Departament of Aerospace Science and Technology

Industrial Fostering and Coordination Institute

RECOMMENDATIONS FOR FLIGHT SAFETY SYSTEMS APPLYING SYSTEM-THEORETIC PROCESS ANALYSIS

Capt. Antonio Vinicius **Diniz** Merladet

Dr. Carlos Lahoz; Dra. Chiara Manfletti; Col. Castilho; Capt. Silveira

MIT STAMP Workshop 2024

Objective

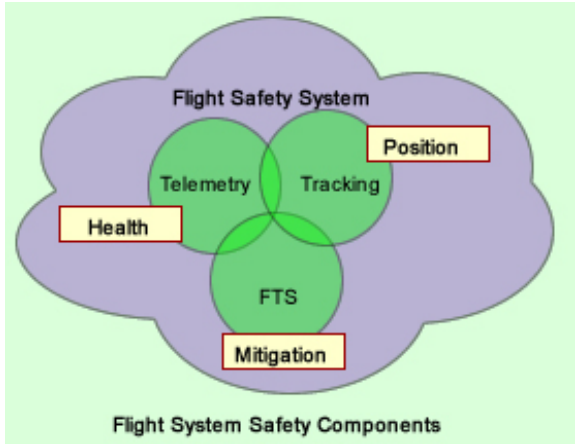
Identify losses, hazards, safety constraints and unsafe control actions of Flight Safety Systems, detecting loss scenarios, suggesting Regulations/Standards harmonization, and proposing Safety/Security Recommendations to minimize the effects of unsafe events or mitigate their consequences for future Launch Operations.

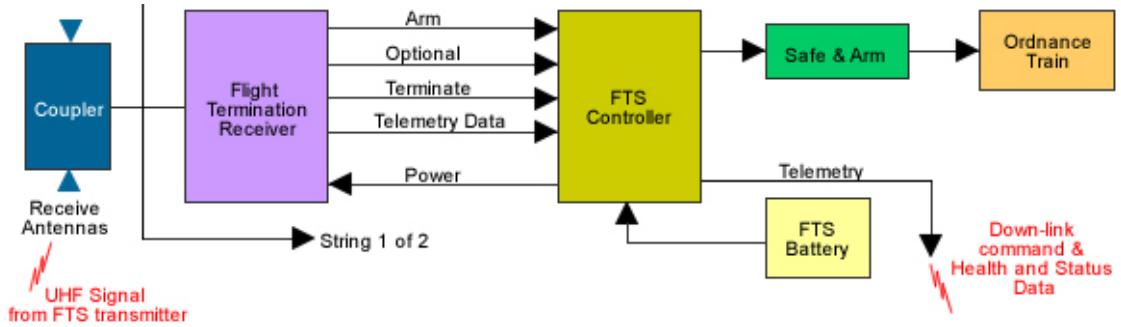
Headlines:

1) Introduction
2) Systemic Factors (Background)
3) System-Theoretic Process Analysis (STPA)
4) STAMP-STPA Results
5) Safety Recommendations for Flight Safety Systems
6) Conclusions

Flight Safety Systems

NASA [42]



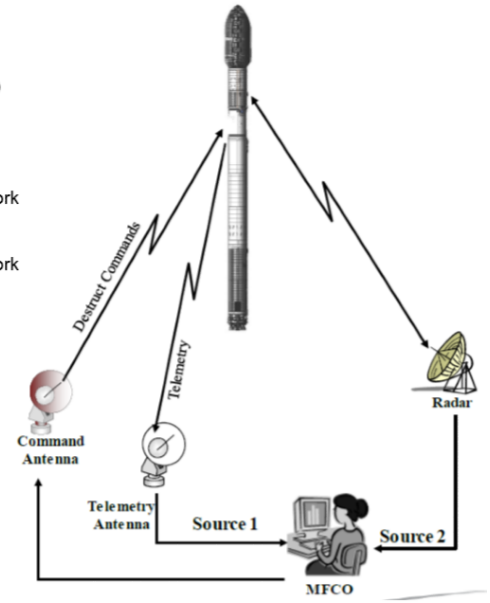


FTS Control Structure – NASA [44]

Flight Systems
- Flight Termination System
  - Receiver
  - FTS Logic Box
  - Battery
  - UHF Antenna
  - Hybrid Coupler
  - Safe & Arm
  - Ordnance
- Metric Tracking Sources (RCC 324)
  - GPS
  - Telemetry Encoder
  - Telemetry Transmitter
  - S-band Antenna
  - L-band Antenna
  - Couplers
  - Power Distribution Box
  - Vehicle Battery
- Radar Transponder
  - Transponder
  - C-band Antenna
  - Hybrid Coupler
  - Power Distribution Box
  - Vehicle Battery

Ground Systems
- Command Transmitters
  - Power Supplies (Redundant Sources)
  - Antennas (Omnis & Directional)
  - Amplifiers (10 kW Tubes)
- Telemetry Receivers
  - Antennas
  - Decoders
  - Ground Communications Network
- Radars
  - Radar Sites
  - Ground Communications Network
  - Timing Infrastructure
- Mission Flight Control
  - MFCO
  - Telemetry Officer
  - Certified Displays

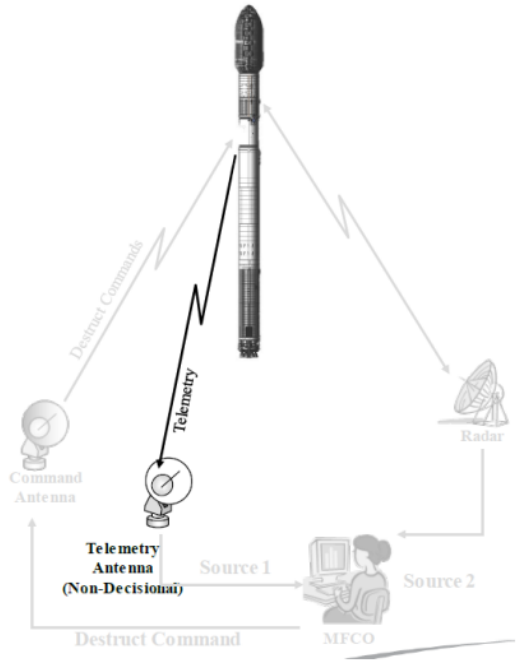
Operational Considerations
- Telemetry Formats
- Telemetry Tapes
- Launch Constraints
- Range assets are degrading and/or being decommissioned



Traditional FTS (actives by ground command) - NASA [46]

Flight Systems
- Metric Tracking Sources (RCC 324)
  - GPS
  - L-band Antennas
  - Coupler
  - IMU/INS
  - Flight Computer
  - Power Distribution Box
  - Vehicle Battery
- Flight Termination System
  - Autonomous Flight Termination Unit
  - Safe & Arm
  - Thrust termination/Ordnance

Other
- Preflight Testing



Autonomous FTS - NASA [46]

Recommendations for Flight Safety Systems?

Significant Chinese Space Launch Failures

In January 1995, a more tragic failure beset the Long March 2E program. Once again, the rocket exploded shortly after launch, but this time falling debris killed six people and injured 23 in a nearby rural area. Like the December 1992 launch, this carried a communications satellite (APStar 2) built by Hughes. In July 1995, CGWIC

The question of China's openness arose again following another significant launch failure in February 1996. A new version of the Long March 3, CZ-3B, was used for launch of the Intelsat 708 satellite. Seconds after liftoff, the rocket inverted itself and crashed to Earth in a village near the launch site. Officially, China reported that 6 died, 57 were injured, and 80 homes destroyed. Western observers who were present at the launch (and whose hotel also was severely damaged) insist that many more must have died. An Israeli attending the launch visited the village the next day and captured the ruin on videotape which was later shown in the West, buttressing the view that more devastation was incurred than China was ready to admit. In this case, Space Systems/Loral manufactured the satellite. The accident investigation board concluded that an inertial guidance system malfunctioned. A Loral-led team reviewed China's assessment of the launch failure, which has subsequently led to an investigation into whether Loral or Hughes, which also participated in the review panel, transferred missile-related technology to China (see **Commercial Launch Services**, below). Intelsat canceled two additional planned launches. The fatalities raised questions about range safety in China. China reportedly agreed to evacuate surrounding villages before future launches and revise launch destruct procedures.

Extracted from [23]

Commercial Space Transportation
Alcântara Launch Center (CLA) / Alcântara Space Center (CEA)

spacenews.com
https://spacenews.com › south-kor... · Traduzir esta página

South Korea's Innospace succeeds in test launch

21 de mar. de 2023 — South Korean rocket startup **Innospace** successfully **launched** a suborbital rocket from Brazil on March 19, demonstrating a hybrid motor it ...

Virgin Orbit

VIRGIN ORBIT FORMALLY ESTABLISHES NEW BRAZILI...

The Alcântara Launch Center has hosted several launches of suborbital rockets, but the facility has not yet been used to reach Earth orbit. By...

27 de jun. de 2022

mundogeo.com
https://mundogeo.com › ... › News · Traduzir esta página

OrionAST Relies on Alcântara Space Center to Launch ...

11 de out. de 2022 — **OrionAST** Relies on **Alcântara Space Center** to Launch Satellites to Identify Space Debris. American company founded in 2013 was selected by ...

Foguete explode durante testes no Centro de Lançamento de Alcântara

Por **Redação Defesa em Foco** - 12 de novembro de 2020 18:19

Extracted from [28]

STPA applied to Flight Safety Systems

Identification of Losses (L) for this STPA applications

FSS.L-1: Human injury; properties damage; human life or environmental losses;

FSS.L-2: Loss of mission; loss or damage to vehicle or payload; and

FSS.L-3: Loss or damage to launch facilities.

Identification of system-level Hazards (H)

Hazard Code	System-Level Hazard Description	Associated Losses
FSS.H-1	Vehicle deviates from the intended route and violates the prescribed flight safety limits. (FTS is not activated)	[FSS.L-1] [FSS.L-2]
FSS.H-2	FTS activates with the vehicle on intended route, inside prescribed flight safety limits.	[FSS.L-2]
FSS.H-3	FTS activates before launch.	[FSS.L-1] [FSS.L-2] [FSS.L-3]
FSS.H-4	FTS activates after launch but before clearing the launch center protected area.	[FSS.L-2] [FSS.L-3]

STPA applied to Flight Safety Systems

Identification of Safety Constraints (SC)

Hazard Code	SC. Code	System-Level Safety Constraints
[H-1]	**FSS.SC-1.1**	Vehicle shall not violate the prescribed flight safety limits.
	FSS.SC-1.2	If the launch vehicle approaches the prescribed flight safety limits, then the deviation of intended route shall be detected and measures taken to prevent the vehicle to violate flight safety limits.
[H-2]	**FSS.SC-2.1**	Vehicle route shall be detected in real time.
	FSS.SC-2.2	Vehicle on intended route shall not be terminated.
[H-3]	**FSS.SC-3.1**	Vehicle shall not be terminated on-ground.
	FSS.SC-3.2	The termination mechanism of an FTS shall not be capable to terminate the vehicle before launch.
[H-4]	**FSS.SC-4.1**	After launch, the vehicle shall not be terminated within launch center protected area.

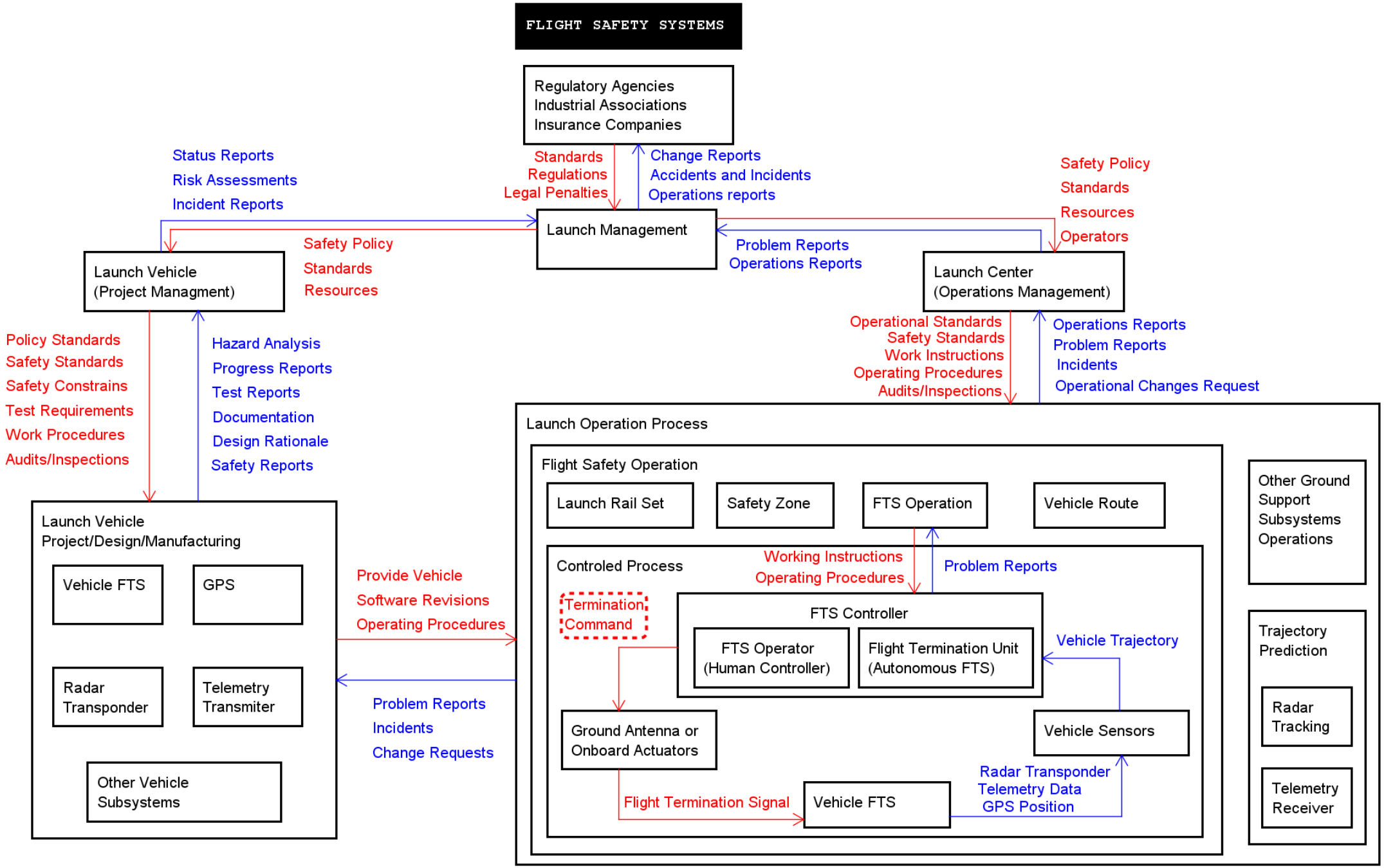
STPA applied to Flight Safety Systems

Modeling the Hierarchical Control Structure (HCS)

Main controllers and quantity of responsibilities identified:

08 for FTS Operation by Human Operator (Ground commanded FTS);
09 for FTS Operation by Flight Termination Unit (Autonomous FTS);
04 for Ground actuators of the FTS signal/command transmission system (Ground commanded FTS);
05 for Vehicle Sensors for trajectory data provision (Autonomous or Ground commanded FTS); and
06 Ground Sensors for trajectory data provision (Ground commanded FTS).

Main Controllers	Responsibilities	Controllers Responsibilities
FSS.C-1 FTS Operation by Human Operator (Ground commanded FTS)	**FSS.C.R-1.2**	Do not provide flight termination commands with the vehicle on ground and without ignition of any vehicle stages.
	FSS.C.R-1.3	Do not provide flight termination commands before clearing the launch center protected area.
	FSS.C.R-1.4	Provide flight termination command when real-time data indicate that the performance of the launch vehicle is erratic causing the vehicle to deviate from intended route.
	FSS.C.R-1.5	Provide flight termination command when the vehicle trajectory is unknown no later than the expiration of the data-loss flight time for the point in flight that the data was lost.


FLIGHT SAFETY SYSTEMS
Regulatory Agencies
Industrial Associations
Insurance Companies
Standards
Regulations
Legal Penalties
Change Reports
Accidents and Incidents
Operations reports
Status Reports
Risk Assessments
Incident Reports
Launch Management
Safety Policy
Standards
Resources
Operators
Launch Vehicle
(Project Managment)
Safety Policy
Standards
Resources
Problem Reports
Operations Reports
Launch Center
(Operations Management)
Policy Standards
Safety Standards
Safety Constrains
Test Requirements
Work Procedures
Audits/Inspections
Hazard Analysis
Progress Reports
Test Reports
Documentation
Design Rationale
Safety Reports
Operational Standards
Safety Standards
Work Instructions
Operating Procedures
Audits/Inspections
Operations Reports
Problem Reports
Incidents
Operational Changes Request
Launch Operation Process
Launch Vehicle
Project/Design/Manufacturing
Vehicle FTS
GPS
Radar
Transponder
Telemetry
Transmiter
Other Vehicle
Subsystems
Provide Vehicle
Software Revisions
Operating Procedures
Problem Reports
Incidents
Change Requests
Flight Safety Operation
Launch Rail Set
Safety Zone
FTS Operation
Vehicle Route
Controled Process
Working Instructions
Operating Procedures
Problem Reports
Termination
Command
FTS Controller
FTS Operator
(Human Controller)
Flight Termination Unit
(Autonomous FTS)
Vehicle Trajectory
Ground Antenna or
Onboard Actuators
Vehicle Sensors
Flight Termination Signal
Vehicle FTS
Radar Transponder
Telemetry Data
GPS Position
Other Ground
Support
Subsystems
Operations
Trajectory
Prediction
Radar
Tracking
Telemetry
Receiver

UCA – STPA applied to Flight Safety Systems

07 UCAs related with FTS Operator responsibilities to provide Termination Commands

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Command the Flight Termination from FTS Operator (Ground Systems) or Flight Termination Unit (Autonomous FTS)	**FSS.UCA-1**: FTS Operator or Flight Termination Unit does not provide Termination Command when the vehicle is out of the intended route. [H-1] **FSS.UCA-2**: FTS Operator or Flight Termination Unit does not provide Termination Command when the trajectory is unknown by the data-loss flight time for the point in flight that the data was lost. [H-1]	**FSS.UCA-3**: FTS Operator or Flight Termination Unit provides Termination Command when the vehicle is still on intended route and the trajectory is available. [H-2] **FSS.UCA-4**: FTS Operator or Flight Termination Unit provides Termination Command when the vehicle is still on ground and no vehicle stages had ignited. [H-3] **FSS.UCA-5**: FTS Operator or Flight Termination Unit provides Termination Command after launch, but before clearing the launch center protected area. [H-4]	**FSS.UCA-6**: FTS Operator or Flight Termination Unit provides Termination Command too late when the vehicle had already violated the prescribed flight safety limits. [H-1] **FSS.UCA-7**: FTS Operator or Flight Termination Unit provides Termination Command too early when the vehicle was not yet out of route. [H-2]	N/A

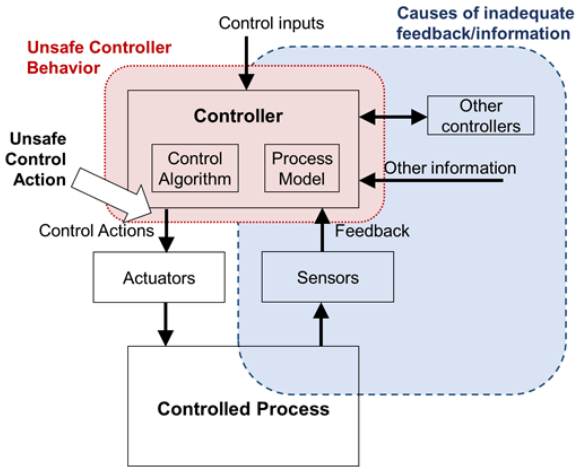
Loss Scenarios – STPA applied to Flight Safety Systems

a) Why would Unsafe Control Actions occur, leading to hazards?

Suppose that **FSS.UCA-4** was provided by the controller:

- What are the causal factors that make the termination command to be provided by FTS Operator or Flight Termination Unit when the vehicle is still on ground?

(04 Loss Scenarios identified related with UCA-4)

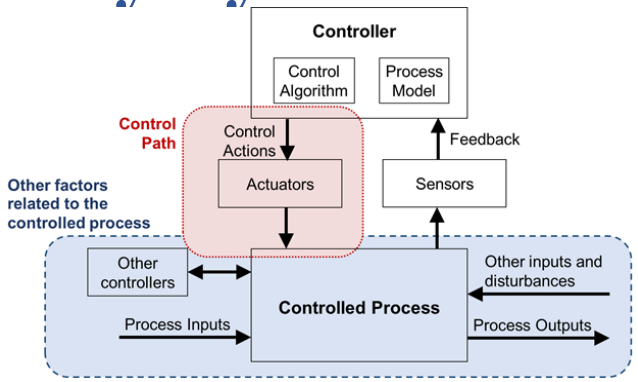


Loss Scenarios	Associated Causal Factors	Rationales
[Operational commands] **FSS.LS-21:** FTS Operator executes procedural actions that result in unintended termination command.	• Wrong or unclear flight termination procedures. • Lack of operational training.	• Simulations and tests can validate the system. • FTS Operator needs proper training.
[Incorrect information provided – vehicle destruction] **FSS.LS-23:** The FTS Operator or Flight Termination Unit receives wrong internal data, informing the vehicle was ignited or exploded on ground.	Malfunctions at: vehicle sensors; vehicle transmitters; ground systems; data processing; communication data. Incompatibility between Ground and Flight Systems.	• Appropriate transmission and receiving systems aligned with onboard and ground sensors can avoid miss-information concerning vehicle status. • Onboard and ground systems need to be compatible.

Loss Scenarios – STPA applied to Flight Safety Systems

b) Why would control actions be improperly executed or not executed, leading to hazards?

- What are the causal factors that make other components to execute a termination command if neither FTS Operator (Ground commanded FTS) nor Flight Termination Unit (Autonomous FTS) sent it?



(11 Loss Scenarios identified)

Loss Scenarios	Associated Causal Factors	Rationales
[Process model inconsistent, incomplete or incorrect – execution of termination command] **FSS.LS-36:** Current state of the process model to execute a termination command is inconsistent, incorrect or incomplete.	• Missing or inaccurate steps to execute a termination command. • Inconsistency of process model defined to acquire and execute a termination command provided. • Incapability of ground or onboard systems to transmit and effectively apply a termination command.	• Consistency between Process model and system status can avoid miss-information concerning vehicle position and public risks. • Functional tests can avoid \operational failures.
[External interference – vehicle termination mechanism or Flight Termination Unit] **FSS.LS-54:** Vehicle termination mechanism receives a termination signal, non-issued by FTS Operator neither by Flight Termination Unit, and the execute the Flight Termination.	• Termination Signal intentionally sent by an external source. • Malfunction at Vehicle FTS termination mechanism, not identifying the Termination Signal was not sent from the FTS Operator neither from Flight Termination Unit (in case of autonomous FTS).	• Systems design, simulations and tests can avoid interferences and susceptibility to external control actions.

Safety Recommendations for Flight Safety Systems

Once identified the loss scenarios, **it is possible to associate safety recommendations (known as safety constraints in STPA approach, that can also be interpreted as requirements for system behavior) to avoid the occurrence of the identified loss scenarios or even to mitigate their consequences**.

Associated with the 54 loss scenarios identified for Flight Safety Systems, **this work proposes 80 safety recommendations, allocating to those responsible for the execution and relating to corresponding requirements** for Launch Safety from FAA – 14 CFR Part 450, Wallops Flight Facility Range Safety Manual and ISO 14620-3:2021.

Safety Recommendations	Related Requirements	Allocated To	Associated LS
[FTS Operator training to command flight termination] **FSS.SR–23**: The FTS Operator shall be trained to appropriately perform functional and operational responsibilities, providing termination commands only when it is necessary, according to the mission and public risks associated.	ISO 14620-3:2021 - Space systems — Safety requirements — Part 3 § 450.149 Safety-critical personnel qualifications.	Launch Center Management, FTS Operators and Testers	FSS.LS-15 FSS.LS-21 FSS.LS-45

Safety Recommendations for Flight Safety Systems

Safety Recommendations	Related Requirements	Allocated To	Associated LS
[FTS Operator training to command flight termination] **FSS.SR–23**: The FTS Operator shall be trained to appropriately perform functional and operational responsibilities, providing termination commands only when it is necessary, according to the mission and public risks associated.	ISO 14620-3:2021 - Space systems — Safety requirements — Part 3: Flight safety systems • Personnel Training • Training of Safety Operators Personnel at the position of Safety Operator shall receive a specific training before taking up their duties. The required training shall be based on the level of responsibility and the actions to be performed. This training must be completed by exercises to simulate normal and degraded situations, with the application of intervention measures.	Launch Center Management, FTS Operators and Testers	**FSS.LS-15:** FTS Operator execute actions that do not result in termination command. **FSS.LS-21:** FTS Operator execute actions that results in unintended termination command. **FSS.LS-45**: FTS Operator issues an incorrect and unsafe control action.

Safety Recommendations for Flight Safety Systems

Safety Recommendations	Related Requirements	Allocated To	Associated LS
[FTS Operator training to command flight termination] **FSS.SR–23**: The FTS Operator shall be trained to appropriately perform functional and operational responsibilities, providing termination commands only when it is necessary, according to the mission and public risks associated.	**§ 450.149 Safety-critical personnel qualifications.** (a) ***General.*** An operator must ensure safety-critical personnel are trained, qualified, and capable of performing their safety-critical tasks, and that their training is current. (b) ***Application requirements.*** An applicant must— (1) Identify safety-critical tasks that require qualified personnel; (2) Provide internal training and currency requirements, completion standards, or any other means of demonstrating compliance with the requirements of this section; and (3) Describe the process for tracking training currency.	Launch Center Management, FTS Operators and Testers	**FSS.LS-15:** FTS Operator execute actions that do not result in termination command. **FSS.LS-21:** FTS Operator execute actions that results in unintended termination command. **FSS.LS-45**: FTS Operator issues an incorrect and unsafe control action.

Safety Recommendations for Flight Safety Systems

Safety Recommendations	Related Requirements	Allocated To	Associated LS
[Vehicle Sensor and transmitters reliability] **FSS.SR–33**: The reliability of vehicle sensors and transmitters shall be verified and validated.	ISO 14620-3:2021 - Space systems — Safety requirements — Part 3: Flight safety systems • Trajectory control system requirements • Requirements (…) **the reliability of the transponder system and space-based system, such as GPS, shall not be less than 0.995 at 95% certainty level and the reliability of the ground equipment shall be compatible with the flight hardware**. These reliabilities shall be established by analysis of all support test data and component test data. • Telemetry data transmitter system requirements • Requirements (…) **the reliability of the telemetry data transmission system shall not be less than 0.995 at 95% certainty level** and This reliability shall be established by analysis of all support test data and component test data.	Reliability engineers, Design Team, Testers and Operators	**FSS.LS-19:** Vehicle cannot transmit the status of the vehicle Trajectory. **FSS.LS-20:** Vehicle sensors unable to obtain trajectory data.

Safety Recommendations for Flight Safety Systems

Safety Recommendations	Related Requirements	Allocated To	Associated LS
[Vehicle FTS reliability] **FSS.SR–57**: The reliability of Vehicle FTS shall be verified and validated.	AC 450.108-1 10.5. **Consideration of FSS Reliability**. (…) Thus, the outcomes of malfunction flight where the FSS fails should be included in the residual risk, with a conditional probability of one minus the reliability of the FSS. FAA - 14 CFR Part 417: **§417.309** Flight safety system analysis. **(b)** System reliability. Each **flight termination system and command control system** must undergo an analysis that demonstrates the system's predicted reliability. Each analysis must: **(2)** Demonstrate that **each system satisfies the predicted reliability requirement of 0.999 at the 95 percent confidence level**. Technical Regulations for Launch and Flight Safety [32]: **4.2** Flight Termination Systems Requirements **4.2.1** General: The reliability of Flight equipment of FTS shall not be less than 0.999 at 95% certainty level.	Reliability engineers, Design Team, Testers and Operators	**FSS.LS-39:** FTU cannot act (send Termination Signal to termination mechanism) to complete the execution of the Control Action. **FSS.LS-40:** Vehicle termination mechanism cannot act (terminating the flight) to execute the Control Action.

Safety Recommendations for Flight Safety Systems

Safety Recommendations	Related Requirements	Allocated To	Associated LS
[FTS Operator time delays] **FSS.SR–42**: The amount of time for decision of the FTS Operator and the reaction time shall be accounted for time delay analysis.	FAA - 14 CFR Part 450: AC 450.108-1 10.4.4 Safety Officer Decision Duration	Operators	**FSS.LS-32:** Operational delays to take a decision about the Flight Termination and reaction times of FTS Operator.
[Time Delay Analysis – vehicle FTS transmission] **FSS.SR–66**: Time delays of the Vehicle FTS to receive, validate and transmit the Termination Command, including also delays associated with the related hardware and software, shall be accounted at time delay analysis, and considered for flight termination decision procedure.	FAA - 14 CFR Part 450: AC 450.108-1 10.4 Consideration of Time Delay 10.4.1 Hardware Delays 10.4.2 Software Delays 10.4.3 Communication Delays	Design Team and Testers	**FSS.LS-42:** The issued control action delays to be enforced by the Flight Termination Unit.

Safety Recommendations for Flight Safety Systems

Safety Recommendations	Related Requirements	Allocated To	Associated LS
[Non-issued termination commands at ground systems] **FSS.SR–75:** Ground Control Systems shall be designed and tested to avoid the provision of incorrect, undesired, or inadvertent termination commands.	FAA - 14 CFR Part 417: - §417.303 (d) - §417.303 (f) Wallops Range Safety Manual: - 4.3.2.7.4 (B) - 4.3.2.7.4 (D) ISO 14620-3:2021 - Space systems — Safety requirements — Part 3	Reliability engineers, Design Team, Simulations and Testers	**FSS.LS-48:** Ground systems transmit a non-issued termination command.
[Prevent from inadvertent initiation of termination mechanisms] **FSS.SR–77:** Vehicle FTS shall be designed and tested to prevent inadvertent initiation of termination mechanisms (electro-explosive devices).	FAA - 14 CFR Part 417: - D417.19 (f) - D417.19 (k) - D417.35 (o) - D417.37 (c) (1) - D417.41 (c)	Reliability engineers, Design Team, Simulations and Testers	**FSS.LS-50:** Vehicle FTS termination mechanism performs a non-issued termination command.

Safety Recommendations for Flight Safety Systems

Safety Recommendations	Related Requirements	Allocated To	Associated LS
SECURITY [Avoid FTS inactivation by external interferences at vehicle FTS] **FSS.SR–74:** Vehicle FTS antenna receiver shall be designed to receive, verify, and transmit to the termination mechanism only the termination commands sent by the FTS Operator through the Launch Center Ground systems. Overcoming interferences from external sources.	FAA - 14 CFR Part 417 [29]: - D417.27 (j) - D417.29 (c) (6) - D417.31 (c) - D417.31 (j) - E417.19 (f) - E417.11 (j)	Design Team, Simulations, and Testers	**FSS.LS-47:** By interferences caused by external sources, the Vehicle FTS antenna receiver (actuator) does not receive or validate termination signals issued by FTS Operator.
SECURITY [Avoid external interferences] **FSS.SR–80:** Vehicle termination mechanism shall be designed not to execute the flight termination if it is not confirmed that the received signal was verified and transmitted by the Flight Termination Unit.	- - -	Design Team, Simulations, and Testers	**FSS.LS-54:** Vehicle termination mechanism receives a termination signal, non-issued by FTS Operator neither by Flight Termination Unit, and the execute the Flight Termination.

Applicability for the Brazilian Aerospace Industry

The results of this STPA will be utilized in practical application for:

- Implement new safety requirements at the Brazilian Space Regulations for Launch (REB-02) from the Brazilian Space Agency (AEB).
- Update the Safety Operational Manual from Alcântara Launch Center (CLA) and Alcantara Space Center (CEA) in order to avoid the loss scenarios identified or mitigate their consequences.
- Review the Evaluation and Acceptance Processes implemented by the Industrial Fostering and Coordination Institute (IFI) for authorize Launch Operations and the testing or flight of space systems.

Improvements to IFI and Brazilian Air Force conducting Launch Evaluation and Acceptance Process (EVAP)

- Implement personnel qualifications/trainings to perform verifications and parallel analyses.
- Increase the amount of qualified personnel.
- Upgrade the computational systems used for the EVAP.
- Review EVAP procedures for adequacy to new Regulations from the Brazilian Space Agency.
- Review internal modal processes and procedures to improve and optimize the analyzes.
- Define deadlines that are expected for the EVAP.
- Define instructions for handling of sensitive information.
- Upgrade the data exchange systems.
- Specify internal trainings for the conduction of EVAP of space systems and operations for launch.

REB 02 and FAA 14 CFR Part 450 – Regulations

- No Security Requirements, even for flight safety systems to be used for flight abort.
- Does not requires redundancies, neither were found single fault tolerance requirements, even for flight safety systems to be used for flight abort.
- No requirements or safety constraints for ground operations during lightning, could result into FTS activation and human injury.
- No requirements for grounding to prevent inadvertent ground ignition by electrical discharge.
- It's not presented the acceptable MoC to determine the safety critical systems and operations.
- There are cases (ex. § 450.143) that are not defined minimun reliability for the safety critical systems.
- REB 02 does not define deadlines that are expected for be delivered the EVAP documentation.
- REB 02 does not define deadlines for AEB processing the EVAP.

Further Analysis

- The analyses of this dissertation can be extended and further detailed by the **identification of loss scenarios and the proposition of safety recommendations for launch vehicle operations and for certification and approval processes.**

- Regarding the **HCS, further analysis can be conducted to segregate them**, resulting in the generation of Hierarchical Control Structures for the **development phase**; for the **activities and preparations** of the operation; for the **control actions and feedbacks necessary during the execution**; and also another HCS for the **activities after** the operation.

- Additionally, the STPA of this study can also be complemented with the **analysis of other control actions presented in the Hierarchical Control Structures, identifying even more UCAs and loss scenarios, finishing with the proposition of safety recommendations**.

- Considering space systems and operations, the **STPA can also be applied to ground support equipment, to space vehicle (payload) operations, in-orbit service, launch approvals process, others launch vehicle systems and similar equipment, system, processes, or operations**.

Conclusions

- Applying STPA for FSS, from the **03 losses** detected, it was identified **04 system-level hazards**, resulting in the proposition of **07 system-level safety constraints**. HCS was modelled based on the **43 responsibilities** that was associated to the main controllers and stakeholders detected. By practical application of the STPA, it was possible to identify **07 UCAs** related to termination commands to be provided by operators (Ground Systems) at human-controlled FTS or from Flight Termination Unit (Onboard System) at autonomous FTS.

- **Based on the 07 UCAs identified for FSS**, it was possible to detect **32 scenarios that can lead to losses**. Considering **conditions when control actions are improperly executed or not executed**, it was possible to detect **other 22 scenarios that could result in losses**. Casual factors and rationales were correlated for each of these 54 loss scenarios.

- Based on the 54 identified loss scenarios, casual factors and rationale; **this study proposes 80 safety recommendations for FSS, correlated with correspondent requirements for Launch Safety,** pointing out **possibilities to** include requirements and **improve current regulations**.

Conclusions

- The results of **this analysis propose possibilities** for launch vehicle developers, certification authorities and launch centers management **to act in order to modify certification/approval processes, acceptance/readiness review evaluations,** operational procedures, design of launch vehicles and/or ground systems **to avoid unsafe actions and undesired system behaviors, or even to mitigate these unsafe actions consequences**.

- The **recommendations obtained can be utilized to improve** space system design, vehicle and ground support equipment productions, launch operations and **launch approval regulations and processes**.

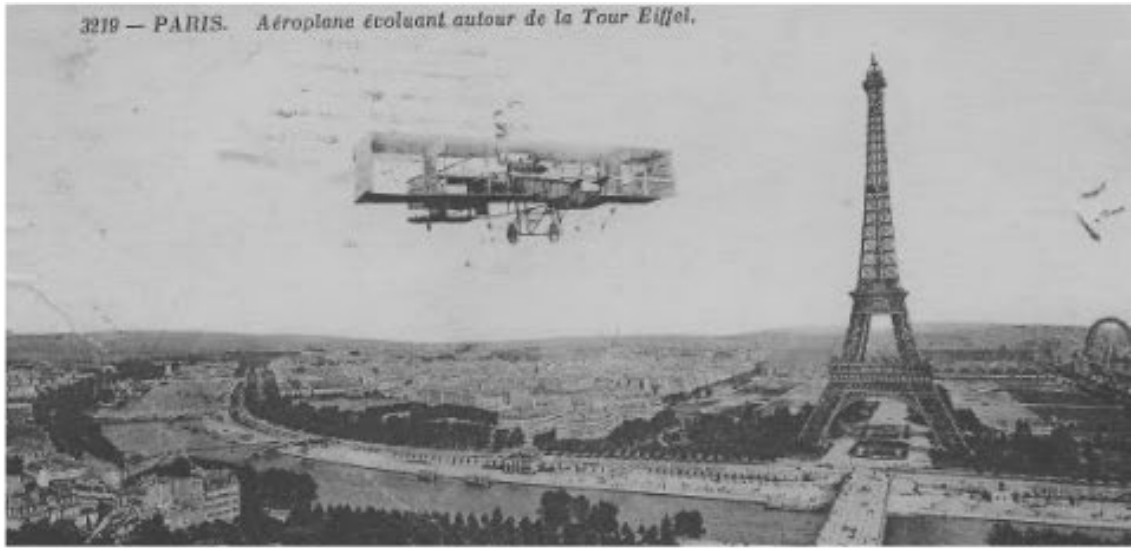
- The analyses of this research **can be extended and further detailed identifying more loss scenarios and safety recommendations; improving the HCS; and applying STPA for other space systems and operations**.

Headlines:

1) Introduction
2) Systemic Factors (Background)
3) System-Theoretic Process Analysis (STPA)
4) STAMP-STPA Results
5) Safety Recommendations for Flight Safety Systems
6) Conclusions

Objective

Identify losses, hazards, safety constraints and unsafe control actions of Flight Safety Systems, detecting loss scenarios, suggesting Regulations/Standards harmonization, and proposing Safety/Security Recommendations to minimize the effects of unsafe events or mitigate their consequences for future Launch 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