STPA Applied to Launch Operations Management

STAMP Workshop
MIT – March 25-28, 2019

1st Lt Diniz, Doc Eng Carlos Lahoz, 1st Lt Silveira, Eng Sérgio Fugivara

Aerospace Engineer

1st Lieutenant
Brazilian Air Force

Master Student
Space Science and Technology
(Space Systems, Launches and Tests)

- Certification
- Conformity Assessment
- Quality Management Systems
- Launch Center Inspections
- Launch Center Readiness
- Launch Vehicle Flight Approval
- Standards - Space Systems

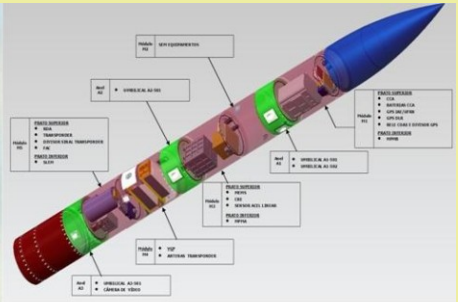
IFI – Strengthening the Brazilian Aerospace Power

Safety at Launch Operations?

VLS-1 V03 - 2003

2015

2016



Objective

Identify hazards, unsafe control actions and loss scenarios in Brazilian Launch Operational Management, in order to minimize the effects of unsafe events or mitigate their consequences for future launch campaigns.

Headlines:

1) Introduction

2) STAMP-STPA Results

3) Future work

4) Conclusion

Headlines:

1) Introduction

2) STAMP-STPA Results

3) Future work

4) Conclusion

Introduction

Systems safety study applied to Launch Operations Management is strategic because it deals with the **preservation of human lives, properties, mission fulfilment, knowledge and environment**.

The goal of this work is the **analysis of systemic factors** that influence the **safety management in Brazilian launch operations** of suborbital vehicles, based on previous Brazilian campaigns.

For achieve this purpose, this study uses **STAMP-STPA**.

Headlines:

1) Introduction

2) STAMP-STPA Results

3) Future work

4) Conclusion

Identify losses (L)

Stakeholders in the system.

- **IAE:** rocket stages development, assembly and launch;
- **IFI:** product assurance, audits/inspections, quality control;
- **DLR:** payload stage development and assembly;
- **AEB:** customer and financial support;
- **CLA:** ground support, facilities, medical care, electric power generation, radar & telemetry station, sensitive information;
- **CLBI:** ground support, telemetry;
- **COMPREP:** logistic transport;
- **Users:** payload/experiments able for launch:
- **Brazilian Air Force:** customer and manager of COMPREP, IAE, IFI, IEAV, CLA and CLBI.

Identify losses (L)

- L-1: Loss of life or injury to persons;
- L-2: Environmental losses;
- L-3: Loss or disclosure of sensitive information;
- L-4: Loss or damage to public or private properties;
- L-5: Loss or damage to the vehicle;
- L-6: Loss of ground support operation; and
- L-7: Mission loss or degradation.

Identify the Hazards (H) system level

H-1: Damage of the structural integrity of the vehicle or payload;

[L-1] [L-2] [L-4] [L-5] [L-7]

H-2: Privation to track/communicate to the vehicle or payload;

[L-1] [L-2] [L-4] [L-6] L-7]

H-3: Permanence of personnel in environment with energetic material, toxic material or with pressure vessels;

[L-1]

Identify the Hazards (H) system level

H-4: Vehicle or payload out of flight route;

[L-1] [L-2] [L-4] [L-7]

H-5: Premature ignition of vehicle stages at the launch rail;

[L-1] [L-2] [L-4] [L-5] [L-6] [L-7]

H-6: Leak of sensitive information;

[L-3]

H-7: Inadequate or unrealized launch facilities maintenance;

[L-1] [L-2] [L-3] [L-4] [L-5] [L-6]

Identify Safety Constraints (SC) system level

The identification of safety constraints (SC) at the system level specifies the conditions that must be met to avoid the hazards (H) and prevent losses (L).

H-5: Premature ignition of vehicle stages at the launch rail.

- **SC-5.1:** At the launch rail, vehicle stages must be prevented from igniting before planned, even when subjected to commands or electric discharges.
- **SC-5.2:** In the event of an unintended ignition, the vehicle must remain fixed to the launching rail, avoiding an unplanned route.
- **SC-5.3:** Vehicle stages and interfaces must be designed so that, in the event of an unintended ignition, they do not result in the vehicle explosion.

Refining system-level hazards

Hazards can be refined into sub-hazards, useful for large analysis efforts and complex applications.

TT&C -Telemetry, Tracking, Command & Monitoring

H-2: Privation to track/communicate to the vehicle or payload;

- H-2.1: Inability to destroy the vehicle in flight.
- H-2.2: Impossibility to locate parts of the vehicle or payload.
- H-2.3: Inability to monitor flight or payload behavior.

Ignition

H-5: Premature ignition of vehicle stages at the launch rail.

- H-5.1: Electrical discharge in the region of the launching rail.
- H-5.2 Vehicle Safety System Faults.

Modeling the Control Structure

Controllers:

- Regulations
- Customer/Users
- Supervisor
- Producer/Developer
- Third Part Analysis
- Launch Centers
- Operators

Modeling the Control Structure

Responsibilities of Third Part

(...)

R-3.2: Conduct inspections and audits at Launch Centers and Producers;

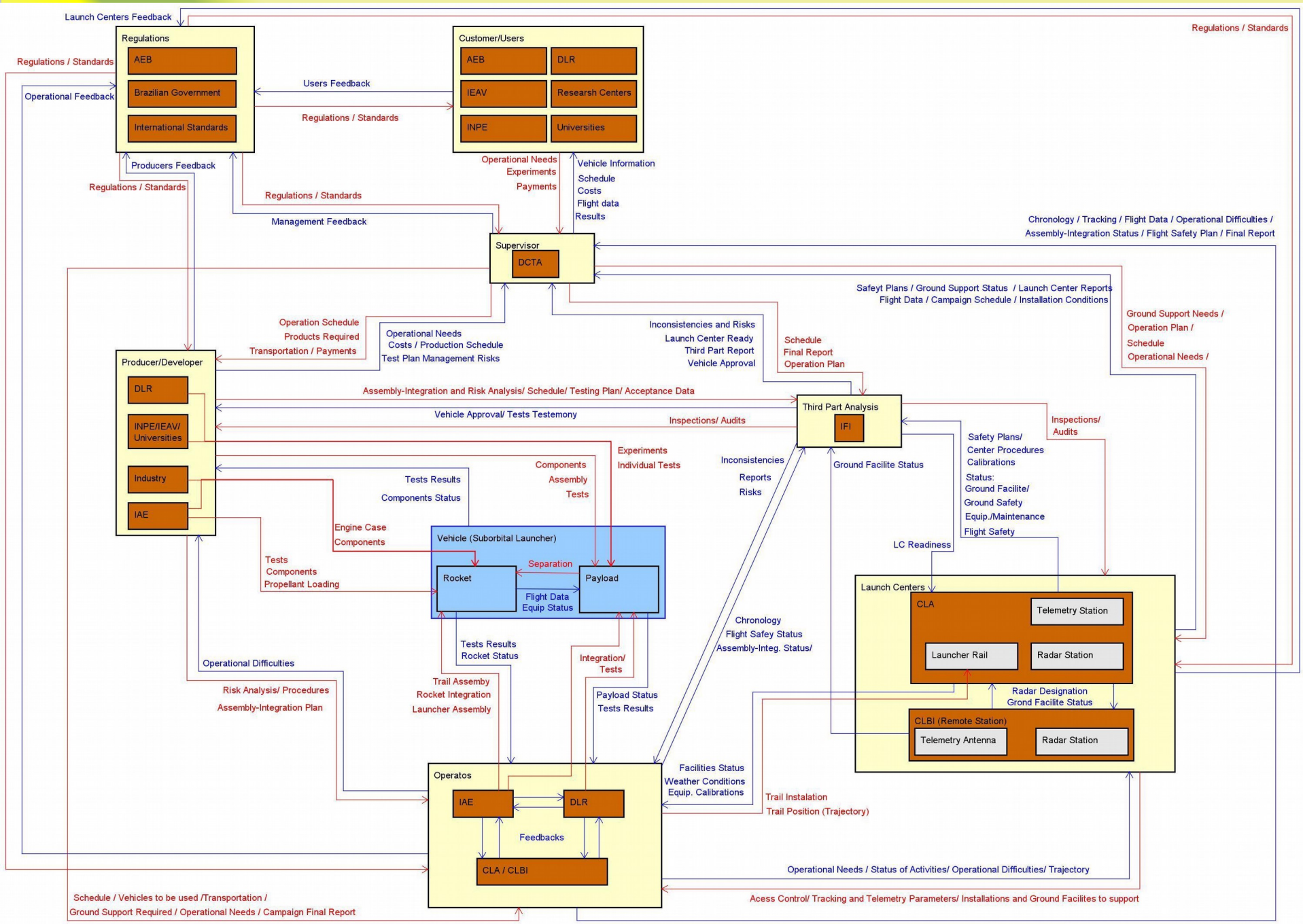
(…)

R-3.4: Issue Technical Report regarding the Approval / Acceptance of the Vehicle for flight;

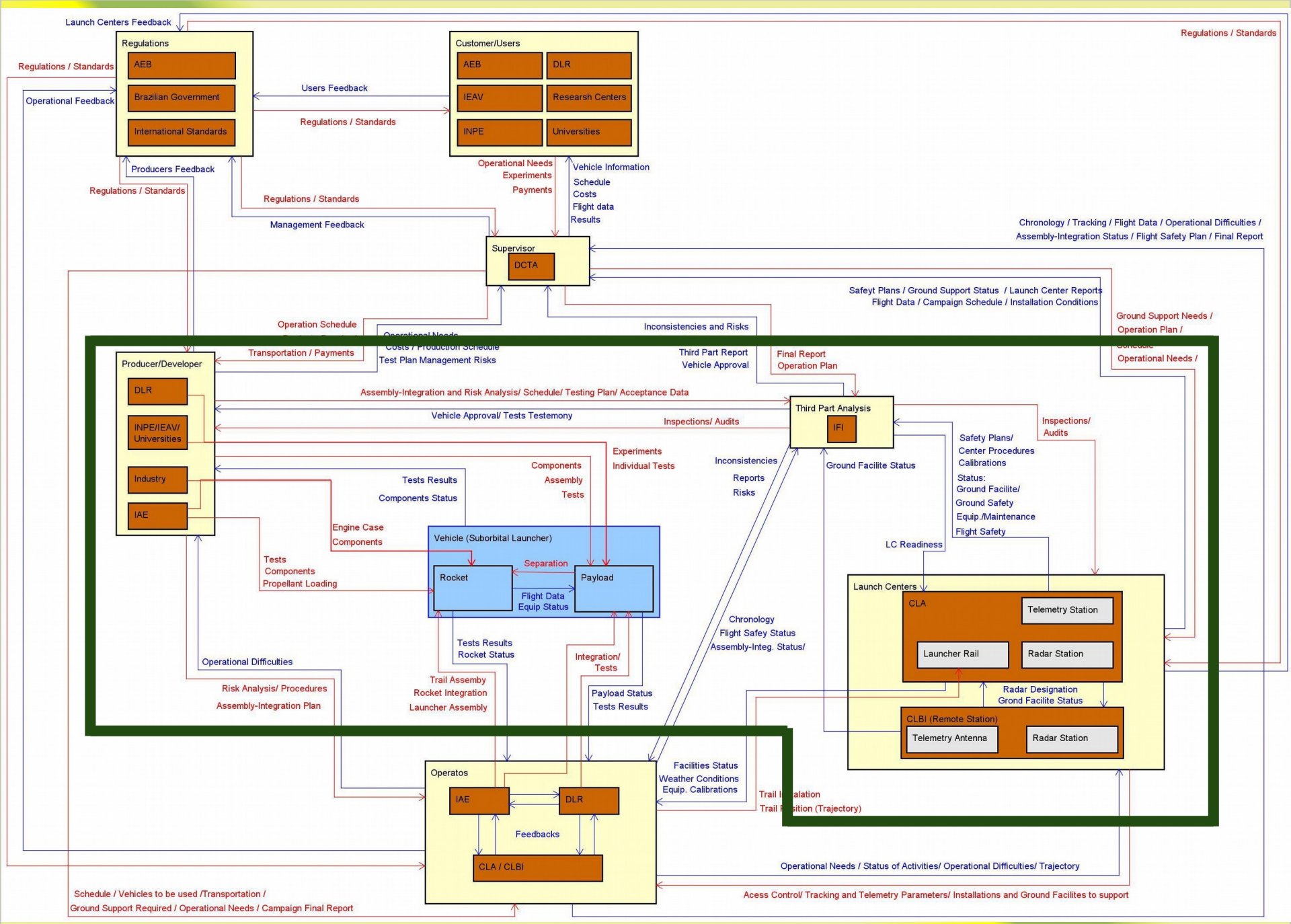
R-3.5: Issue Technical Report regarding the Readiness of the Launch Center;

(…)

R-3.13: Evaluate the adequacy of the safety procedures that will be used in the Campaign;

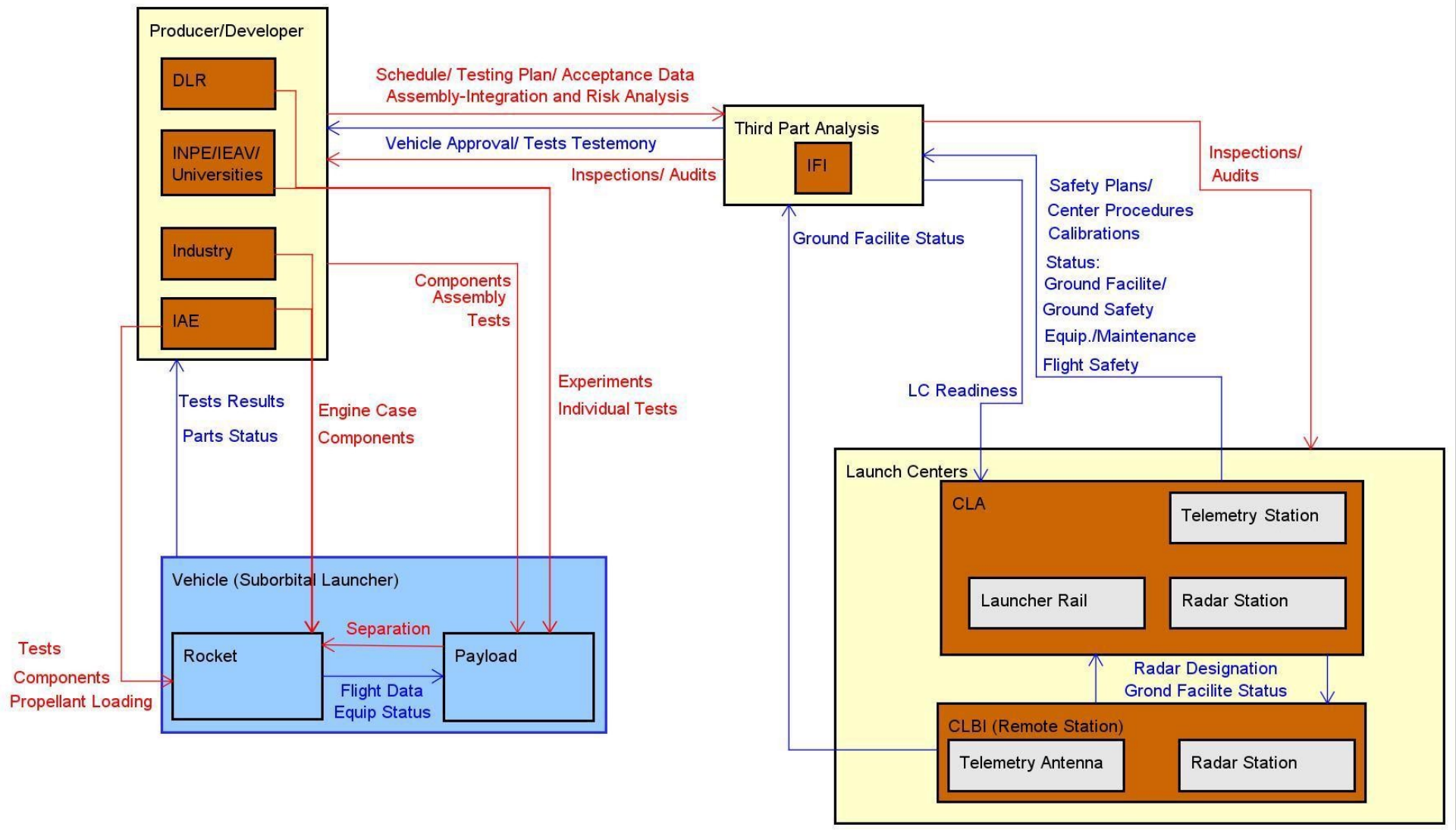


HCS of a typical Brazilian Suborbital Launch Operation. (Utilized “STAMP Workbench” software [11])



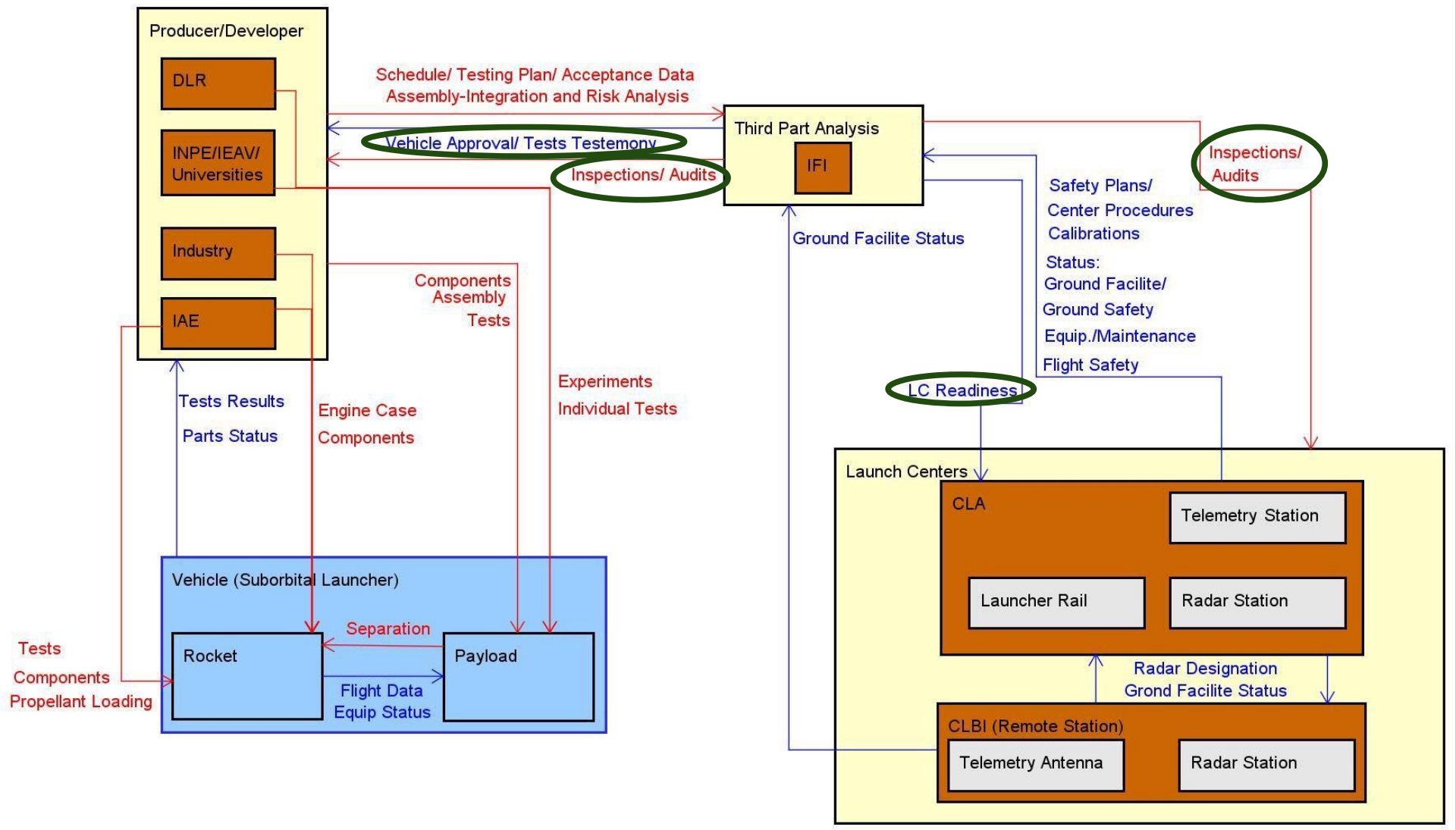
HCS of a typical Brazilian Suborbital Launch Operation. (Utilized “STAMP Workbench” software [11])

Unsafe Control Actions (UCAs)



Reduced Control Structure of the system involving the Third Part – Launch Centers – Producers/Developers. (Utilized “STAMP Workbench” software [11])

Unsafe Control Actions (UCAs)



Reduced Control Structure of the system involving the Third Part – Launch Centers – Producers/Developers. (Utilized “STAMP Workbench” software [11])

Unsafe Control Actions (UCAs)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Analysis of Vehicle and Payload for approval	UCA-1: Third Part does not provide vehicle analyses concerning flight route when a new launch rail will be used. [H-1] [H-4] [H-5] UCA-2: Third Part does not provide vehicle analyses to verify the capability to fulfill a unusual mission. [H-2] [H-4] UCA-3: Third Part does not provide vehicle analyses to check the integration procedures when the payload has pressure vessels. [H-3]	UCA-4: Third Part provides vehicle approval when the Launch Center did not evaluate or check vehicle safety criteria. [H-4] [H-10]	UCA-5: Third Part provides vehicle analysis too early and items are produced or tested after the approval. [H-1] [H-2] [H-4] [H-5] UCA-6: Third Part provides vehicle analysis too late, after the start of campaign activities. [H-7] [H-8] [H-9]	UCA-7: Third Part stoped too soon the vehicle analysis, due to unavailability of personnel, the acceptance tests can not be accompanied or approved. [H-1] [H-2] [H-4] [H-5] UCA-8: Third Part stopped too soon the vehicle analysis so the acceptance of components could not be verified. [H-1] [H-2] [H-4] [H-5] UCA-9: Third Part stopped too late the vehicle analysis when the campaign schedule was crucial to mission fulfillment. [H-7] [H-8] [H-9]

Unsafe Control Actions (UCAs)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Production Inspections and Audits	UCA-10: Third Part does not provide inspections and audits in production to check the Manufacturing Process, parts accepted to use at the vehicle but not verified. [H-1] [H-2] [H-4] [H-5]	UCA-11: Third Part provides inspections and audits in production so the developer receive the parts without check for nonconformities. [H-1] [H-2] [H-4] [H-5]	UCA-12: Third Part provides inspections and audits in production too late, after the parts are produced. [H-1] [H-2] [H-4] [H-5] UCA-13: Third Part provides inspections and audits in production too early, only before assembly of the production line. [H-7] [H-8] [H-9]	UCA-14: Third Part stopped too soon the inspections and audits, do not verifying the critical equipments and process for the mission safety. [H-1] [H-2] [H-4] [H-5]

Unsafe Control Actions (UCAs)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Launch Center Ready Situation	UCA-15: Third Part does not provide LC readiness, so the supervisor and operators can not confirm if the Ground Support Equipments are ready to track the Vehicle. [H-2] [H-7] UCA-16: Third Part does not provide LC readiness, when the facilities and equipment are not compatible with those requested for vehicle integration. [H-2] [H-7] [H-8] [H-9]	UCA-17: Third Part provides LC readiness for the vehicle without verify the payload safety criteria. [H-3]	UCA-18: Third Part provides LC readiness too early and occurred a modification on the date of the Operation, so the situation of readiness is different from that evaluated / approved. [H-3] [H-7] [H-8]	UCA-19: Third Part stopped too soon the LC readiness analysis, the information obtained in a large advance from the campaign and the reports does not reflect the current readiness situation of the Launch Center. [H-2] [H-7] [H-8]

STAMP-STPA

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Inspections and Audits at Launch Centers	UCA-20: Third Part does not perform Inspections and Audits at LC when operational systems will be used by the first time. [H-2] [H-7] [H-8] UCA-21: Third Part does not perform Inspections and Audits at LC when uncalibrated equipment are available for the operators at the assembly installations. [H-2] [H-7] UCA-22: Third Part does not perform Inspections and Audits at LC when external maintenance contracts are expired. [H-7] UCA-23: Third Part does not perform Inspections and Audits at LC when safety equipment received have not been verified. [H-7]	UCA-24: Third Part provides routine inspections and audits at LC during a launch campaign. Resulting in delays at the mission schedule. [H-8]	UCA-25: Third Part performs Inspections and Audits at LC too early, before final vehicle definition. [H-2] [H-7] [H-8] UCA-26: Third Part performs Inspections at LC only annually, even if theres more than one operation per year. [H-2] [H-7] [H-8] UCA-27: Third Part performs Inspections at LC too late, so it need to be carried out simultaneously to the Operation. [H-7] [H-8] [H-9]	UCA-28: Third Part stopped too soon the Inspections at LC, because it started to be performed shortly before the beginning of the campaign activities, and needed to finish the verification without complete evaluation of the equipaments. [H-2] [H-7] [H-8]

Identifying Loss Scenarios

UCAs	Loss Scenarios
UCA-8: Third Part stopped too soon the vehicle analysis so the acceptance of components could not be verified. [H-1] [H-2] [H-4] [H-5]	Damage of parts at storage. Parts not useful for assembly. Applied corrective measures without verify/ study the effects. (Fins/2016)
UCA-10: Third Part does not provide inspections and audits in production to check the Manufacturing Process, parts accepted to use at the vehicle but not verified. [H-1] [H-2] [H-4] [H-5]	Acceptance of parts without verification of the products neither the process. Behavior of the system (ignition / flight / recovery) can be different from the project. (Thermal Protection - Propellant / 2015)
UCA-18: Third Part provides LC readiness too early and occurred a modification on the date of the Operation, so the situation of readiness is different from that evaluated / approved. [H-3] [H-7] [H-8]	Components of the vehicle not ready. Campaign date change. Ground Support Equipments not checked again. Equipments uncalibrated or with calibration date expired. Some systems nonoperational for lack of maintenance.

Headlines:

1) Introduction

2) STAMP-STPA Results

3) Future work

4) Conclusion

Future Work

- Obtain a complete UCAs from the HCS and related loss scenarios.
- Propose recommendations and safety restrictions for future brazilian launch operations.
- Identify Leading Indicators of risk.
- Apply STAMP-STPA for an orbital launch operation.
- Apply STAMP-STPA for complex and critical subsystems of the vehicle/payload (rocket engines).

Headlines:

1) Introduction

2) STAMP-STPA Results

3) Future work

4) Conclusion

Conclusion

•28 UCAs identified at only 4 Control Action. The HCS proposed has more than 100 Control Actions / Feedbacks to study and identify UCAs, Loss Scenarios and Constraints in order to propose Safety Recommendations.

•This work, after further detailing and verifications, will allow IFI to act in order to help the avoidance of unsafe actions at future Brazilian launch campaigns or to mitigate their consequences.

Identify the Hazards (H) system level

H-8: Delays in launch campaign (greater than 1 week for start or 1 day at the campaign);

[L-7]

H-9: Costs above budget (more than 10% than expected);

[L-7]

H-10: Unable to recover the payload.

[L-2] [L-7]

STAMP-STPA - References

[1] Leveson, N. G. A new accident model for engineering safer systems. Safety Science, v. 42, n. 4, 2004, p. 1-2.

[2] DCA 400-6/2007: Life Cycle of Aeronautical Systems and Materials.

[3] Leveson, N. G. Engineering a Safer World: Systems Thinking Applied to Safety,,Cambridge, Mass.: The MIT Press, 2012.

[4] Leveson, N. G.; Thomas, J. STPA Primer. USA, 2013.

[5] Walls, L., Revie, M., Bedford, T. Risk, Reliability and Safety: Innovating Theory and Practice. 26th ESREL. Glasgow, Scotland, 2016, p. 129.

[6] Young, W. & Leveson, N. Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory. Proceedings of the ACM, 2014, Vol 57 no 2, p. 35.

[7] Accident Investigation Report – VLS-1 V03. COMAER, 2004.

[8] Leveson, N. G. STPA-Handbook. USA, 2018.

[9] DCA 800-2/2016: Quality and Safety of Systems and Products at COMAER.

[10] Leveson, N. G.; Stephanopoulos, G. A system-theoretic, control-inspired view and approach to process safety. AIChE Journal, v. 60, n. 1, 2014, p 13.

[11] STAMP Workbench 1.0.1/bcc4c6, developed by Apache Software Foundation. Copyright (C) 2018 Information-technology Promotion Agency, Japan (IPA).