

HANBIT-Nano Launch Mishap

CAST application and comparison with the Official Investigation Report

Antonio Vinicius Diniz Merladet
Prof. Dr. Chiara Manfletti · Prof. Dr. Carlos Lahoz

September 2026

Technische Universität München

ITA

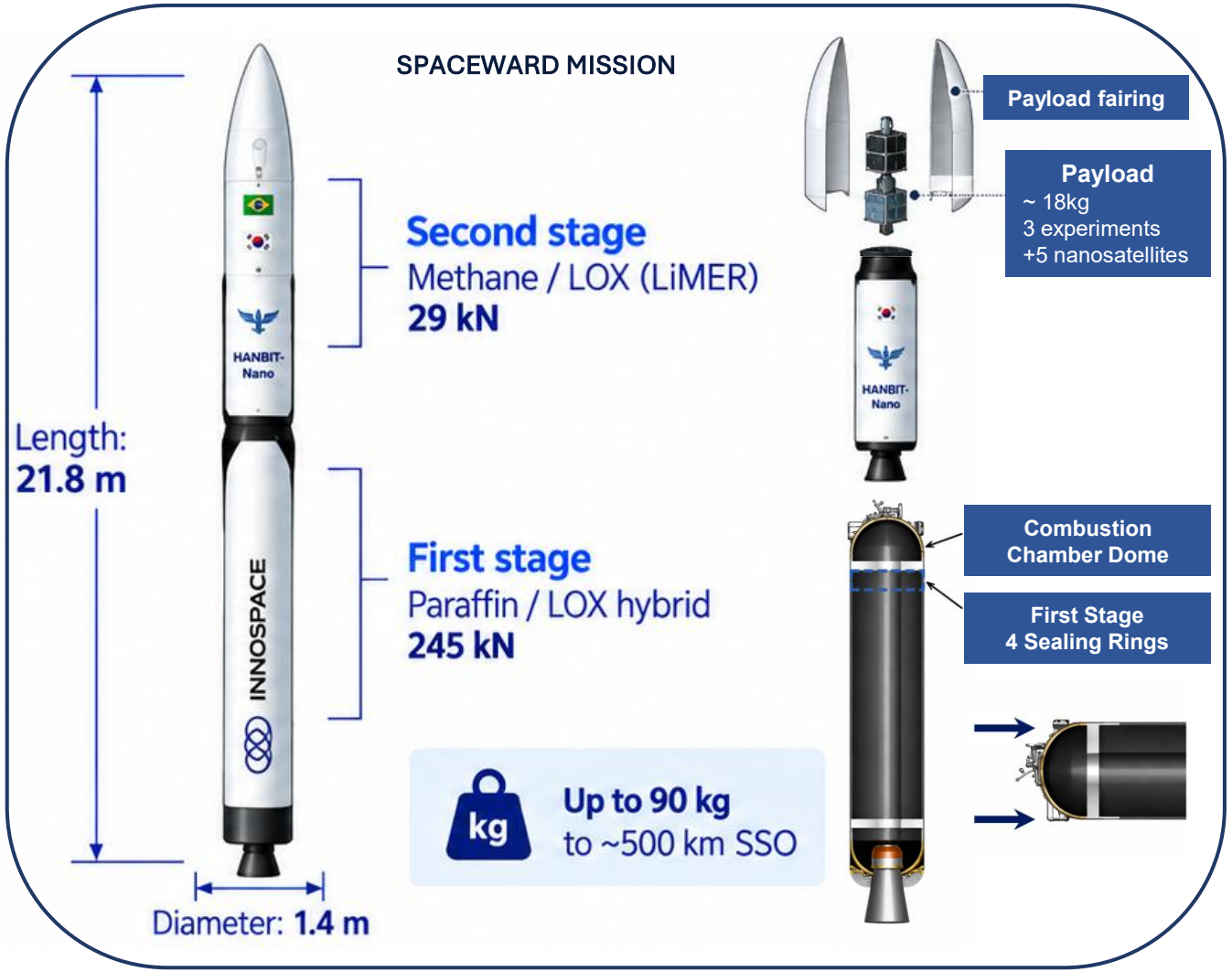
FORÇA AÉREA BRASILEIRA

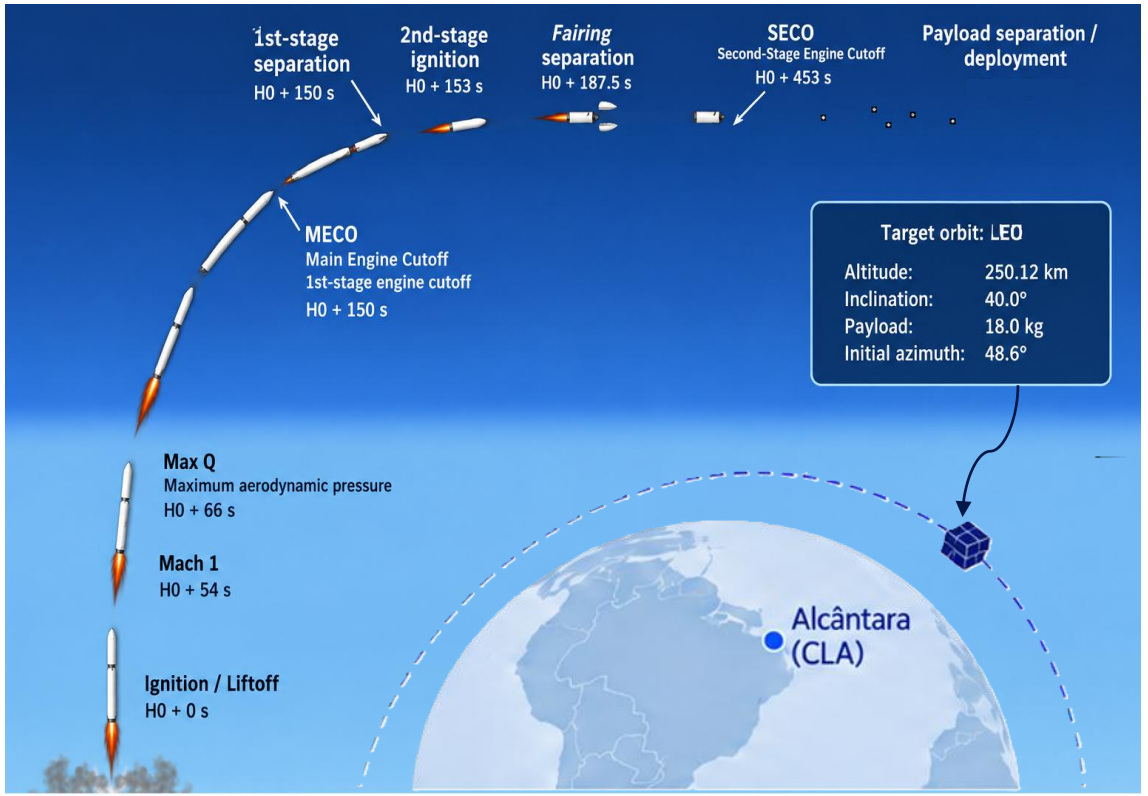


Source: INNOSPACE, Alcantara Space Center, 2025

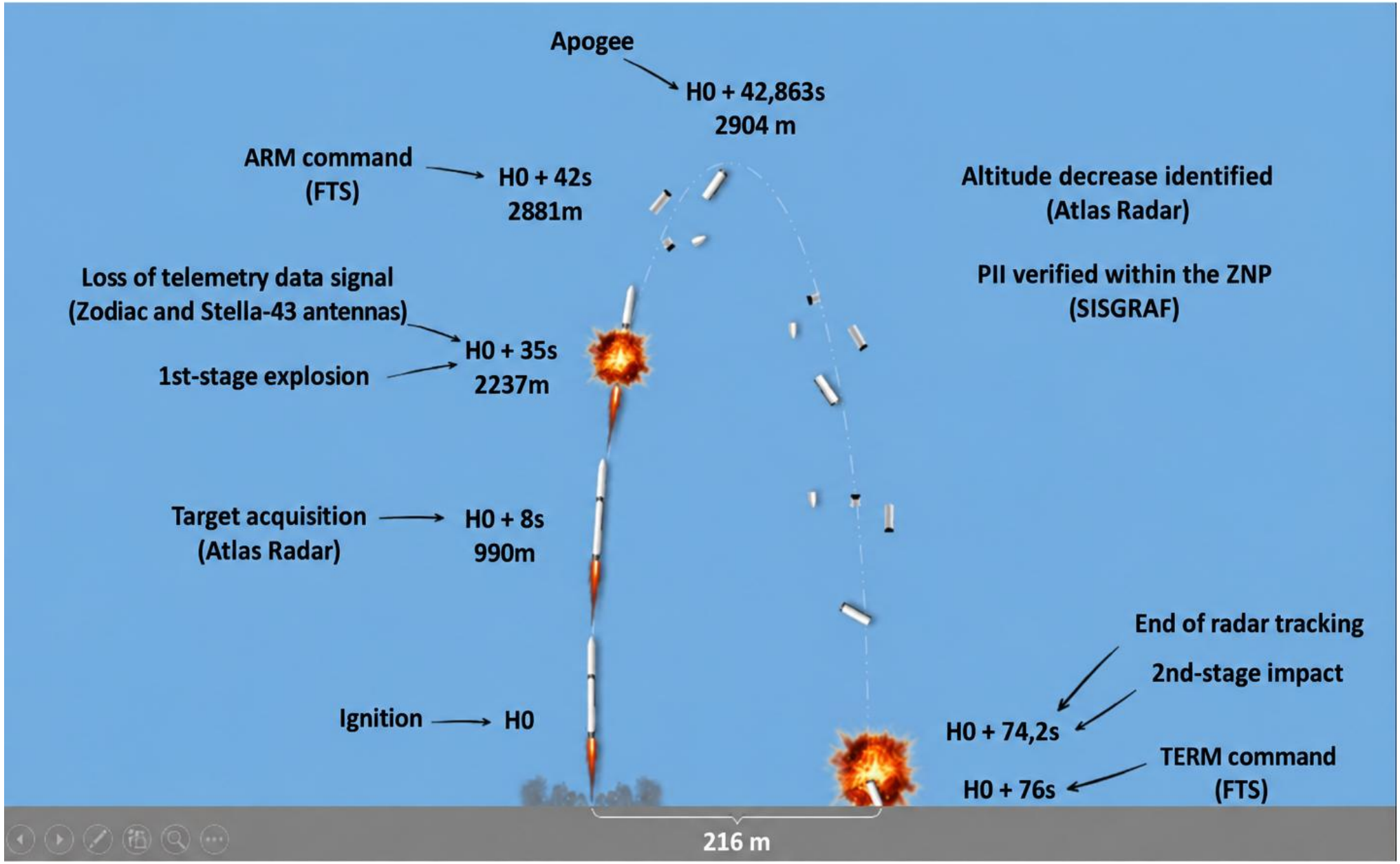
HANBIT-Nano and SPACEWARD Mission

Vehicle architecture and mission data from the official SIPAE Final Report





Source: adapted from SIPAE Final Report IE-001/CENIPA/2025/SIPAE



Source: adapted from SIPAE Final Report IE-001/CENIPA/2025/SIPAE

HANBIT-Nano Mishap Sequence

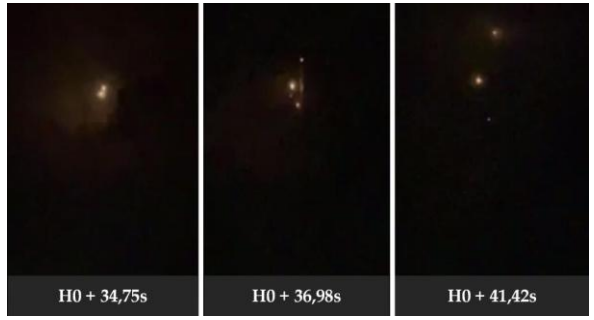
Key events from launch to ground impact (external observer imagery)



1. INITIAL NOMINAL ASCENT
H0 to ~30 s



2. CHAMBER RUPTURE AND FRAGMENTATION
H0 + 33.42 s



3. ASCENDING DEBRIS / BALLISTIC TRANSITION
H0 + 34 s to ~62 s



4. GROUND IMPACT AND EXPLOSION
H0 + 76.78 s

H0: 01:13:01 UTC
Liftoff
Initial ascent nominal

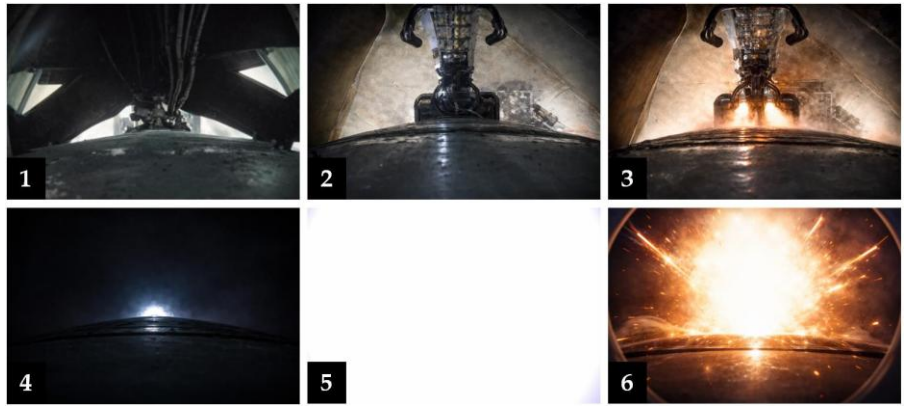
H0 + 33.42 s
First-stage combustion chamber rupture
~2.46 km altitude • vehicle fragmentation

H0 + 42.863 s
Apogee
2.904 km • ballistic descent begins

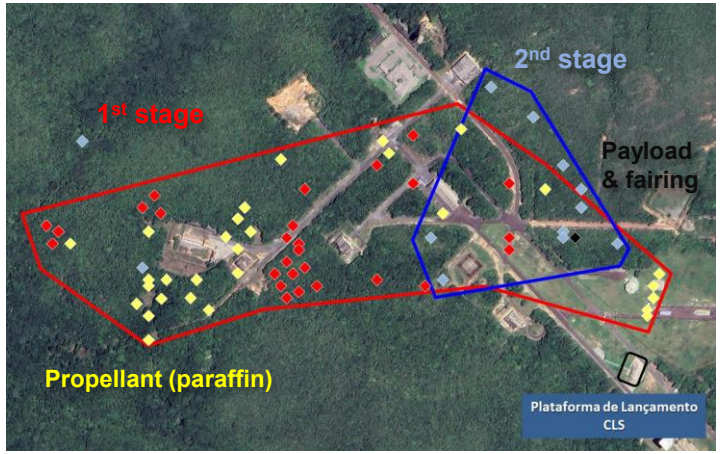
H0 + 76.78 s
Loaded second-stage impact and explosion
~216 m from launch pad • inside approved safety area

Outcome

- Vehicle and payloads lost
- Launch-site property damaged
- No injuries
- Debris remained within the designated safety area

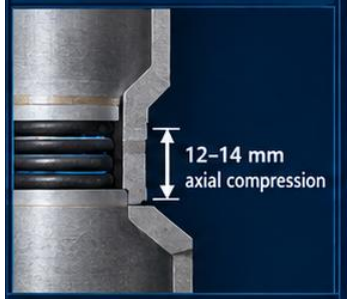


Source: adapted from SIPAE Final Report IE-001/CENIPA/2025/SIPAE



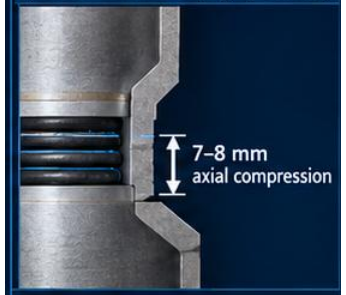


Initial assembly



Seal pack overcompressed during first assembly (12–14 mm).

Second assembly
(after forward chamber plug replacement)



Same sealing rings reused after forward chamber plug replacement, with lower compression during reassembly (7–8 mm).

1 Assembly and Compression (Images/Diagram from the Official Report)

Figure 57 – Positioning of the Metallic Dome

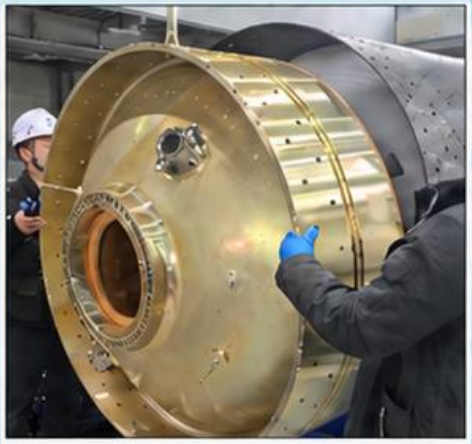
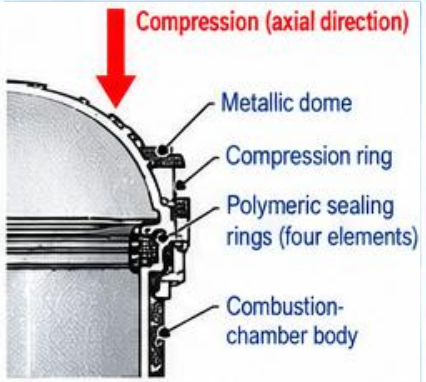


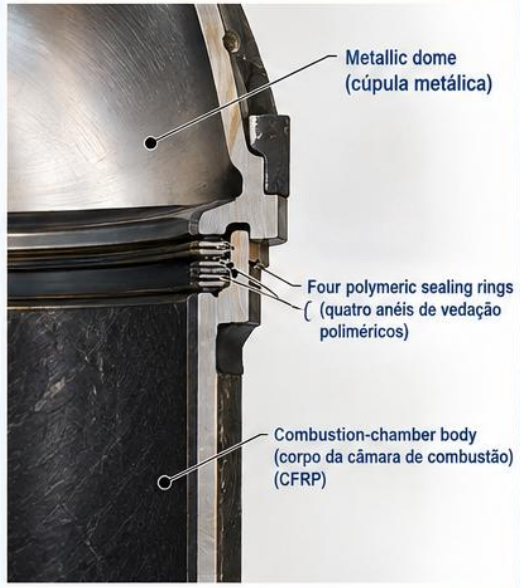
Figure 58 – Installation of the Metallic Compression Ring





Schematic representation of the direction of the axial load applied during assembly, responsible for compressing the polymeric sealing rings between the dome and the combustion-chamber body.

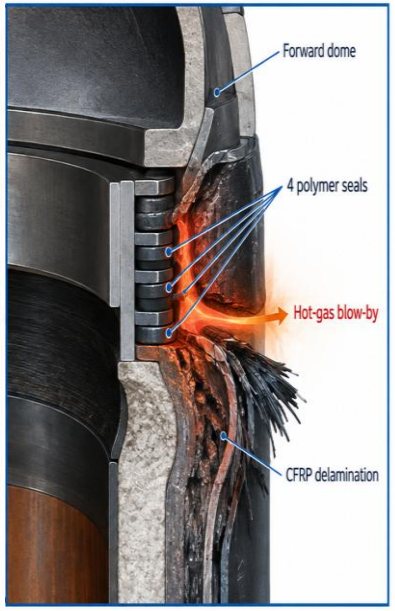
2 INTERNAL CONFIGURATION (cutaway view)



3 FAILURE SEQUENCE (simplified)



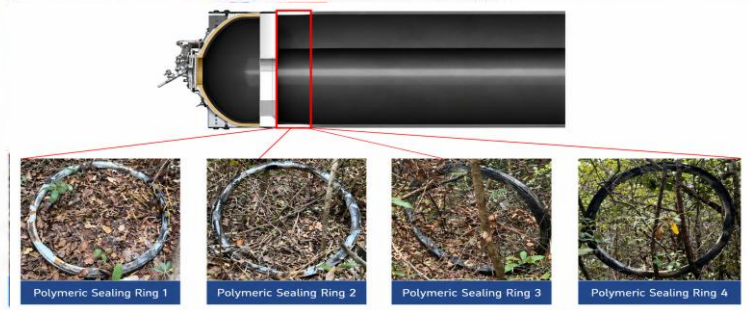
1. During assembly, the compression ring applies axial load, compressing the four polymeric sealing rings against the interface.
2. Loss of sealing integrity (local micro-clearance) allows hot gases to pass through the sealing region (directed leakage).
3. Hot gas impingement causes thermal degradation and erosion of the polymeric seals (grooves and surface damage).
4. Continued leakage leads to heating and structural failure of the forward region of the combustion chamber.



(Figure 34).

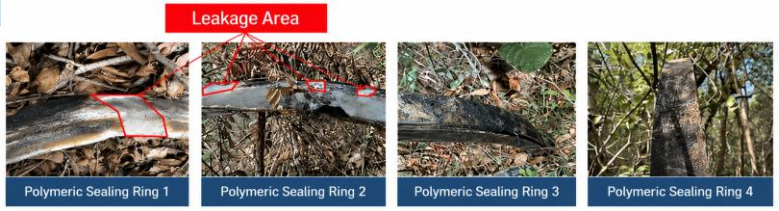
Evidence from the Official Report

Figure 35 – Recovered Polymeric Sealing Rings (from the First-Stage Combustion Chamber)



Four polymeric sealing rings recovered from the first-stage combustion chamber, showing surface discoloration, soot deposits, and signs of thermal degradation.

Figure 36 – Details of Sealing Rings 1 and 2 (from the First-Stage Combustion Chamber)



Details of sealing rings 1 and 2, showing surface discoloration, soot deposits, and signs of thermal degradation.

Figure 34 – Recovered Fracture in the Combustion-Chamber Dome (from the First-Stage Combustion Chamber)



Detail of the fracture region in the combustion-chamber dome, showing typical 'brooming' morphology, characterized by the projection of elongated carbon fibers, delamination between layers, and progressive rupture of the composite fibers.

Why CAST?

RESEARCH QUESTION

How did control and feedback activities allow a hazardous component state to pass through component change, assembly and launch readiness to flight, mishap and learning?

Analytical Procedure

Five CAST parts, moving from the physical loss and existing controls to system-wide improvement

1 PART 1

BASIC INFORMATION & PHYSICAL FACTORS

Define the analysis boundary.

Identify losses, hazards and system-level constraints.
Examine physical requirements, controls and inadequacies.

System boundary + physical loss model

2 PART 2

EXISTING SAFETY CONTROL STRUCTURE

Reconstruct controllers and subcontrollers.
Map control actions, feedback, communications and coordination.
Identify effective and weakened paths.

How safety was actually controlled

3 PART 3

COMPONENT ANALYSIS

Examine responsibilities, actions and decisions.
Reconstruct process models, local rationale and context.
Retain open questions without hindsight labeling.

Why local actions made sense at the time

4 PART 4

WHOLE-CONTROL-STRUCTURE ANALYSIS

Connect findings across controllers.
Examine coordination, safety information, change and organizational factors.
Derive systemic findings.

How interactions created or sustained risk

5 PART 5

RECOMMENDATIONS & EFFECTIVENESS FEEDBACK

Derive control changes and prevention measures.
Define closure criteria and implementation checks.
Add effectiveness feedback and reopening logic.

How the system should prevent recurrence

ONE TRACEABLE CHAIN

Losses & hazards → control structure → controller reasoning → systemic interactions → prevention controls

METHOD GUARDRAILS

Neutral action records

Realized actions are recorded as contributing actions/decisions, not labeled retrospectively as “unsafe control actions.”

Evidence ≠ inference

Factual claims, reconstructed process models, findings, and unresolved questions remain explicitly separated.

Comparison comes last

The official investigation comparison is performed only after the CAST outputs are fixed.

Analytical stage	Traceable outputs
Evidence foundation	27 factual claims (FC); 10 proximal events (PE); 11 CAST research questions (RQ-CAST); 13 evidence questions (Q); evidence-grading rule.
CAST Part 1: basic information and physical factors	5 losses (L); 7 hazards (H); 14 system-level constraints (SC); 9 physical system requirements (PSR); 11 physical/procedural control elements (PCE); 10 inadequate control functions (ICF); 31 hazard-specific safety constraints (HSC); 24 process controls (HPC); 29 inadequate controls/malfunctions (ICM); 23 hazardous contextual factors (HCF); 7 detailed hazard findings (DF-H).
CAST Part 2: existing hierarchical safety control structure	8 controller nodes (C); 46 controller responsibilities (CR); explicit actuator and sensor/feedback channels; 5 controlled processes (CP); 6 effective controls (PC); 8 weakened control/feedback paths (WP); 10 authorization and verification provisions (AVP-01–AVP-10) across 5 interfaces.
CAST Part 3: control-structure component analysis	8 controller analyses; 26 controller-level CAC records; 9 detailed responsibility analyses (F); 37 safety constraints to execute responsibilities (SCR); 24 detailed CAC refinements; 29 process-model mismatches (PM-M); 29 detailed contextual factors (CF); 10 open questions (F-Q); 9 findings (F).
CAST Part 4: overall system factors	11 interaction patterns (IP); 15 systemic findings (SF); 5 whole-control-structure factor checks.
CAST Part 5: recommendations and continual improvement	28 proposals (R-01–R-28); 6 loss/hazard-to-control pathways; effectiveness-feedback logic.
Comparison conducted after completion of the CAST analysis	Physical and contextual findings; 3 official contributing-factor categories; 7 official recommendations; 15 comparison-aspect records (CAR-01–CAR-15); complete SM-7 traceability crosswalks covering all 15 systemic findings and all 28 proposals.

Evidence Foundation and Traceability

A claim register and staged comparison constrain hindsight without turning missing evidence into facts

E — Established [E]

Explicitly documented in the event-evidence set or a controlling public rule.

May support factual findings and actions.

I — Inference [I]

System explanation consistent with established facts, but not explicitly stated or fully verified.

May support interpretation when clearly labeled and bounded.

Q — Question [Q]

Information is absent, incomplete, proprietary, or otherwise unresolved.

Defines evidence needs and confidence limits; never becomes an established fact.

EVIDENCE INVENTORY BEFORE CAST INTERPRETATION

These registers define what the analysis knows, what it asks, and what remains unresolved.

27 factual claims

FC-01-FC-27

FC-04: 12–14 mm first compression.
FC-07/08: Same rings reused; 7–8 mm after remount.

10 proximal event / control conditions

PE-1–PE-10

PE-1: Minimum-only criterion gave no mandatory stop.
PE-5: No public independent proof barrier after remount.

11 CAST research questions

RQ-CAST-1–11

RQ-CAST-1: Why did 12–14 mm not trigger a stop?
RQ-CAST-4: What independent assurance followed remount?

13 unresolved evidence questions

Q-1–Q-13

Q-4: What disposition followed the 12–14 mm result?
Q-6: Which tests verified the remounted boundary?

STAGED ANALYTICAL PATH

Public evidence & controlling rules → **Claim register + [E] / [I] / [Q]** → **CAST model, findings & proposals fixed** → **Official comparison as separate stage** → **Traceable crosswalk without causal scoring**

CAST Part 1: Losses, Hazards, and Safety Constraints

Start with unacceptable system states and constraints, not with a presumed root cause

5 LOSSES what must not happen

7 SYSTEM-LEVEL HAZARDS unsafe system states

14 SYSTEM-LEVEL CONSTRAINTS what the system must enforce

SYSTEM-LEVEL HAZARDS

- H-1: The launch vehicle loses pressure or hot-gas containment. [L-1, L-2, L-3]
- H-2: The launch vehicle loses structural integrity or departs from its controlled trajectory. [L-1, L-2, L-3]
- H-3: An energized stage or large fragment enters an area containing people, critical infrastructure, or environmentally sensitive assets. [L-2, L-3, L-5]
- H-4: The vehicle is prepared for launch or operated with an unverified safety-critical configuration. [L-1, L-2, L-3]
- H-5: A loaded stage retains hazardous propellant or impact energy during uncontrolled descent. [L-2, L-3, L-5]
- H-6: Safety-relevant evidence is unavailable for independent examination or corrective-action validation. [L-4]
- H-7: Nominal plume effects exceed accepted launch-site limits. [L-2, L-3, L-5]

ASSOCIATED POSSIBLE WORST-CASE LOSSES

L-1: Loss of the launch vehicle, payloads, or mission objectives.
L-2: Damage to launch-site property or critical infrastructure.
L-3: Loss of life or serious injury to personnel or the public.
L-4: Reduced ability to determine causes, validate corrective actions, and prevent recurrence.
L-5: Environmental loss.

REPRESENTATIVE TRACE CHAINS

H-4 Verified launch configuration

SC-7: No safety-critical configuration shall be released after change, remount, repair or assembly-history deviation until its integrity is independently verified against the current as-built/as-modified state.

H-5 Loaded-stage consequence

SC-9: Flight-safety intervention logic shall be capable of reducing total expected harm before an uncontrolled loaded stage or large fragment reaches the ground.

STAMP / CAST principle: hazards are system states, not causes, failed parts, or blame labels.

CAST Part 1: Physical Controls and Hazard-Specific Analysis

Detailed worksheets connect requirements and controls to inadequacies, context, and hazard findings

9	PHYSICAL REQUIREMENTS PSR-1–PSR-9
11	CONTROL ELEMENTS PCE-1–PCE-11
10	INADEQUATE FUNCTIONS ICF-1–ICF-10

DETAILED HAZARD WORKSHEETS

31 HSC	24 HPC	29 ICM	23 HCF	7 DF-H

EXAMPLE A — H-1 PRESSURE / HOT-GAS CONTAINMENT

Physical-control layer

PSR-2	Validated minimum/maximum compression, recovery, condition, reuse and disposition criteria.
PCE-3	Assembly/metrology recorded the states, but the first value was not connected to an upper-limit stop.
ICF-1	No validated upper compression limit or mandatory discard state.

Hazard-specific worksheet

HSC-1.1	Bound ring compression by validated minimum and maximum limits.
HPC-1.3	Independent hold point before pressure-boundary closure.
ICM-1.2	No mandatory stop for the 12–14 mm entry.
HCF-1.3	A later in-range value could appear compliant.

DF-H1: containment was lost after an indeterminate seal state was released; microscopic initiation remains evidence-bounded.

EXAMPLE B — H-4 VERIFIED LAUNCH CONFIGURATION

Selected worksheet chain

HSC-4.1	Reopen every affected readiness, acceptance, authorization and release decision after material change.
HPC-4.2	Independent assurance hold points and sign-offs.
ICM-4.4	The public record does not demonstrate one final synchronized baseline.
HCF-4.2	Late information reduced the available review time.
DF-H4	The as-modified pressure-boundary state was not supported by publicly demonstrable configuration-specific independent proof and one common release baseline.

Hazard worksheets convert broad constraints into testable control conditions.

CAST Part 2: The Safety Control Structure

Identify focal control actions and controlled processes: the mishap crossed technical, organizational, operational, and learning control loops.

HCS BASIS 8 controller nodes · 46 responsibilities · 5 controlled processes
INTERFACES ACT/SNS channels · 10 AVP across 5 interfaces · e.g., AVP-03 material-change reopening

Controlled Processes

CP-1

Pressure-boundary configuration & integrity

What state is the chamber / seal actually in?

→

CP-2

Campaign integration, readiness & cumulative assurance

What evidence remains valid after change?

→

CP-3

Authorization, acceptance & launch-release state

Are all release decisions using the same current baseline?

→

CP-4

Powered flight, trajectory monitoring & consequence control

What hazardous energy state remains after failure?

→

CP-5

Post-accident evidence, corrective-action closure & learning

Can the system confirm causes and verify prevention?

CAST ROLE **Explain the control path across the sociotechnical system.**
Not replace the official physical mechanism or convert unresolved evidence into allegations.

CAST Part 2: HCS Construction and Release Interfaces

The HCS is built from controller responsibilities, control/feedback channels, and distinct release decisions

8	46	10	5	ACT ↔ SNS
CONTROLLER NODES	RECONSTRUCTED RESPONSIBILITIES	AVP PROVISIONS	RELEASE INTERFACES	actions + feedback

CONTROLLER NODES REPRESENTED IN THE HCS

C-1	AEB licensing, authorization & supervision
C-2	COMAER / DCTA / CLA governance, waivers & chronology release
C-3	INNOSPACE mission & safety management
C-3.1	Propulsion Engineering / QA / GSO
C-3.2	Assembly & Integration
C-4	COMAER / IFI / CLA prelaunch acceptance
C-5	CLA real-time flight safety / OSTV / FTS
C-8	SIPAE / CENIPA investigation & learning

REPRESENTATIVE RESPONSIBILITY + INTERFACE EXAMPLES

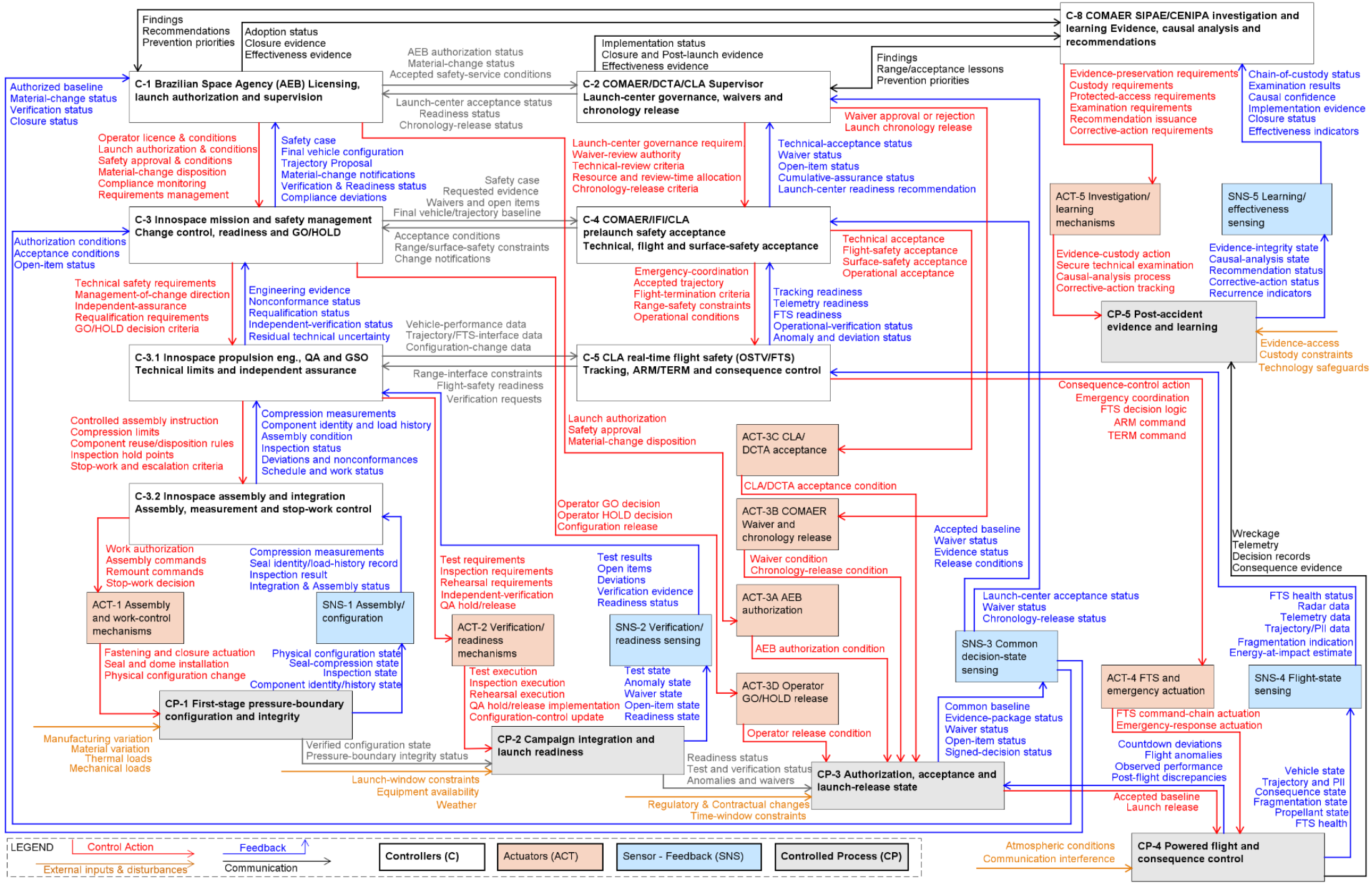
C-3.2	Preserve component identity/load history; stop work and escalate when the state is out-of-limit or indeterminate.
C-5	Maintain tracking/telemetry and consequence-state feedback; apply independent ARM/TERM authority using validated criteria.
C-8	Preserve evidence, protected technical access, independent examination, and effectiveness feedback.

AVP-03 — MATERIAL-CHANGE REOPENING

Classify safety-significant changes and reopen every affected authorization, acceptance and verification decision.

ACT/SNS example HOLD / RELEASE action ↔ current configuration and verification-status feedback

Part 2 retains 6 effective controls and identifies 8 weakened control / feedback paths.


C-8 COMAER SIPAE/CENIPA investigation and learning Evidence, causal analysis and recommendations
Findings
Recommendations
Prevention priorities
Adoption status
Closure evidence
Effectiveness evidence
C-1 Brazilian Space Agency (AEB) Licensing, launch authorization and supervision
Authorized baseline
Material-change status
Verification status
Closure status
AEB authorization status
Material-change status
Accepted safety-service conditions
Launch-center acceptance status
Readiness status
Chronology-release status
C-2 COMAER/DCTA/CLA Supervisor Launch-center governance, waivers and chronology release
Implementation status
Closure and Post-launch evidence
Effectiveness evidence
Findings
Range/acceptance lessons
Prevention priorities
Waiver approval or rejection
Launch chronology release
Evidence-preservation requirements
Custody requirements
Protected-access requirements
Examination requirements
Recommendation issuance
Corrective-action requirements
Chain-of-custody status
Examination results
Causal confidence
Implementation evidence
Closure status
Effectiveness indicators
Operator licence & conditions
Launch authorization & conditions
Safety approval & conditions
Material-change disposition
Compliance monitoring
Requirements management
Safety case
Final vehicle configuration
Trajectory Proposal
Material-change notifications
Verification & Readiness status
Compliance deviations
Launch-center governance requirem
Waiver-review authority
Technical-review criteria
Resource and review-time allocation
Chronology-release criteria
Technical-acceptance status
Waiver status
Open-item status
Cumulative-assurance status
Launch-center readiness recommendation
ACT-5 Investigation/ learning mechanisms
SNS-5 Learning/ effectiveness sensing
Safety case
Requested evidence
Waivers and open items
Final vehicle/trajectory baseline
C-3 Innospace mission and safety management Change control, readiness and GO/HOLD
Acceptance conditions
Range/surface-safety constraints
Change notifications
C-4 COMAER/IFI/CLA prelaunch safety acceptance Technical, flight and surface-safety acceptance
Authorization conditions
Acceptance conditions
Open-item status
Technical acceptance
Flight-safety acceptance
Surface-safety acceptance
Operational acceptance
Evidence-custody action
Secure technical examination
Causal-analysis process
Corrective-action tracking
Evidence-integrity state
Causal-analysis state
Recommendation status
Corrective-action status
Recurrence indicators
Technical safety requirements
Management-of-change direction
Independent-assurance
Requalification requirements
GO/HOLD decision criteria
Engineering evidence
Nonconformance status
Requalification status
Independent-verification status
Residual technical uncertainty
Emergency-coordination
Accepted trajectory
Flight-termination criteria
Range-safety constraints
Operational conditions
Tracking readiness
Telemetry readiness
FTS readiness
Operational-verification status
Anomaly and deviation status
CP-5 Post-accident evidence and learning
Evidence-access
Custody constraints
Technology safeguards
Vehicle-performance data
Trajectory/FTS-interface data
Configuration-change data
C-3.1 Innospace propulsion eng., QA and GSO Technical limits and independent assurance
C-5 CLA real-time flight safety (OSTV/FTS) Tracking, ARM/TERM and consequence control
Range-interface constraints
Flight-safety readiness
Verification requests
Consequence-control action
Emergency coordination
FTS decision logic
ARM command
TERM command
Launch authorization
Safety approval
Material-change disposition
ACT-3C CLA/ DCTA acceptance
Controlled assembly instruction
Compression limits
Component reuse/disposition rules
Inspection hold points
Stop-work and escalation criteria
Compression measurements
Component identity and load history
Assembly condition
Inspection status
Deviations and nonconformances
Schedule and work status
CLA/DCTA acceptance condition
C-3.2 Innospace assembly and integration Assembly, measurement and stop-work control
Operator GO decision
Operator HOLD decision
Configuration release
ACT-3B COMAER Waiver and chronology release
Accepted baseline
Waiver status
Evidence status
Release conditions
Waiver condition
Chronology-release condition
Wreckage
Telemetry
Decision records
Consequence evidence
Work authorization
Assembly commands
Remount commands
Stop-work decision
Compression measurements
Seal identity/load-history record
Inspection result
Integration & Assembly status
Test requirements
Inspection requirements
Rehearsal requirements
Independent-verification
QA hold/release
Test results
Open items
Deviations
Verification evidence
Readiness status
ACT-3A AEB authorization
Launch-center acceptance status
Waiver status
Chronology-release status
FTS health status
Radar data
Telemetry data
Trajectory/PII data
Fragmentation indication
Energy-at-impact estimate
ACT-1 Assembly and work-control mechanisms
SNS-1 Assembly/ configuration
ACT-2 Verification/ readiness mechanisms
SNS-2 Verification/ readiness sensing
AEB authorization condition
SNS-3 Common decision-state sensing
ACT-4 FTS and emergency actuation
SNS-4 Flight-state sensing
Fastening and closure actuation
Seal and dome installation
Physical configuration change
Physical configuration state
Seal-compression state
Inspection state
Component identity/history state
Test execution
Inspection execution
Rehearsal execution
QA hold/release implementation
Configuration-control update
Test state
Anomaly state
Waiver state
Open-item state
Readiness state
ACT-3D Operator GO/HOLD release
Operator release condition
Common baseline
Evidence-package status
Waiver status
Open-item status
Signed-decision status
FTS command-chain actuation
Emergency-response actuation
CP-1 First-stage pressure-boundary configuration and integrity
Manufacturing variation
Material variation
Thermal loads
Mechanical loads
Verified configuration state
Pressure-boundary integrity status
CP-2 Campaign integration and launch readiness
Readiness status
Test and verification status
Anomalies and waivers
CP-3 Authorization, acceptance and launch-release state
Countdown deviations
Flight anomalies
Observed performance
Post-flight discrepancies
Vehicle state
Trajectory and PII
Consequence state
Fragmentation state
Propellant state
FTS health
Launch-window constraints
Equipment availability
Weather
Regulatory & Contractual changes
Time-window constraints
Accepted baseline
Launch release
Atmospheric conditions
Communication interference
CP-4 Powered flight and consequence control
LEGEND
Control Action
External inputs & disturbances
Feedback
Communication
Controllers (C)
Actuators (ACT)
Sensor - Feedback (SNS)
Controlled Process (CP)

What Worked and Where Control Weakened

CAST retains successful controls; the mishap is not a narrative that the entire system failed

EFFECTIVE CONTROLS RETAINED

✓ **Meteorology & electrical-field monitoring**	conditions tracked and incorporated into operations
✓ **Radar, telemetry & communications**	multiple tracking and information channels functioned
✓ **Protected-zone & emergency-response design**	debris remained inside the designated safety area
✓ **FTS validation & real-time authority**	command chain validated; OSTV authority did not depend on operator concurrence
✓ **Post-impact emergency & evidence response**	contingency actions followed the ground explosion
✓ **Personnel qualification & medical fitness**	operators and coordinators were appropriately qualified

WEAKENED CONTROL / FEEDBACK PATHS

Component state & engineering

- ! **WP-1 Requirement → assembly**
- ! **WP-2 Assembly → engineering / QA**
- ! **WP-3 Component history → readiness**

Change & distributed assurance

- ! **WP-4 Change → system safety**
- ! **WP-5 Independent assurance → management**
- ! **WP-6 Operator changes → CLA / AEB**

Consequence control

- ! **WP-7 Trajectory / propellant state → OSTV**

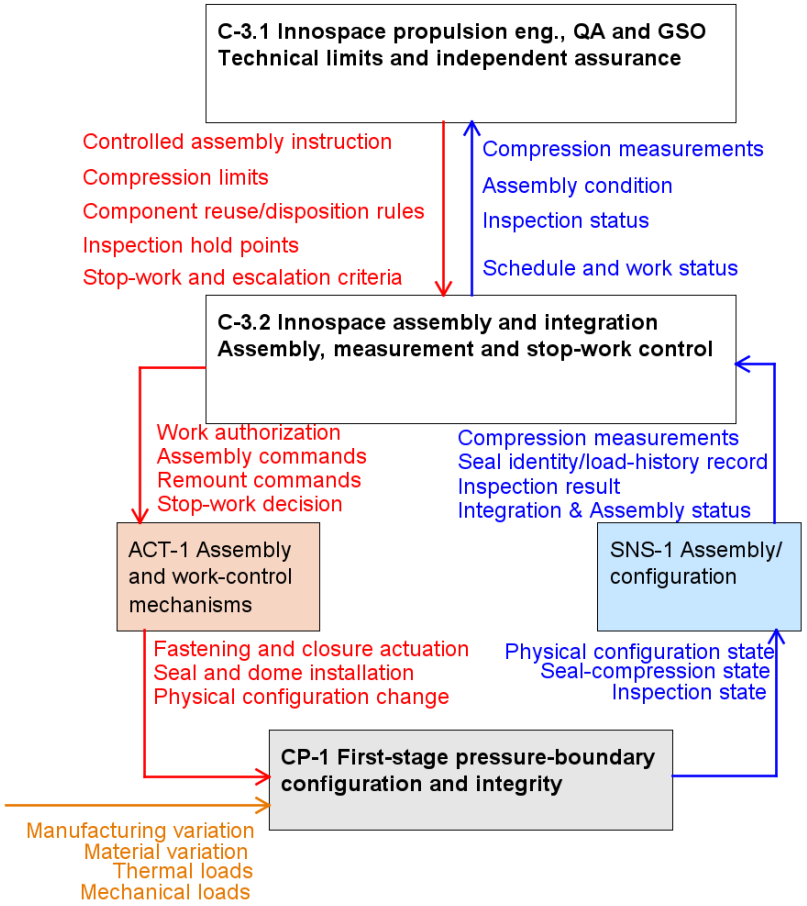
Learning

- ! **WP-8 Wreckage → SIPAE learning**

Interpretation: successful controls reduced consequences; weakened paths explain how safety-relevant state and feedback lost decision value across interfaces.

Control-structure component analysis

One Controller Interface in Detail C-3.1 Propulsion Engineering / QA / GSO and C-3.2 Assembly & Integration



C-3.1 RESPONSIBILITIES RELEVANT TO THIS INTERFACE

- Define validated pressure-boundary and seal acceptance limits.
- Interpret measurements against material and assembly history.
- Disposition nonconformances and unknown component states.
- Verify configuration-specific integrity after remount.
- Maintain independent QA / GSO hold points.
- Provide current technical evidence to mission management and acceptance authorities.

OBSERVED / DOCUMENTED CONTEXT

- **E** First assembly: 12–14 mm ring compression.
- **E** Instruction: minimum >7 mm; no reproduced upper limit.
- **E** Stronger dome installed; same rings reused.
- **E** Second assembly: 7–8 mm and formally compliant.
- **Q** Public record does not reproduce an independent representative post-remount validation barrier.

PROCESS-MODEL / CONTROL INTERPRETATION

A locally compliant final geometry can represent “acceptable now” while inadequate to preserve “what this component has already experienced.”

CAST implication Component state must carry load / reuse history, and remount must automatically reopen configuration-specific integrity evidence and independent release.

PART 3 INVENTORY 8 analyses · 26 CAC · 9 F · 37 SCR · 24 CAC refinements · 29 PM-M · 29 CF · 10 F-Q · 9 findings

Controller analysis asks what information and process model shaped a locally reasonable action: not who to blame after the outcome is known.

CAST Part 4: From Local Decisions to System Interactions

The component analyses converge on interaction patterns rather than a single root cause

26 controller-level CAC records

11 interaction patterns

15 systemic findings

11 CROSS-CONTROLLER INTERACTION PATTERNS

- **IP-1** Measurement without control semantics
- **IP-2** Safety improvement with interface migration
- **IP-3** Local compliance masking degradation
- **IP-4** Assurance compression across organizations
- **IP-5** Fragmented design, range and authorization control
- **IP-6** Successful corridor control with residual consequence
- **IP-7** Protection versus learning tension
- **IP-8** Open-loop corrective action
- **IP-9** Nominal operation with secondary consequence
- **IP-10** Multiple valid decisions without a common state
- **IP-11** Verification discontinuity across the lifecycle

WHOLE-STRUCTURE 5 factor checks
coordination · safety information · culture · change/dynamics · economic/environmental context

15 SYSTEMIC FINDINGS

1 Component-state
SF-1, SF-2, SF-3, SF-4, SF-5, SF-10

2 Readiness & distributed assurance
SF-6, SF-7, SF-12

3 Authorization & verification continuity
SF-8, SF-14, SF-15

4 Consequence & launch-site control
SF-9, SF-13

5 Evidence & organizational learning
SF-11

Systemic path: control process, component history, reassessment, release-state continuity, consequence variables, and learning were incomplete across interfaces.

CAST Result: Change-Triggered Requalification

A safety-motivated hardware improvement created a new configuration that had to be re-proven as a system

CAST findings SF-3 / SF-5 · interaction IP-2 **Improving one margin can invalidate assumptions elsewhere.** The relevant unit of assurance is the changed system, not only the changed part.

LOCAL CHANGE

Stronger dome

Installed to increase structural margin after the earlier chamber damage.

Locally rational safety improvement

WHAT THE CHANGE ALSO DID

Pressure boundary reopened
physical interface changed

—

Same rings reused
component history carried forward

—

Assurance basis shifted
prior proof no longer fully representative

The public record does not reproduce a formal system-level reassessment or independent representative post-remount validation as a release barrier.

CHANGE-TRIGGERED CONTROL

Reassess	affected hazards and interfaces
Reopen	verification / acceptance evidence
Requalify	the actual as-modified pressure boundary
Independent	closure before readiness and release

SC-4 formalizes this system-level change trigger.

Not the claim: **“the stronger dome caused the mishap”**

CAST claim: **the change migrated assurance obligations across interfaces**

TRANSFERABLE LESSON **A safety-motivated change is still a configuration change: re-prove the changed system, not only the replacement part.**

CAST Result: Distributed Acceptance and Launch Release

Independent barriers only remain effective when they reference one current system state

SF-8 · SF-14 · SF-15 **Several valid decisions can still diverge if their accepted baselines diverge.** Interface finding, not regulatory noncompliance.

COMMON ACCEPTANCE BASELINE

VEHICLE | TRAJECTORY | WAIVERS | OPEN ITEMS | RISK | VERIFICATION EVIDENCE

One controlled state consumed by distinct authorities; material change reopens every affected decision.

1 OPERATOR INTERNAL GO

Final as-built / as-modified readiness

INNOSPACE

2 AEB AUTHORIZATION

Mission authorization + safety approval

AEB

3 CLA / DCTA ACCEPTANCE

Technical, flight & surface-safety acceptance

CLA / DCTA

4 CHRONOLOGY RELEASE

Release against current accepted state

Launch-center authority

MATERIAL CHANGE
reopen affected decisions

automatic reopening →

EVIDENCE DISCIPLINE

[E] Distinct release functions and formal waivers are documented.

[Q] The public record does not reproduce one common final cross-authority baseline or the final chronology-release basis.

These absences do not establish noncompliance.

TRANSFERABLE LESSON **Independent decision authority works only when every barrier uses the same current evidence state.**

CAST Result: Evidence Access and Organizational Learning

Post-mishap learning determines causal confidence and whether corrective actions actually reduce recurrence

SF-11 / SF-12 · IP-7 / IP-8 **Evidence preservation is part of the safety-control loop.** not an administrative afterthought

1. **OCCURRENCE** — physical + digital evidence
2. **PRESERVE** — custody · telemetry · configuration records
3. **EXAMINE** — secure independent laboratory / expert access
4. **CONFIDENCE** — confirm, reject, or bound causal hypotheses
5. **CORRECT** — translate findings into control changes
6. **VERIFY** — closure evidence · independent review · recurrence checks

OBSERVED LIMITATION IN THIS MISHAP

SIPAE did not retain rocket components for laboratory analysis because of project intellectual-property restrictions; no microscopic material examination of the launcher wreckage was performed.

CAST RESPONSE

Prearrange protected custody, secure laboratory access, cleared experts, retained raw data, and disclosure controls before an occurrence.
Proprietary / security safeguards remain legitimate constraints.

CLOSE THE LOOP

- **R-22** Protected evidence custody and examination
- **R-23** Objective closure + independent effectiveness evidence
- **R-24** Leading indicators + reopening thresholds

Learning is complete only when later evidence shows the revised control structure actually reduced recurrence risk.

TRANSFERABLE LESSON **If evidence cannot be independently examined, uncertainty propagates into corrective-action validation.**

CAST Part 5: Prevention Architecture

28 research-derived control proposals organized by preventive function

TRACEABILITY
6 end-to-end pathways · effectiveness / reopening logic

WHAT A PROPOSAL CAN DO	BLOCK PATHWAY	TRIGGER HOLD / DEFER	MITIGATE CONSEQUENCE	IMPROVE LEARNING	traceable to CAST findings + control paths

PREVENT RELEASE 20 proposals	10 **Pressure-boundary integrity & component-state assurance** R-01–R-10	5 **Readiness, waivers & decision support** R-11–R-14, R-16	3 **Authorization & common acceptance baseline** R-15, R-26–R-27	2 **Operational verification & closure** R-21, R-28	
MITIGATE CONSEQUENCES 5 proposals	4 **Flight termination & consequence control** R-17–R-20	1 **Launch-site & plume protection** R-25			
LEARN & VERIFY 3 proposals	1 **Evidence preservation & investigation** R-22	2 **Corrective-action learning & indicators** R-23–R-24			

The above counting classifies each proposal by its prevention domain; it do not indicate causal importance or expected effectiveness.

REPRESENTATIVE CONTROLS

- R-02 serialize seals + load history
- R-17 evaluate loaded-stage FTS strategy
- R-22 protected evidence custody
- R-24 leading indicators + stop thresholds
- R-26 common acceptance package

Where CAST Extends the Official Prevention Architecture

Additional or structurally extended controls identified after the independent CAST analysis

RESULTS COMPARISON **The extension represents CAST's ability to analyze the context around the control architecture. Additional findings do not mean the Official Investigation missed aspects; it was focused on the causes, while CAST analyzes the causal factors.**

Cumulative assurance

SF-6 / SF-7 / SF-12 **R-11–R-13, R-16**

Protected review time, interacting-deviation assessment, evidence gates, and explicit decision rights.

Common release baseline

SF-8 / SF-14 **R-15, R-26–R-27**

Cross-authority change disposition and one configuration-controlled vehicle / trajectory / waiver / evidence state.

Operational verification

SF-10 / SF-15 **R-21, R-28**

Live stop/go evidence, open-item control, and closure from preflight criteria through post-flight feedback.

Protected evidence access

SF-11 **R-22**

Prearranged custody, secure laboratory access, telemetry retention, cleared experts, and controlled disclosure.

Nominal plume safety

SF-13 **R-25**

Launch-site compatibility for nominal plume, thermal, acoustic, mechanical, and infrastructure effects.

Effectiveness feedback

SF-12 **R-23 / R-24**

Objective corrective-action closure, recurrence checks, leading indicators, and reopening after adverse feedback.

KEY DISTINCTION **Some controls have direct or partial official counterparts; the additional architecture is where CAST makes the interfaces and feedback loops explicit and testable.**

CAST vs. Official SIPAE Investigation

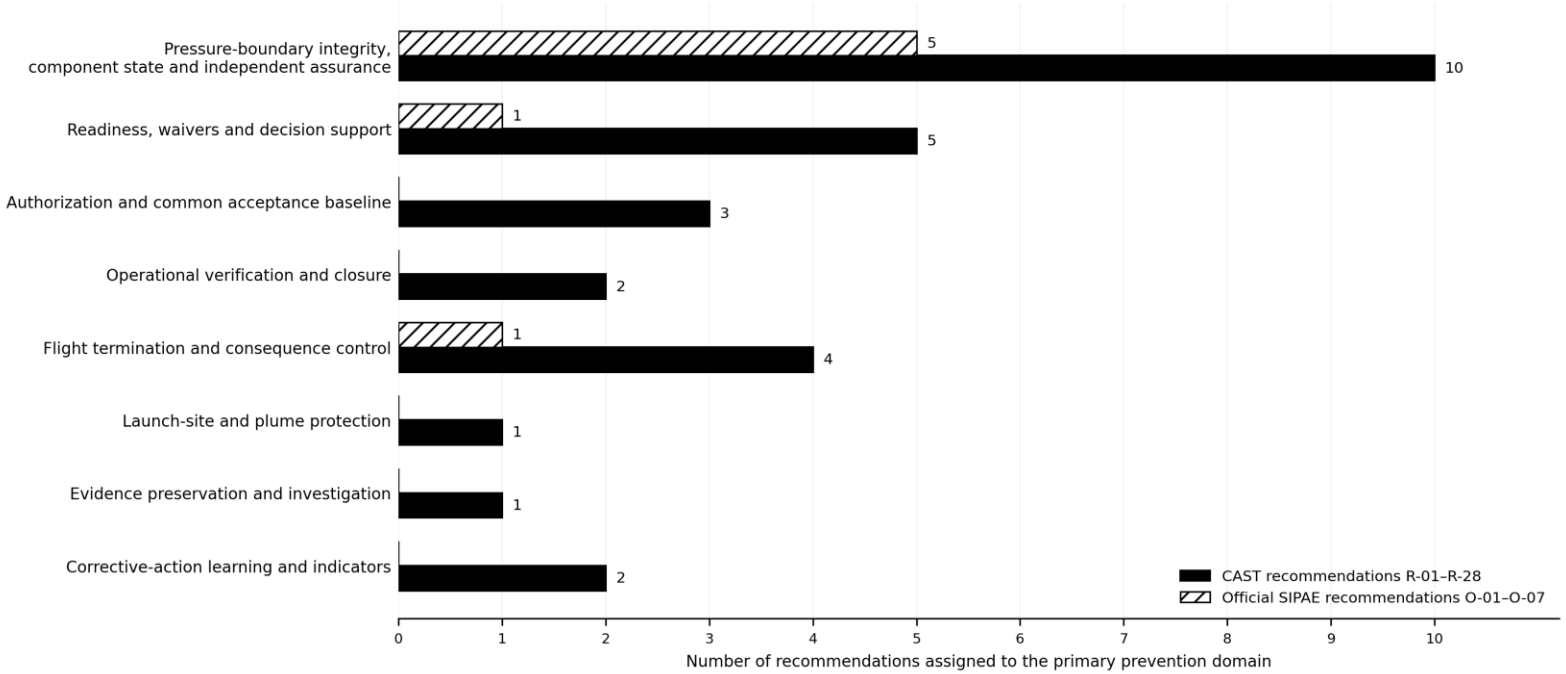
COMPARISON TRACE physical/contextual findings · 15 CAR · SM-7 crosswalks: 15 SF + 28 Recommendation proposals

Convergence on the occurrence and official recommendations, with broader control-system decomposition and prevention domains

COMPLEMENTARY, NOT ADVERSARIAL

Same occurrence evidence;
CAST aligned with all 3 factor categories of the official report and mapped all 7 official recommendations.

RECOMMENDATIONS DOMAIN ALLOCATION



1 CONVERGENCE — Physical sequence retained

CAST aligned with all 3 official contributing-factor categories
And mapped all 7 official recommendations represented

2 DECOMPOSITION / EXTENSION

- **O-04** independent assembly check → readiness / release independence with stop authority
- **O-07** FTS evaluation → modeling, consequence variables, exercises, and near-pad vulnerability controls

3 RELATIONSHIP TYPES

The comparison is qualitative, not a score

- common acceptance baseline · live verification / closure
- protected evidence custody · nominal plume protection
- corrective-action effectiveness

HOW TO READ "28 vs 7"

More recommendations ≠ a better investigation.

The contribution is broader control coverage, traceability, and effectiveness feedback.

Recommendation Proposal	Added control and preventive relevance	CAST and official investigation relationship
R-01: Define validated minimum and maximum seal-compression limits, rejection rules and calibrated metrology.	Adds qualification-backed bounds and an auditable procedure basis, as suggested in the Parker O-Ring Handbook (2021). Preventive relevance: Direct release barrier: the 12–14 mm entry would become an out-of-limit stop and disposition condition before release (H-1/H-4).	CAST trace: SF-1, SF-10; ICF-1–ICF-2; C-3.1/C-3.2 Official relationship: Direct counterpart to O-01.
R-12: Assess waivers, nonconformances, lost test coverage, late evidence and repeated anomalies cumulatively.	Requires cumulative assessment of deviations, common drivers and test coverage. Preventive relevance: Could expose cumulative assurance obligation and trigger a no-go decision even when each individual deviation appears acceptable.	CAST trace: SF-6, SF-12; IP-4 Official relationship: No direct official counterpart.
R-17: Revise FTS strategy to evaluate early termination after catastrophic propulsion/structural failure with loaded stages.	Specifies quantitative debris, blast, thermal and energy-dispersion modeling. ISO 14620-3 provides the flight-safety objective. NASA-STD-8719.25 supplies technical range-safety requirements. FAA Part 450 provides complementary operational controls. Preventive relevance: Consequence mitigation, not rupture prevention: could reduce loaded-stage impact energy and near-pad blast/thermal damage after structural failure (H-3/H-5).	CAST trace: SF-9; IP-6; C-5 Official relationship: Direct counterpart to O-07.
R-25: Reassess configuration-specific nominal plume loads, launch-pad standoff and near-pad facility tolerance before flight.	Converts the report's fence-damage fact into a validated nominal-plume, standoff and facility-tolerance control as required by ISO 14620-2:2019, safety requirements – Part 2: Launch site operations. Preventive relevance: Prevents the separate nominal-plume infrastructure consequence; it is not a control for the chamber-rupture pathway.	CAST trace: SF-13; IP-9; H-7 Official relationship: No direct official recommendation counterpart.

Why CAST Was Worth the Time

The value was a greater control-system structure and traceable prevention framework, not a different physical cause

THE RETURN ON THE ANALYSIS

CAST turned one documented mishap into a reusable explanation of how safety-relevant state, authority, feedback, and learning can degrade across process limits and boundaries.

Same public evidence · no proprietary research data

1 Changed the reason of analysis

From the chamber / seal alone to control relationships spanning configuration, readiness, authorization, flight consequence control, and learning.

5 controlled processes

2 Reconstructed local decision context

Actions were assessed against responsibilities, process models, available feedback, and context: not treated retrospectively as sufficient explanations.

controller analyses + local rationality

3 Made interface weaknesses explicit

State memory, change-triggered assurance, common release baselines, consequence variables, and protected evidence access became visible control problems.

11 interaction patterns → 15 systemic findings

4 Linked findings to verifiable controls

The analysis ends with traceable proposals, closure criteria, effectiveness feedback, and reopening logic rather than recommendation issuance alone.

28 proposals + effectiveness feedback

METHOD RETURN

Evidence → constraints → HCS → controller reasoning → interaction patterns → systemic findings → proposals → effectiveness feedback

This is the audit trail that makes the additional prevention proposals logic inspectable.

Conclusion: From Physical Failure to System Control

CAST preserved the physical explanation and extended prevention across the control structure

The rupture occurred in the first-stage pressure boundary.

The prevention opportunities are distributed across the proposed control structure.

1 WHAT FAILED

Progressive loss of sealing at the dome-casing interface led to first-stage chamber rupture and vehicle fragmentation.

Consistent with the official physical sequence

2 WHAT CAST ADDED

Component-state memory, change-triggered assurance, common release-state continuity, consequence-state representation, and learning controls.

15 systemic findings across interacting controllers

3 WHAT PREVENTION REQUIRES

Traceable control changes that preserve state, reopen assurance after change, synchronize release evidence, manage total harm, and verify corrective-action effectiveness.

28 research-derived proposals across 8 prevention domains

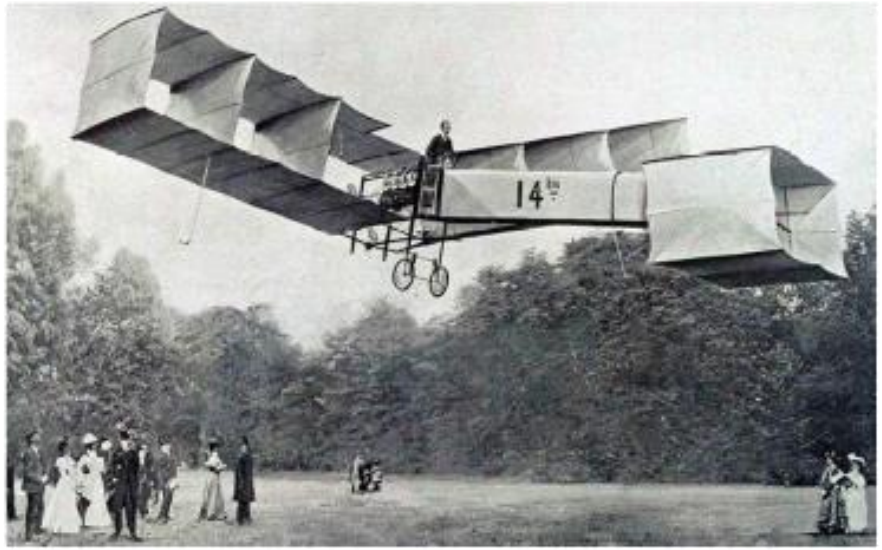
EVIDENCE-BOUNDED CONCLUSIONS

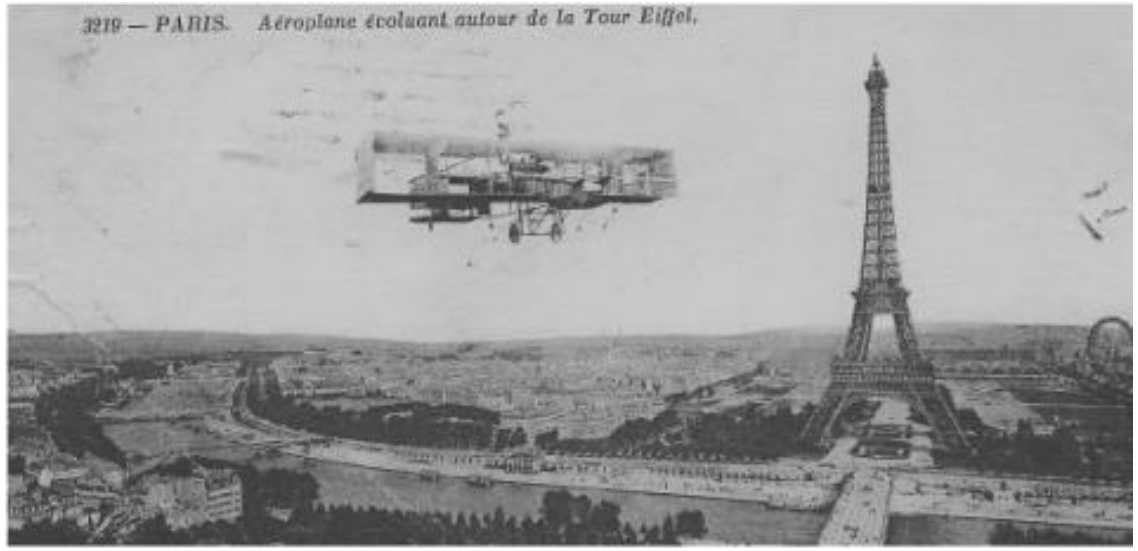
The study does not establish legal noncompliance, subjective intent, a uniquely proven microscopic initiation mechanism, or the counterfactual outcome of alternative FTS timing.

FINAL TAKEAWAY

CAST was valuable not because it found a different event or cause, but because it turned the same evidence into a broader, traceable prevention framework capable to be applied to other similar systems and 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

Capt Diniz – dinizavdm@fab.mil.br

Launch Video

