH-3: Structural compromise of rocket/payload components during flight**

**System State/Condition:** Critical rocket components, such as fins or separation systems, deforms during flight, reducing the rocket's ability to perform as intended.

## System-level Hazards

**SH-4: Ground systems inducing adverse interactions with the launch vehicle.**

**System State/Condition:** Interaction between ground systems (such as electric, mechanical, software, or communication systems) and the launch vehicle that induces anomalies, creating the potential for compromising safety, performance, or mission assurance.

**SH-5: Undetermined trajectory and Point of Impact of rocket stages after separation**

**System State/Condition:** Following an unintended separation of the payload from the rocket, the trajectory and point of impact of the rocket stages become undetermined as the tracking system focuses solely on the payload equipped with a transponder.

**SH-6: Rocket stages or payload reaching unsafe areas (out of prescribed Flight Safety Limits) due to early separation**

**System State/Condition:** The rocket stages or payload deviate from the predetermined flight path, impacting areas outside the designated safety boundaries.



# Raised Questions

Events	Questions Raised
<p><b>EV.1: INTEGRATION</b> - The rocket was prepared and integrated, including payload, propulsion stages (S31 and S30), and separation mechanisms.</p>	<p><b>Q.1.3:</b> Were all assembly procedures executed and verified during the pre-launch phase following approved protocols?</p>
<p><b>EV.2: S31 / LAUNCH RAIL</b> - The S31 first-stage motor ignited successfully (with a backflow of flame at the launch rail during the ignition phase going up to second stage), the rocket lifted off, and the first-stage separation occurred as planned, with the second-stage motor (S30) igniting.</p>	<p><b>Q.2.2:</b> Was the separation between the first and second stages within design parameters?</p> <p><b>Q.2.4:</b> What caused the observed flame backflow after ignition?</p> <p><b>Q.2.6:</b> Could the flame backflow affect the vehicle/payload structure or the separation mechanism?</p>
<p><b>EV.3: PREMATURE SEPARATION</b> - During the S30 motor burn (second stage), the payload separated prematurely, deviating from the intended mission profile, and the rocket was not able to achieve the planned mission profile.</p>	<p><b>Q.3.2:</b> Was the separation mechanism influenced by structural deformation, electrical issues, or software anomalies?</p> <p><b>Q.3.3:</b> Are the ground systems limited to perform tracking of only one flying component or is it capable of tracking multiple rocket stages and the payload simultaneously?</p>
<p><b>EV.4: PAYLOAD RECOVERY</b> - The payload recovery system activated successfully, and the payload was retrieved from the sea; however, the primary mission objective of achieving microgravity conditions was not met, rendering scientific experiments unviable.</p>	<p><b>Q.4.2:</b> Were there signs of damage or stress on the payload separation mechanism or other components?</p>

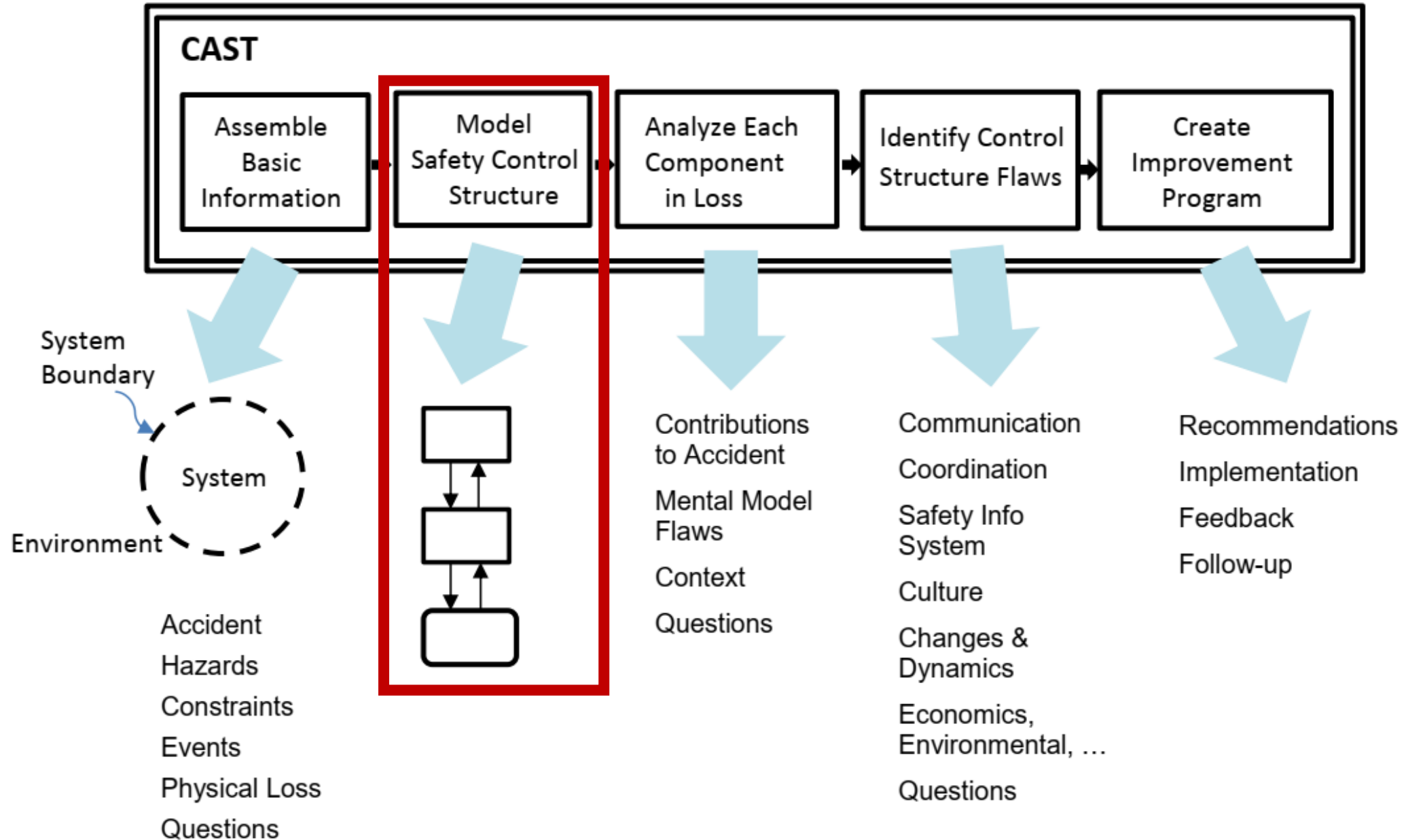
## System-level Hazards SH-1: Uncontrolled separation of the payload during flight

Hazard Safety Constraints (HSC)	Physical Controls and Equipment (PCE)	Inadequate Controls or Malfunctions (ICM)	Hazardous Contextual Factors (HCF)
<p><b>HSC-1.2:</b> Locking mechanisms must prevent premature or unintended activation of the separation system. [SH-1]</p>	<p><b>PCE-1.1:</b> Payload separation mechanism and its trigger system. [HSC-1.1, HSC-1.2]</p> <p><b>PCE-1.2:</b> Locking mechanisms for the payload separation system. [HSC-1.2]</p>	<p><b>ICM-1.1:</b> Locking mechanism did not engage during flight, leading to premature payload release. [PCE-1.1, PCE-1.2]</p> <p><b>ICM-1.3:</b> The existing locking system was not sufficiently verified pre-launch, leading to undetected vulnerabilities. [PCE-1.2]</p>	<p><b>HCF-1.1: Inadequate Procedures:</b> Pre-launch integration procedures and inspection of separation systems were inadequate for the current launcher with horizontal assembly (...) additional steps (for pressure release) were not part of the procedures and were not executed. [ICM-1.1]</p> <p><b>HCF-1.2: Time Pressures:</b> Constricted launch schedule reduced the time available for thorough checks of the payload separation mechanisms. [ICM-1.1, ICM-1.3]</p>
<p><b>HSC-1.4:</b> Torque verification systems must ensure separation system components are properly installed and tightened pre-launch. [SH-1]</p>	<p><b>PCE-1.4:</b> Torque monitoring tools for assembly processes. [HSC-1.4]</p>	<p><b>ICM-1.4:</b> Manual torque checks of separation belts were not executed, and existent inconsistencies were not verified during assembly. [PCE-1.4]</p>	<p><b>HCF-1.4 Pre-launch verifications:</b> Limited oversight of torque checks during critical assembly phases. [ICM-1.4]</p>



## H-6: Rocket Stages or Payload reaching Unsafe Areas due to Early Separation

Hazard Safety Constraints (HSC)	Physical Controls and Equipment (PCE)	Inadequate Controls or Malfunctions (ICM)	Hazardous Contextual Factors (HCF)
<p><b>HSC-6.1:</b> Flight safety limits must account for early separations and predicted flight loss scenarios to ensure that the safety zone remains valid for all mission scenarios. [SH-6]</p>	<p><b>PCE-6.1:</b> Safety zone modeling tools with contingency planning for early separations and loss scenarios. [HSC-6.1]</p>	<p><b>ICM-6.1:</b> Flight safety limits did not consider the potential loss scenarios with early separations, leading to risks in non-isolated areas. [PCE-6.1]</p>	<p><b>HCF-6.1: Simulation Limitations:</b> Pre-launch safety zone models did not incorporate scenarios for early separations or other flight malfunctions. [ICM-6.1]</p>
<p><b>HSC-6.2:</b> Rocket stages or payload capable of overreaching flight safety limits and exceeding public risk assessment must be equipped with flight termination systems. [SH-6]</p>	<p><b>PCE-6.2:</b> Flight termination systems installed on rocket stages and payloads. [HSC-6.2]</p>	<p><b>ICM-6.2:</b> Absence of flight termination systems led to uncontrolled S30 stage exceeding flight safety limits. [PCE-6.2]</p>	<p><b>HCF-6.2: FSS/FTS:</b> Flight termination systems <b>were excluded from stages and payload after several VSB-30 launch successes</b>, despite potential scenarios with the overreach of flight safety limits boundaries. [ICM-6.2]</p>



# Modeling the Safety Control Structure – Controller Responsibilities

**CT-1: Supervisor (DCTA) {4 CRs}**

**CT-2: Independent Review Board (IFI) {4 CRs}**

- **CR-2.1:** Conduct the Launch Center, Vehicle, and Payload Acceptance Review (TR), auditing readiness and compliance with technical and safety requirements.
- **CR-2.2:** Perform final Assembly Verification through inspections, test witnessing, and audits before system integration is approved.

**CT-3: Producers/Developers**

- **CT-3.1: Launch Vehicle Developers (IAE) {4 CRs}**
- **CT-3.2: Payload Developers (DLR, INPE/IEAV/ Universities) {3 CRs}**

**CT-4: Operators**

**CT-4.1: Launch Vehicle Operators (IAE Operators) {3 CRs}**

**CR-4.1.1:** Perform assembly procedures, ensuring proper integration of all vehicle components following approved protocols.

- **CT-4.2: Payload Operators (DLR/INPE Operators) {3 CRs}**

- **CR-4.2.1:** Perform assembly and integration of the payload following approved protocols.
- **CR-4.2.2:** Conduct final payload tests, including compatibility with the vehicle, and validate readiness for launch.

**CT-5: Launch Center**

- **CT-5.1: Launch Site Operations (CLA) {3 CRs}**

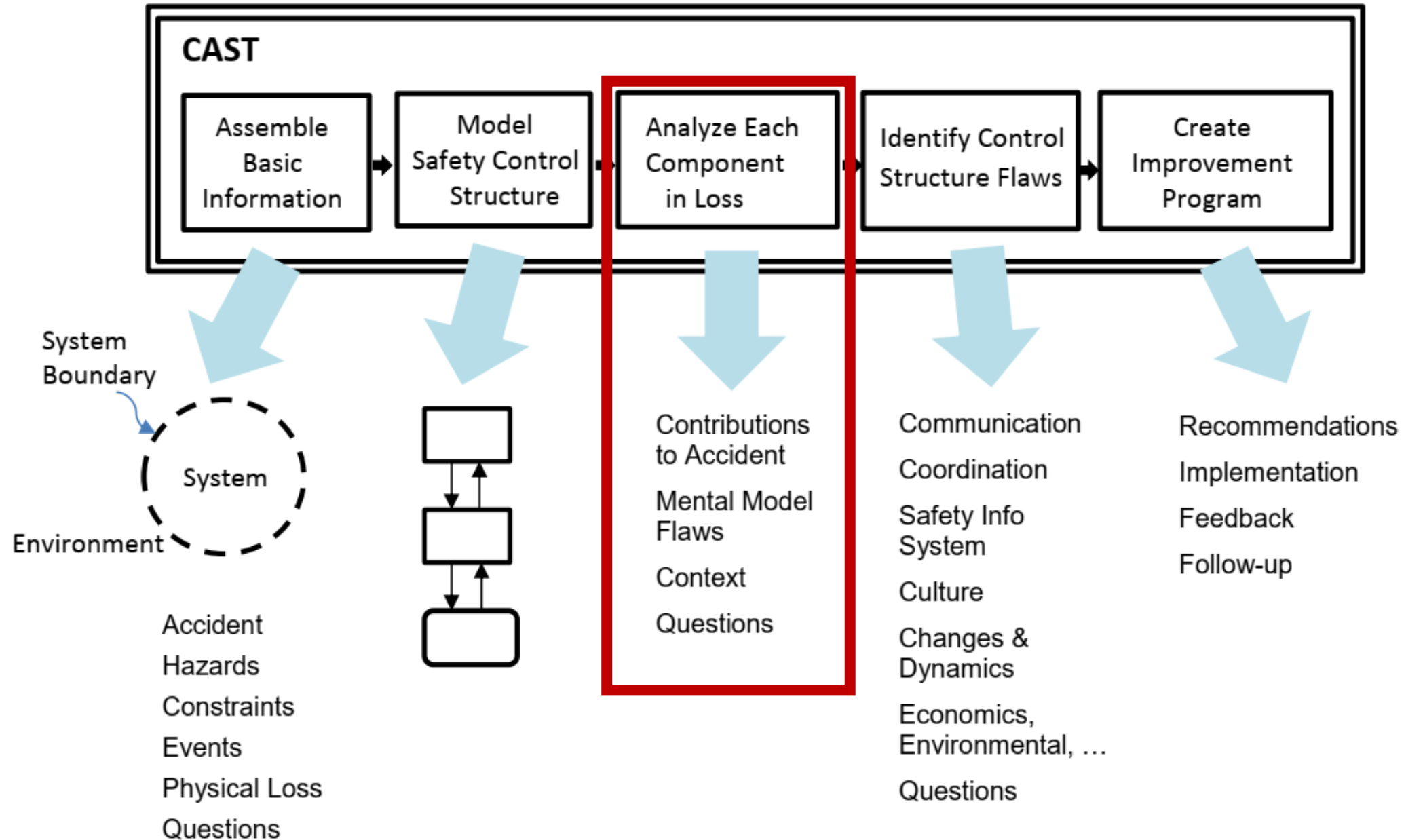
- **CR-5.1.2:** Provide real-time telemetry and radar tracking during launch and report deviations to the Supervisor and Operators.

- **CT-5.2: Remote Stations (CLBI) {2 CRs}**



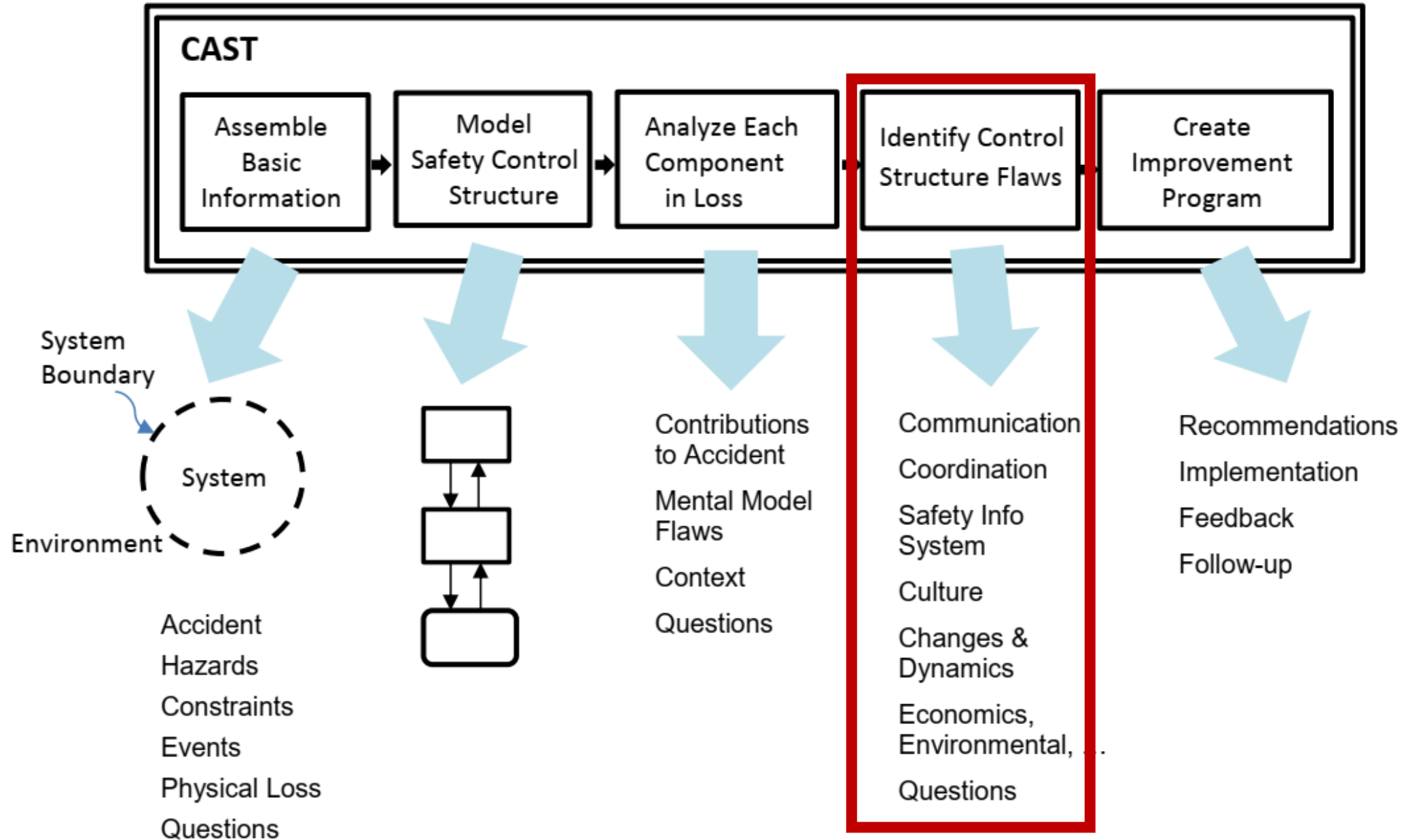
# Safety Control Structure

**RESTRICTED**





Controller Responsibilities (CR)	Why? (Contextual Factors Affecting the Unsafe Control)	Questions Raised
<p><b>CR-2.1:</b> Independent Review Board (IRB)'s Launch Center, Vehicle, and Payload Acceptance/Readiness Review.</p> <p><b>Component Responsibilities:</b></p> <ul style="list-style-type: none"> <li>- Ensure compliance and readiness of Launch Center, Vehicle and Payload with technical and safety standards.</li> <li>- Validate documentation and test results.</li> </ul> <p><b>Contribution to Hazardous State:</b> Approved the mission despite risks, including incomplete assembly reviews and unverified procedures for payload attachment mechanisms.</p>	<ul style="list-style-type: none"> <li>- <b>Incomplete Documentation:</b> Documentation lacked necessary details about final integration checks and tests, specifically for the payload separation system.</li> <li>- <b>Ambiguous Acceptance Criteria:</b> Criteria were inconsistently defined, allowing unverified risks to pass through.</li> <li>- <b>Schedule Pressures:</b> Tight deadlines led to rushed reviews, with inadequate time for detailed inspection.</li> <li>- <b>Ineffective Coordination:</b> Communication gaps between the IRB, Vehicle Operators, and Payload Operators led to unresolved risk ownership.</li> </ul>	<ul style="list-style-type: none"> <li>- Were all critical test and review documents submitted and validated before the acceptance review?</li> <li>- How were unresolved risks, such as payload attachment issues, tracked and resolved?</li> <li>- Were there sufficient resources to conduct an exhaustive acceptance review?</li> </ul>

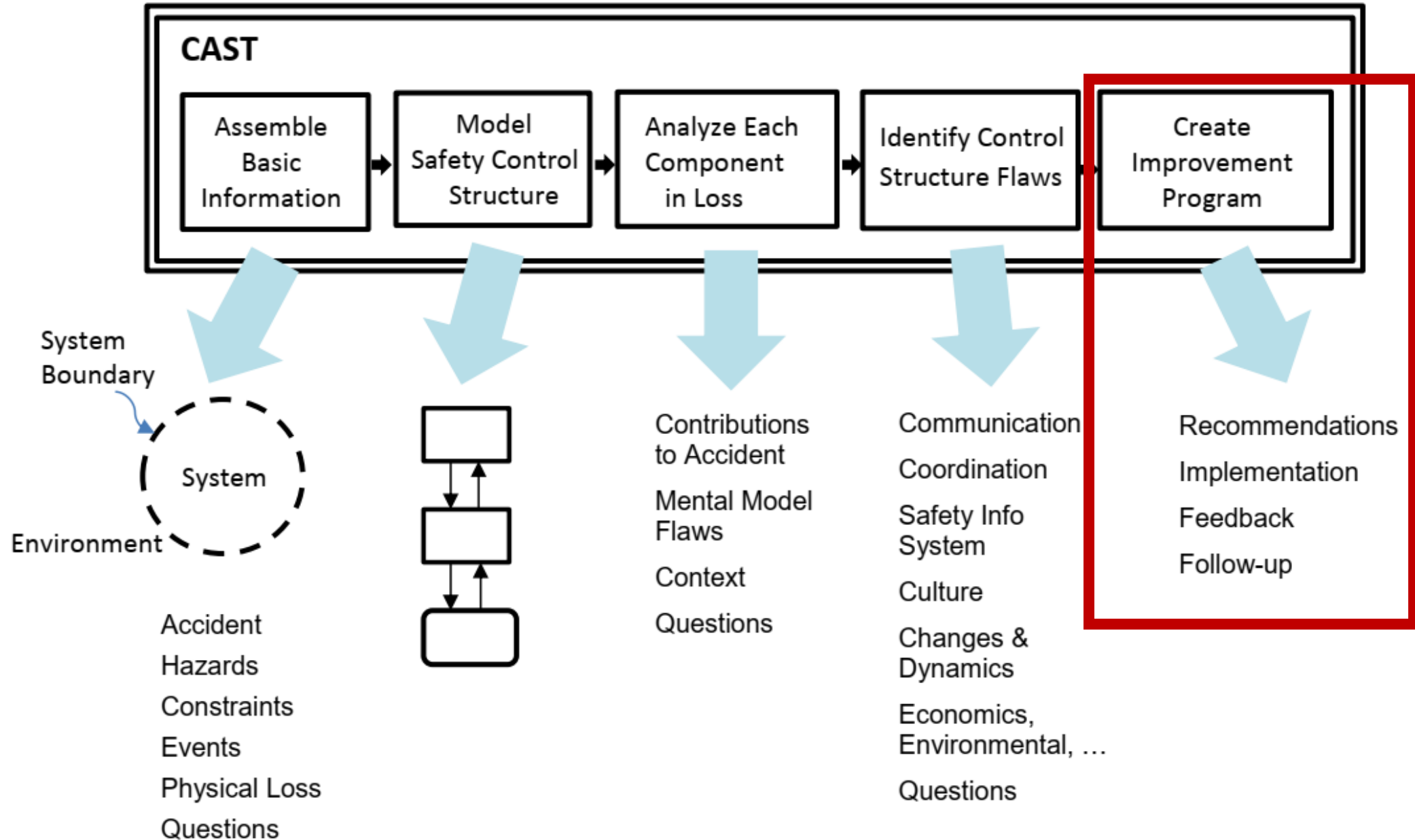




Safety Constraints	Unsafe Control Actions (UCA)	Process Models (PM)	Contextual Factors (CFC)
<p><b>CR-2.1: IRB's Launch Center, Vehicle, and Payload Acceptance/Readiness Review.</b></p> <p><b>SCR-2.1.1:</b> Ensure compliance of vehicle and payload with technical and safety standards.</p> <p><b>SCR-2.1.2:</b> Validate all assembly, integration, and test documentation.</p> <p><b>SCR-2.1.5:</b> Validate flame deflector system performance for varying thrust conditions before launch.</p> <p><b>Contribution to Hazardous State:</b> Approved the mission despite unresolved risks in the payload separation system and incomplete documentation.</p>	<p><b>UCA-2.1.3:</b> IRB did not demand additional testing or verification for high-risk subsystems and their procedures, particularly the second-stage <b>separation mechanism</b>. [SCR-2.1.3]</p> <p><b>UCA-2.1.5:</b> IRB approved rocket components with insufficient <b>thermal protection validation</b>. [SCR-2.1.1]</p> <p><b>UCA-2.1.6:</b> IRB, operators and supervisors did not verify the adequacy of the <b>flame deflector</b> design during the pre-launch approval or assembly phase. [SCR-2.1.5]</p>	<p><b>PM-2.1.3:</b> Underestimated the criticality of detailed integration checks and their impact on system safety. [UCA-2.1.3]</p> <p><b>PM-2.1.5:</b> Assumed existing documentation sufficiently validated thermal protection without additional independent review. [UCA-2.1.5]</p> <p><b>PM-2.1.6:</b> Assumed static deflector designs were sufficient without dynamic modeling of thrust conditions. [UCA-2.1.6]</p>	<p><b>CFC-2.1.1: Review Criteria:</b> Lack of standardized review criteria made it difficult to identify critical gaps in documentation and system readiness. [PM-2.1.1, PM-2.1.3]</p> <p><b>CFC-2.1.6: Awareness:</b> Limited expertise in evaluating new thermal protection materials during vehicle acceptance. [PM-2.1.5]</p> <p><b>CFC-2.1.7: Flame backflow:</b> Limited collaboration between IRB, structural and propulsion teams during flame deflector design. [PM-2.1.6]</p>



Safety Constraints	Unsafe Control Actions (UCA)	Process Models (PM)	Contextual Factors (CFC)
<p><b>CR-5.1.2: Provide real-time telemetry and radar tracking of all rocket stages and payload components during flight.</b></p> <p><b>SCR-5.1.2.1:</b> Ensure continuous telemetry and radar tracking of all vehicle components throughout flight.</p> <p><b>SCR-5.1.2.2:</b> Detect trajectory deviations or anomalies in real-time.</p> <p><b>Contribution to Hazardous State:</b> Loss of tracking for rocket stages after payload separation led to undetermined trajectories, reducing situational awareness and the ability to mitigate risks.</p>	<p><b>UCA-5.1.2.1:</b> GSE focused tracking solely on payload during nominal flight, neglecting rocket stages or early separations. [SCR-5.1.2.1]</p> <p><b>UCA-5.1.2.2:</b> GSE did not monitor all components of the vehicle and payload in real-time during critical flight phases. [SCR-5.1.2.1] [SCR-5.1.2.2]</p>	<p><b>PM-5.1.2.1:</b> Assumed tracking the payload alone would provide sufficient information for post-flight analysis. [UCA-5.1.2.1]</p> <p><b>PM-5.1.2.3:</b> Relied excessively on the payload's transponder without considering redundant tracking methods. [SCR-5.1.2.1]</p>	<p><b>CFC-5.1.2.1: System Design Limitation:</b> Tracking systems prioritized payload, neglecting other critical vehicle components. [PM-5.1.2.1]</p> <p><b>CFC-5.1.2.2: Procedural Deficiency:</b> Lack of clear protocols to manage real-time tracking of multiple objects with possible non-transponder-equipped components. [UCA-5.1.2.2] [PM-5.1.2.3]</p>





# CAST recommendations for further VSB-30 Operations

Hazard Safety Constraints (HSC)	Physical Controls and Equipment (PCE)	Inadequate Controls or Malfunctions (ICM)	Hazardous Contextual Factors (HCF)
<p><b>SH-4:</b> Ground systems interactions.</p> <p><b>HSC-4.5:</b> Flame deflector systems must prevent flame backflow, debris projection, and interference with the vehicle. [SH-4]</p>	<p><b>PCE-4.5:</b> Adaptive flame deflector systems designed to handle varying propulsion dynamics. [HSC-4.5]</p>	<p><b>ICM-4.5:</b> Inadequate flame deflector design led to flame backflow during liftoff. [PCE-4.5]</p>	<p><b>HCF-4.5 Flame Deflector:</b> Lack of dynamic simulations for modeling the interactions between the flame deflector and rocket exhaust. [ICM-4.5]</p>
Safety Constraints	Unsafe Control Actions (UCA)	Process Models (PM)	Contextual Factors (CFC)
<p><b>CR-2.1: IRB's Vehicle and Payload Acceptance Review.</b></p> <p><b>SCR-2.1.5:</b> Validate flame deflector system performance for varying thrust conditions before launch.</p>	<p><b>UCA-2.1.6:</b> IRB, operators and supervisors did not verify the adequacy of the <b>flame deflector</b> design during the pre-launch approval or assembly phase. [SCR-2.1.5]</p>	<p><b>PM-2.1.6:</b> Assumed static deflector designs were sufficient without dynamic modeling of thrust conditions. [UCA-2.1.6]</p>	<p><b>CFC-2.1.7: Flame backflow:</b> Limited collaboration between IRB, structural and propulsion teams during flame deflector design. [PM-2.1.6]</p>

**CAST R.63: Redesign flame deflectors for each launch configuration** to mitigate identified loss scenarios and improve performance under varying thrust conditions. Incorporate configurations to **minimize flame backflow risks** and ensure compatibility with the vehicle's propulsion dynamics. Implement verification and validation processes, including simulations and testing, to assess the effectiveness of redesigned deflectors before launch rail integration. [HSC-4.5, PCE-4.5, ICM-4.2, HCF-4.5, UCA-2.1.6, CFC-2.1.7]



DEPARTMENT OF AEROSPACE SCIENCE AND TECHNOLOGY  
Sovereignty in the form of Science and Technology

# Fault Tree Analysis (FTA)



INDUSTRIAL FOSTERING AND COORDINATION INSTITUTE  
*Wings for a strong industry*



**RESTRICTED**



# Fault Three Analysis (FTA)

**RESTRICTED**

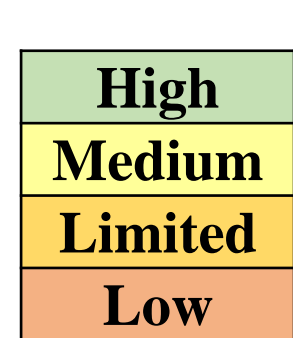


# Comparison of VSB-30 V11 CAST/FTA Recommendations

Main Area	CAST (66 Recommendations – 54 Topics)	FTA (25 Recommendations – 16 topics)
<b>Material Selection, Manufacturing, and Product Validation</b>	Covers <b>5 topics</b> , focusing on material testing, thermal protection, adhesives, advanced inspections, and supplier documentation.	<b>Same coverage but limited</b>
<b>Separation Systems</b>	Covers <b>5 topics</b> , addressing design review, validation, stress testing, procedural modifications, and integration process.	<b>1 topic</b>
<b>Flight Control and Stability</b>	Covers <b>14 topics</b> , including identification of flight anomalies, predictive modeling, telemetry/tracking upgrades, adaptive flight control, decision support for mission/safety, and fault tolerance.	<b>3 topics</b>
<b>FSS / FTS</b>	Covers <b>4 topics</b> , ensuring public risk criteria, debris trajectory safety, telemetry for termination, and safety envelopes.	<b>No coverage</b> on aspects of Flight Safety Systems or even Flight Termination Systems.
<b>Launch Platform &amp; Ground Support</b>	Covers <b>5 topics</b> , regarding pre-launch verification, separation tools and tools, deflector design, and transport procedures.	<b>3 topics</b>
<b>Operational &amp; Environmental Factors</b>	Covers <b>6 topics</b> , including weather modeling, failure scenario simulations, stress testing, safety zones, and mission validation.	<b>1 topic</b>
<b>Human &amp; Organizational Factors</b>	Covers <b>14 topics</b> , addressing safety reviews, anomaly response, training programs, independent review boards, communication improvements, incident escalation protocols, and risk assessments.	<b>3 topics</b>

# Criteria for the Comparison of Hazard Analysis Methods

Criteria	Definition
Coverage	The extensiveness and depth of the method in identifying and analyzing potential hazards.
Human Factors Analysis	How well the method considers human interactions, actions, errors, and behavior.
Risk Classification	The ability to assess and categorize risks by severity, likelihood, or consequences.
Systems Interactions	The ability to analyze interactions within and between systems.
Causality Analysis	The effectiveness in identifying causes of hazardous events.
Scenario Analysis	The ability to evaluate different potential scenarios and their impacts.
Requirements / Constraints	The ability to define and assign safety requirements or constraints for the specific accident, in order to prevent future incidents and accidents.



# CAST/FTA comparison summary for accident investigations

Criteria	CAST	FTA dedicated for Accident Investigation
Coverage	<b>High</b> – Extensive coverage by analyzing broader system behaviors, interactions, and organizational influences.	<b>Medium/Limited</b> – Focuses primarily on fault identification within predefined events.
Human Factors Analysis	<b>High</b> – Integrates human errors, interactions, and behaviors; considering technical and organizational factors.	<b>Low</b> – Not covered. Considers human factors only if explicitly included in the fault tree.
Accident Risk Classification	<b>Medium/Limited</b> – Avoids misleading prioritization; emphasizes systemic loss scenarios and their contributing factors rather than quantitative risk or severity ranking.	<b>Medium</b> – Uses numerical probability to assess failure likelihood and impact, limited by fault logic and without ranking severity.
Systems Interactions	<b>High</b> – Examines dependencies and interactions between subsystems and systems for a holistic safety view.	<b>Low</b> – Limited to faults within a single system; lacks intersystem analysis.
Causality Analysis	<b>High</b> – Explores causal factors by analyzing the system as a whole, including human and organizational factors.	<b>High/Medium</b> – Focuses on identifying root causes of events, limited to the possible failures.
Scenario Analysis	<b>High</b> – Evaluates diverse scenarios dynamically, addressing system-level behaviors and interdependencies.	<b>Medium/Limited</b> – Restricted to predefined failure paths and static fault trees.
Requirements/Constraints	<b>High</b> – Systematically derives and assigns constraints and safety requirements. The CAST Improvement Program also proposes implementation plans, feedback, and follow-up.	<b>Limited/Low</b> – Identifies possible system malfunctions based on fault identification, assigning only failure-related constraints.

## Conclusion

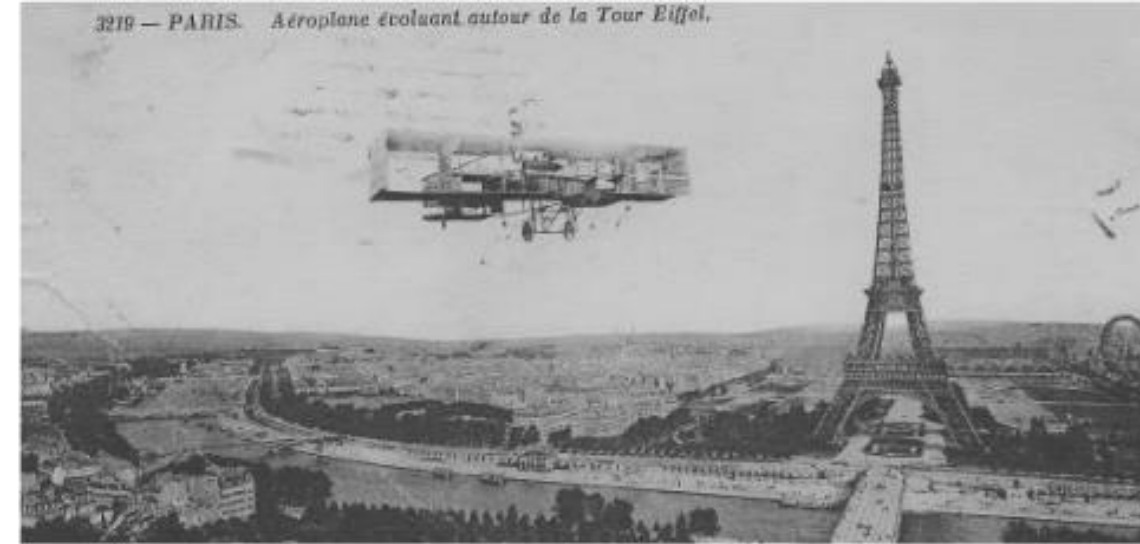
Comparing Accident Investigation Hazard Analysis Methods for a suborbital rocket launch operation.

### FTA (Fault Tree Analysis):

- **FTA is effective yet limited for structured fault identification and probability breakdown, focusing on identifying failures within a single system.** It lacks **systemic analysis** and does not capture broader interactions or human and organizational factors.

### CAST (Causal Analysis using System Theory):

- CAST stands out as a most comprehensive methodology for accident investigations due to its **holistic and systemic approach.** Unlike FTA, CAST analyzes interactions across the entire system, incorporating **human factors, operational behaviors, and organizational influences.** CAST avoids the rigid fault-prioritization of FTA, exploring interdependencies, dynamic scenarios, and deeper root causes, making it more suitable for modern aerospace operations.



“Invent is to imagine what nobody thought; it is to believe what no one has sworn;  
it is to risk what no one dared; is to accomplish what no one has tried.  
Invent is transcend.”

**Alberto Santos Dumont**