Departament of Aerospace Science and Technology

Industrial Fostering and Coordination Institute

Technical University of Munich

Comparison of Hazard Analysis Methods applied to Flight Safety Systems

Capt. Diniz - Dr. Carlos Lahoz
Dra. Chiara Manfletti - Col. Castilho - Capt. Silveira

2024 MIT STAMP Workshop

Objective

The purpose of this analysis is to compare the results obtained from Systems Theoretic Process Analysis (STPA) with the results from the application of Traditional Hazard Analysis Methods regarding Flight Safety Systems for operations with Launch Vehicles.

Headlines:

1) Introduction
2) Systems Theoretic Process Analysis (STPA)
3) Functional Hazard Assessment (FHA)
4) Failure Mode and Effects Analysis (FMEA)
5) Zonal Safety Analysis (ZSA)
6) Fault Tree Analysis (FTA)
7) Hazard and Operability Study (HAZOP)
8) Conclusion

Introduction

Systems safety studies applied to Flight Safety Systems, to be used during launch operations, are strategic because they deal with the preservation of human lives, properties, mission fulfilment, knowledge, and the environment.

The goal of this work is to compare the application and the results obtained from the application of different safety approaches, methods, and techniques to analyze the factors that influence safety in Flight Safety Systems for launch operations.

Criteria for the Comparison of Hazard Analysis Methods

Criteria	Definition
Coverage	The extensiveness and depth of the method in identifying and analyzing potential hazards. High indicates comprehensive analysis of hazards across different system aspects.
Human Factors Analysis	How well the method considers human interactions, actions, errors, and behavior. High means extensive consideration.
Risk Classification	The ability to assess and categorize risks by severity, likelihood, or consequences. High means focus on risk prioritization.
Systems Interactions	The ability to analyze interactions within and between systems. High means thorough analysis of system relationships.
Causality Analysis	The effectiveness in identifying causes of hazardous events. High means strong focus on root causes.
Scenario Analysis	The ability to evaluate different potential scenarios and their impacts. High means comprehensive scenario analysis.
Requirements/ Constraints	The ability to define and assign safety requirements or constraints. High means a systematic approach to implementing constraints or to generate requirements.

High
Medium
Limited
Low

Flight Safety Systems

Flight Systems

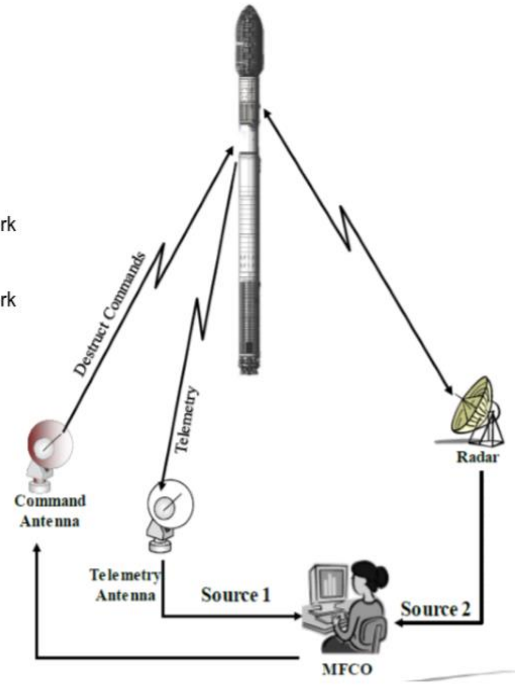
- Flight Termination System
  - Receiver
  - FTS Logic Box
  - Battery
  - UHF Antenna
  - Hybrid Coupler
  - Safe & Arm
  - Ordnance
- Metric Tracking Sources (RCC 324)
  - GPS
  - Telemetry Encoder
  - Telemetry Transmitter
  - S-band Antenna
  - L-band Antenna
  - Couplers
  - Power Distribution Box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



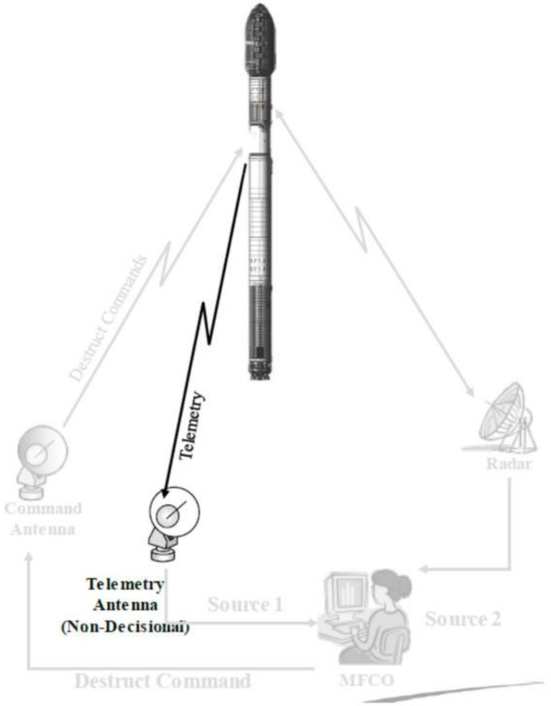
Traditional Flight Termination System (FTS)

Flight Systems

- Metric Tracking Sources (RCC 324)
  - GPS (x3)
  - 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 Flight Termination System (AFTS)

Source: NASA Kennedy Space Center (KSC)

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;

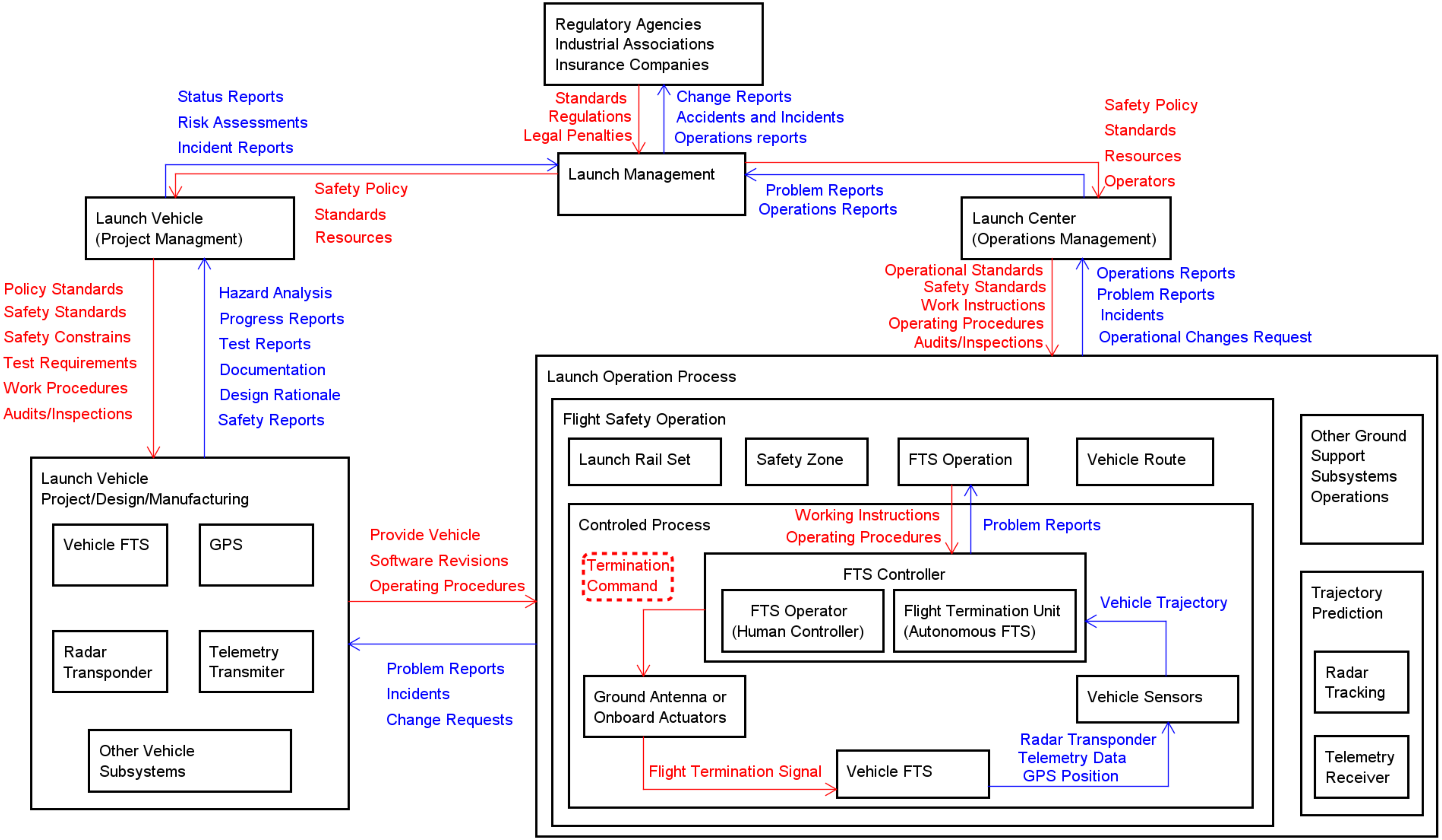
FSS.L-2: Loss of mission; loss or damage to vehicle or payload; and

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]

FLIGHT SAFETY SYSTEMS



Regulatory Agencies
Industrial Associations
Insurance Companies

Standards
Regulations
Legal Penalties

Change Reports
Accidents and Incidents
Operations reports

Launch Management

Status Reports
Risk Assessments
Incident Reports

Safety Policy
Standards
Resources

Launch Vehicle
(Project Managment)

Safety Policy
Standards
Resources
Operators

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 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

Launch Operation Process

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

STPA – Unsafe Control Actions

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 the ground and vehicle stages have not 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

FSS.H-3: FTS activates before launch.

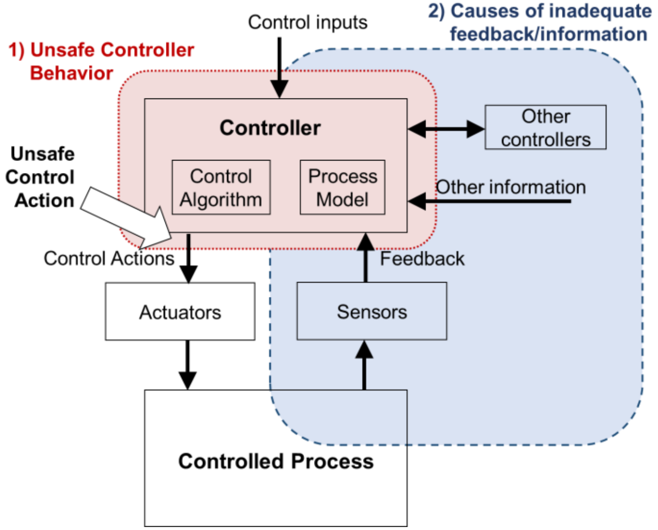
FSS.L-1: Human injury; properties damage; human life or environmental losses;
FSS.L-2: Loss of mission; loss or damage to vehicle or payload; and
FSS.L-3: Loss or damage to launch facilities.

STPA – Loss Scenarios (Partial Results)

a) Why would Unsafe Control Actions occur, leading to hazards? (32 LS)

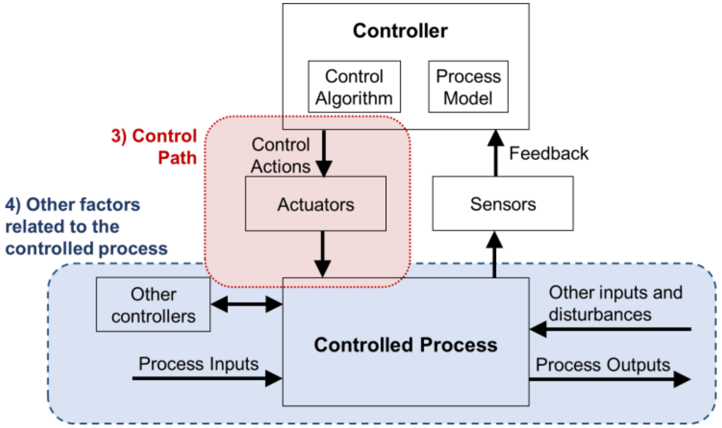
(04 LS identified related with UCA-4)

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. • Inaccurate sensor data. • Lack of operational training.	• Simulations and tests can validate the system. • Sensor redundancies. • FTS Operator needs proper training.



b) Why would control actions be improperly executed or not executed, leading to hazards? (22 LS)

Loss Scenarios	Associated Causal Factors	Rationales
[External interference] **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. • Signal interferences, resulting in the identification of a Termination Signal not sent from the FTS Operator and neither from Flight Termination Unit (in the case of autonomous FTS).	Systems design, simulations and tests can avoid interferences and susceptibility to external control actions.



Functional Hazard Assessment (FHA)

Functional Hazard Assessment (FHA) is a structured approach used to systematically identify and evaluate potential hazards associated with the functions of a system or product. The primary goal of FHA is to ensure that the system or product operates safely under all foreseeable conditions. This analysis typically occurs during the design phase of a system or product's lifecycle.

Process: FHA begins by identifying the functions that the system or product is intended to perform. These functions can range from basic operations to more complex processes.

Identification of Hazards: Once the functions are identified, the next step is to systematically analyze each function to identify potential hazards associated with it. This involves considering various factors such as environmental conditions, operational scenarios, and potential failure modes.

Classification and Evaluation of Hazards: After identifying potential hazards, FHA assesses the severity and likelihood of each hazard occurring. This evaluation helps prioritize hazards based on their potential impact on safety.

Risk Mitigation: Finally, FHA recommends risk mitigation measures to eliminate or reduce the identified hazards to an acceptable level. These measures may include design modifications, procedural changes, or the implementation of safety features.

Functional Hazard Assessment (FHA) – Partial Results

Function	Hazard	Hazard Effect	Severity	Likelihood	Mitigation
Monitor Vehicle Trajectory and Performance	1.1 Incorrect trajectory data due to sensor failure	Vehicle deviates from intended path	Catastrophic	Remote	Redundant sensors, regular calibration, and self-check routines
	1.2 Delayed data processing	Late detection of trajectory deviation	Critical	Occasional	High-speed processors, real-time data processing software
Execute Autonomous Flight Termination	2.1 False trigger of flight termination	Unnecessary destruction of launch vehicle	Catastrophic	Remote	Multiple confirmation checks, manual override option
	2.2 Failure to execute termination command	Vehicle goes out of control, potential safety risk to populated areas	Catastrophic	Remote	Redundant termination systems, periodic system tests
Communicate Status and Commands with Ground Control	3.1 Loss of communication link	Inability to receive commands or send status updates	Critical	Occasional	Redundant communication channels, secure and robust communication protocols
	3.2 Incorrect status information sent to ground control	Ground control makes incorrect decisions based on faulty data	Critical	Remote	Data validation and verification protocols, cross-checks with onboard systems

FHA vs STPA

Criteria	FHA	STPA
Coverage	Medium - Focuses on identifying hazards within a system, analyzing their effects.	High - Offers a broader and more comprehensive analysis of system safety, considering hardware, software, human factors, and environmental aspects.
Systems Interactions	Low - Primarily focuses on hazards within a single system and does not extensively analyze interactions between systems.	High - Examines interactions and dependencies between subsystems and other systems, providing a more holistic view of safety across the entire system.
Requirements/ Constraints	Medium - Can generate safety constraints or propose requirements based on hazard analysis.	High - Actively creates and implements safety constraints to prevent hazards, integrating these constraints into system design and operation, providing a more systematic approach to hazard mitigation.

Failure Mode and Effects Analysis (FMEA)

FMEA is a systematic method for identifying and evaluating potential failure modes of a system, product, or process, along with their potential effects. It involves:

Identification: Recognizing components, functions, and potential failure modes.

Assessment: Evaluating the effects of failure modes on performance, safety, and reliability.

Rating: Assigning severity, occurrence, and detection ratings to prioritize risks.

Risk Prioritization: Calculating a Risk Priority Number (RPN) to focus on critical failure modes.

Mitigation: Implementing actions to address high-priority failure modes, such as design modifications or process improvements.

Documentation and Review: Maintaining records and periodically reviewing and updating the analysis to ensure ongoing effectiveness.

FMEA – Partial Results

Component	Failure Mode	System Effects	Vehicle Effects	S – O – D / RPN	Comments/Mitigation
Vehicle FTS Signal receiver	No Signal Reception	Vehicle FTS will never receive Termination Command.	FTS uncapable to terminate the vehicle.	10 – 3 – 2 60	Vehicle shall has redundancy at FTS antenna reception.
Vehicle FTS Signal receiver	Intermittent	FTS Signal will not be always received.	Vehicle FTS may receive Termination Command when is too late (vehicle already out of Range Safety).	8 – 5 – 4 160	Ground FTS Antenna shall send Termination Command continuously until vehicle termination be determined.
Vehicle FTS Batteries	Battery capacity	Not enough electric charge to activate destruct charges.	FTS uncapable to completely terminate the vehicle.	10 – 3 – 5 150	Vehicle shall has redundancy at FTS batteries.
Ground Vehicle Position Display(s)	Delay to display position data.	Real Vehicle location is different from the presented to FTS Operator.	Vehicle termination command may be sent from operator when is too late (vehicle already out of Range Safety).	4 – 5 – 8 160	Criticality depends of the delays of the system.
Vehicle Position Sensors	Noisy (too many edges)	Calculated vehicle position will not be precise.	FTS Operator will receive not accurate vehicle position.	2 – 5 – 5 50	Criticality will depend of the error at vehicle location provided.
Ground FTS Operator Command Software/ Hardware	Incorrect commands	Ground FTS Software or hardware do not work properly	1) Termination signal send to vehicle without a command from FTS Operator. (Vehicle Loss) 2) Command do not arrive to Ground Antenna. (Public Safety)	8 – 2 – 7 112 10 – 2 – 7 140	Those Vehicle Effects can also be produced by incorrect function of other ground components (as FTS antenna send signal without command or ground cables do not transmit termination signal)

FMEA vs STPA

Criteria	FMEA	STPA
Human Factors Analysis	Low - Typically does not consider human factors directly unless explicitly included in the analysis.	High - Extensively considers human interactions, errors, and behavior within the system, addressing both technical and organizational factors.
Risk Classification	High - Evaluate the severity of potential failure modes and prioritize risks based on a Risk Priority Number (RPN).	Limits risk classification, recognizing its potential oversimplification and danger in complex systems. STPA advocates for a holistic approach to safety analysis, focusing on identifying hazards comprehensively without assigning fixed risk scores.
Systems Interactions	Low - Primarily focuses on functional failures within a single system and does not extensively analyze interactions between systems.	High - Examines interactions and dependencies between subsystems and other systems, providing a more holistic view of safety across the entire system.

Zonal Safety Analysis (ZSA)

ZSA concentrates on identifying and mitigating common cause failures that could impact multiple systems or components within a specific zone. ZSA Process:

- **Define the Zone:** The first step involves clearly defining the area or zone to be analyzed.
- **Identify Systems and Components:** Meticulously identify all the systems and components located within the designated zone.
- **Common Cause Failure Analysis:** Brainstorm and analyze potential events (fire, electrical surge, etc.) that could trigger common cause failures, impacting multiple systems or components within the zone.
- **Evaluate Consequences:** Assess the potential consequences of these common cause failures on system functionality, safety, and personnel.
- **Develop Mitigation Strategies:** Based on the analysis, develop strategies to mitigate the identified common cause failures. These strategies could involve design modifications, improved maintenance procedures, or implementing redundant systems.

Zonal Safety Analysis (ZSA) – Partial Results

Zone	Equipment	Equip. Failure Mode	Vehicle Level Effects	Consequences	Mitigations to Threat the Zone
Sensor Systems	Onboard Sensors	Sensor failure	Incorrect trajectory data	Trajectory deviation	Regular sensor calibration and redundancy in sensor systems
	Data Processing Systems	Data processing delays	Late detection of trajectory deviation	Delayed corrective actions	High-speed processors and real-time data processing algorithms
Flight Termination Systems	Flight Termination Unit	False triggering of flight termination	Unnecessary destruction of launch vehicle	Unnecessary destruction of launch vehicle	Multiple confirmation checks and manual override option
	Vehicle Antenna	FTS will not receive Termination Command	Loss of FTS receiver capabilities	Failure to receive termination command	Redundancy at FTS antenna reception
	Vehicle FTS Signal Receiver	Unable to recognize or receive Ground signals	Flight not terminated	Failure to recognize termination signal	Redundancy at FTS signal reception
	Vehicle Batteries	Not enough electric charge to receive and interpret signals	Loss of FTS receiver capabilities	Insufficient power for FTS operation	Redundancy of FTS Batteries and monitoring of battery health
Comm. Systems	Signal Receivers	Transmission failure	Incorrect data received	Incorrect data reception	Redundant communication channels and robust communication protocols
	Connectors	Connections opened	Loss of communication in one of the vehicle lines	Communication line failure	Redundancy in cable systems and regular inspection
	Electric Cables	Cable rupture	Loss of communication in one of the vehicle lines	Communication line failure	Error detection and correction mechanisms in data transmission

ZSA vs STPA

Criteria	ZSA	STPA
Coverage	Low - Focuses on zonal issues, identifying hazards related to specific functions of a system.	High - Offers a broad and comprehensive analysis of system safety, considering hardware, software, human factors, and environmental aspects.
Systems Interactions	Medium - Considers interactions between different zones and systems to some extent, especially in terms of spatial relationships.	High - Examines interactions and dependencies between subsystems and other systems, providing a holistic view of safety across the entire system.
Scenario Analysis	Limited - Does not typically include detailed scenario analysis. Usually includes suggestions of mitigations measures to threat the zone	High - Considers various scenarios, including normal operations, deviations, and failures, to understand how hazards can arise and how they can be mitigated, providing a comprehensive approach.

Fault Tree Analysis (FTA)

FTA identifies and assesses the probability of specific system failures or hazards, revealing how various events or failures contribute to undesirable outcomes.

Methodology:

- It starts with a top-level undesirable event, then breaks it down into contributing causes using a fault tree diagram with logic gates and basic events.
- Analysts systematically verifies each branch to identify combinations of events leading to the top event.

Techniques:

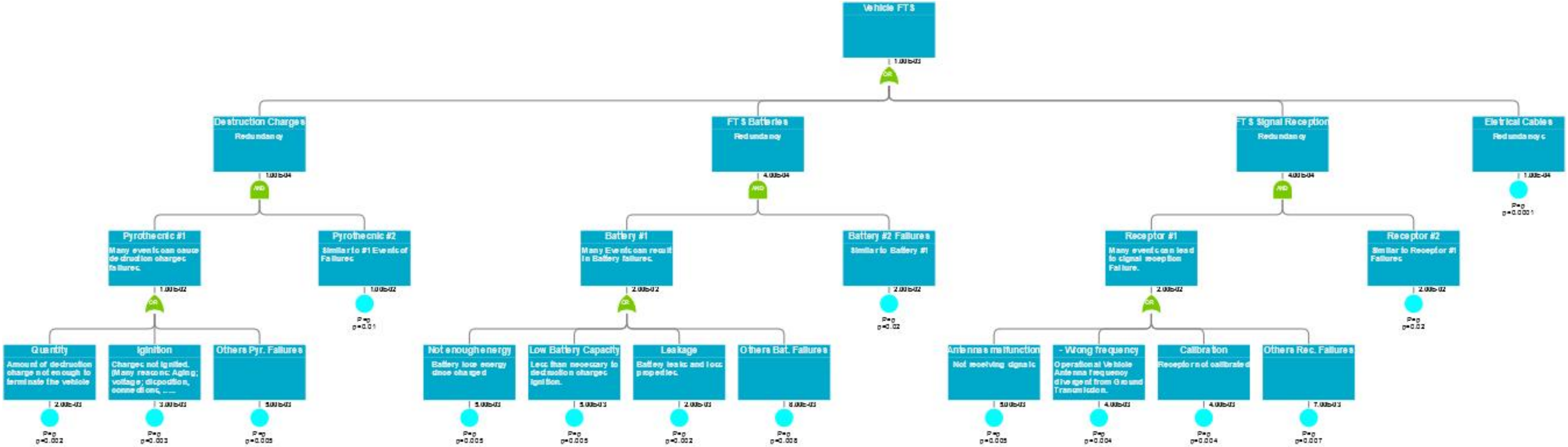
- Data collection via interviews and documentation review.
- May include event tree analysis and quantitative assessment.

Outputs:

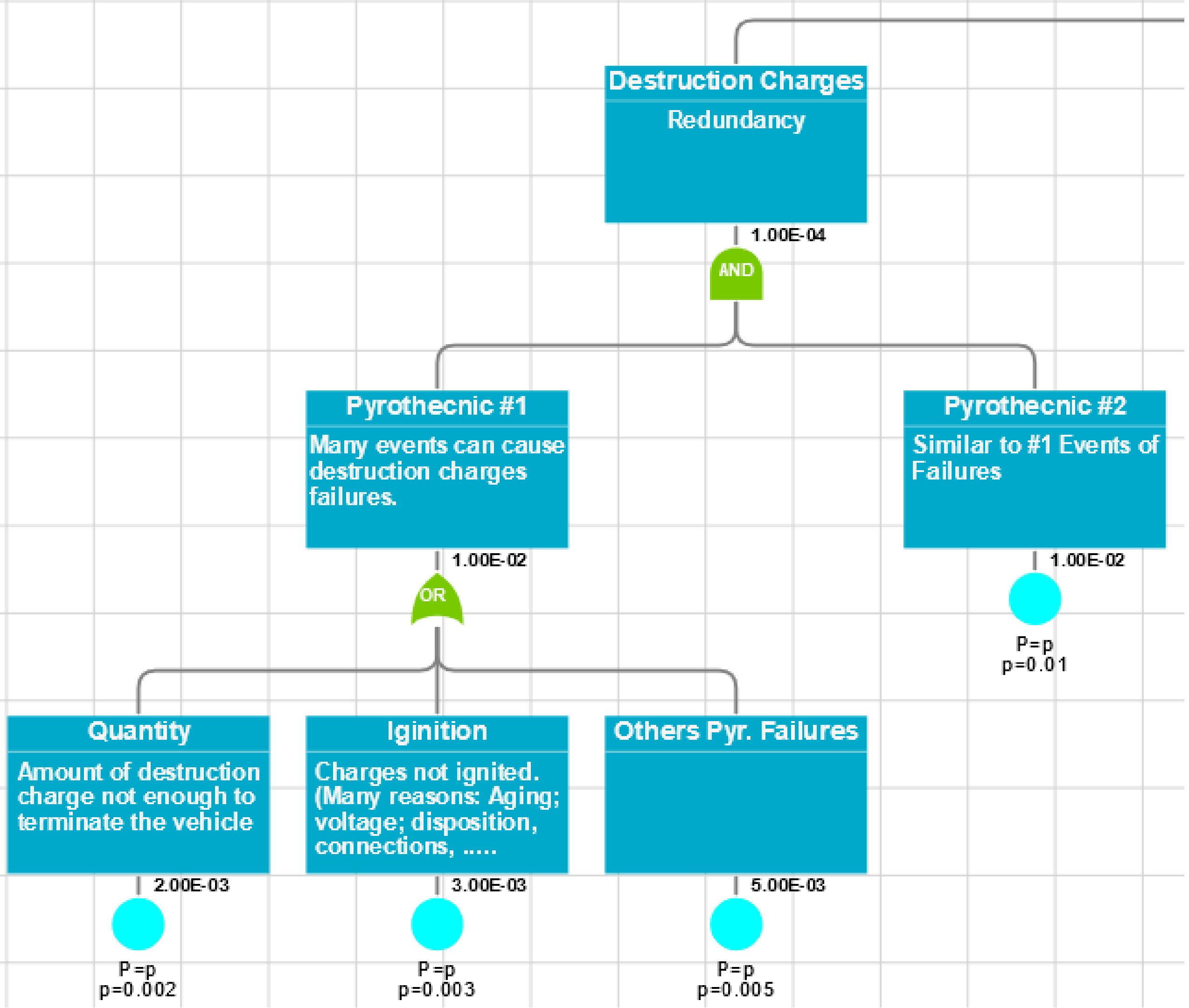
- Provides fault tree diagram showing logical relationships.
- Identifies critical failure paths and may yield quantitative probabilities.

FTA – Vehicle FTS (Partial Results)

FTS is commanded.
However, the flight is not terminated



FTA - Charges


Destruction Charges
Redundancy
1.00E-04
AND
Pyrothecnic #1
Many events can cause destruction charges failures.
1.00E-02
OR
Pyrothecnic #2
Similar to #1 Events of Failures
1.00E-02
P=p
p=0.01
Quantity
Amount of destruction charge not enough to terminate the vehicle
2.00E-03
P=p
p=0.002
Iginition
Charges not ignited. (Many reasons: Aging; voltage; disposition, connections, ...
3.00E-03
P=p
p=0.003
Others Pyr. Failures
5.00E-03
P=p
p=0.005

FTA vs STPA

Criteria	FTA	STPA
Human Factors Analysis	Low - Generally does not consider human factors unless explicitly included in the fault tree.	High - Extensively incorporates human interactions, errors, and behavior, addressing both technical and organizational factors, thus correcting the lack of human factors analysis in FTA.
Risk Classification	High - Can assess the severity of top-level faults and prioritize them based on their likelihood and impact.	Medium - STPA avoids traditional risk prioritization, considering it potentially misleading and advocating for a holistic approach instead. The Risk Classification is provided by STPA during the identification of Loss Scenarios, presenting clearly the consequences instead of assign severity.
Systems Interactions	Low - Focuses on faults within a single system, with limited analysis of intersystem interactions.	High - Examines interactions and dependencies between subsystems and other systems, providing a holistic view of safety across the entire system.

Hazard and Operability Study (HAZOP)

HAZOP is a systematic technique used to identify and assess hazards associated with the operation of a system or process. It involves a multidisciplinary team conducting structured brainstorming sessions to explore potential deviations from the intended operation and their consequences.

Node Identification: HAZOP begins by dividing the system or process into discrete nodes or sections. Each node represents a specific component, subsystem, or operational stage.

Parameter Variation: The HAZOP team needs to systematically vary process parameters (such as pressure, temperature, and flow rate) and examine the potential consequences of each variation. This helps identify deviations from the intended operation that could lead to hazards.

Guideword Application: HAZOP uses a set of predefined guidewords (such as "more," "less," "no," "reverse") to stimulate brainstorming and identify potential deviations. Each guideword prompts the team to consider different types of deviations and their implications.

Documentation and Analysis: Throughout the study, the team documents identified deviations, their causes, and potential consequences. This information is then analyzed to assess the severity of hazards and prioritize risk mitigation measures.

HAZOP – Partial Results

Guide Word	Deviation	Possible Causes	Consequences	Action Required
NO or NOT	No Location Provided to FTS Operator or to Flight Termination Unit	- Antenna failure. - Telemetry system glitch or interference. - Command failure at Ground FTS Antenna.	- Loss of vehicle confirmation, risking public harm. - Vehicle Termination failure, public risk, and potential straying into populated areas.	- Ensure redundancy and regular maintenance of FTS components. - Implement cybersecurity measures and emergency protocols. - Conduct design review, align ground antennas, and establish backup systems. - Perform signal integrity checks, update protocols, and test environmental robustness.
NO or NOT	Not established FTS Communication	- Signal obstruction due to environmental factors. - Ground antenna misalignment. - Ground FTS Antenna failure. - FTS receptor signal recognition. - Signal degradation or loss during transmission. - Faulty termination command protocol.	- Vehicle Termination failure, public risk, and potential straying into populated areas. - Increased risk of uncontrolled vehicle path. - Potential vehicle loss due to unconfirmed termination. - Increased risk of vehicle straying into populated areas. - Increased risk of vehicle straying into populated areas.	- Conduct design review, regular alignment checks, and environmental robustness testing. - Ensure redundancy, production quality assurance, and qualification tests. - Implement backup communication systems and signal integrity tests. - Review and update termination command protocols and ensure signal integrity.
LESS	Less pyrotechnic charges or Less obstructions to the liquid propulsion injection	- Inadequate pyrotechnic charges or obstructions. - Insufficient obstructions in liquid propulsion injection.	- Continued thrust, potential collision, and deviation from intended path. - Increased risk to vehicle and airspace users.	- Conduct design review and quality assurance. - Perform qualification tests, maintenance, and implement additional obstructions as required.

HAZOP – Partial Results

Guide Word	Deviation	Possible Causes	Consequences	Action Required
OTHER THAN	Wrong Vehicle Trajectory provided	- Sensor failure or inaccurate trajectory data. - Software error in trajectory computation.	- Command mismatch with vehicle route, potential collisions, or mission compromise. - Increased collision risk and compromised objectives.	- Conduct ground tests, enhance redundancy, and improve software validation. - Implement real-time verification and calibration protocols.
PART OF	Partial loss of telemetry data	- Signal interference or system failure.	- Incomplete data for termination decisions, risking incorrect commands and safety hazards.	- Ensure redundant telemetry, improve shielding, and conduct system diagnostics.
PART OF	Only part of the FTS destruction charges activates	- Faulty pyrotechnic charges or incomplete commands.	- Incomplete propulsion termination, uncontrolled behavior, and safety risks.	- Conduct comprehensive testing and improve command protocols. - Ensure regular maintenance and replacements.
EARLY	Early termination command	- Operator error or premature transmission. - Faulty timing mechanism.	- Unplanned mission termination, safety hazards, and vehicle loss. - Lack of redundant confirmation steps.	- Provide operator training, review timing mechanisms, and establish redundancies. - Ensure confirmation steps and timing mechanism reviews.
LATE	Late termination command	- Delay in operator decision. - Signal transmission lag.	- Increased risk of vehicle entering restricted airspace. - Delayed response to off-nominal conditions. - Compromised public safety.	- Faster signal transmission methods. - Improved decision-making protocols. - Real-time monitoring enhancements.

HAZOP vs STPA

Criteria	HAZOP	STPA
Human Factors Analysis	Medium - Can include human factors by considering deviations caused by human errors, but it is not focus of the analyses.	High - Extensively incorporates human interactions, errors, and behavior, addressing both technical and organizational factors comprehensively, thus enhancing human factors analysis beyond what HAZOP typically achieves.
Causality Analysis	Medium - Identifies causes of deviations (e.g., equipment failure, human error) and their potential impacts, providing a basic causality analysis.	High - Investigate deeper into the causal factors leading to unsafe states, using a control structure to trace how failures propagate through the system, offering an even more detailed and comprehensive causality analysis.
Requirements/ Constraints	Limited - May suggest design changes or operational controls to address identified hazards but does not systematically generate safety constraints.	High - Actively creates and implements safety constraints to prevent hazards, integrating these constraints into system design and operation, providing a systematic approach to hazard mitigation.

Conclusion

Application of Hazard Analysis Methods to Flight Safety Systems for launch vehicle operations.

- **FMEA** (Failure Modes and Effects Analysis) provides a structured approach for identifying failure modes but may overlook broader system considerations.
- **HAZOP** (Hazard and Operability Study) is effective for identifying process deviations but may lack depth in human factors and systems interactions.
- **FHA** (Functional Hazard Assessment) focuses on functional failures and risk classification, providing insights into system functions.
- **FTA** (Fault Tree Analysis) is suitable for fault and probability analysis but may not capture broader system dynamics.
- **ZSA** (Zonal Safety Analysis) is limited in coverage and may not provide a comprehensive safety assessment.
- **STPA** (System-Theoretic Process Analysis) emerges as the most comprehensive method, excelling in coverage, human factors analysis, systems interactions, causality analysis, scenario analysis, and the ability to assign requirements/constraints. Its systemic approach makes it suitable for complex modern systems.

Comparison summary

Criteria	STPA	FMEA	HAZOP	FHA	FTA	ZSA
Coverage	High	Medium	High	Medium	Medium	Low
Human Factors Analysis	High	Low	Medium	Medium	Low	Limited
Risk Classification	Medium	High	Medium	High	High	Low
Systems Interactions	High	Limited	Limited	Low	Low	Medium
Causality Analysis	High	High	Medium	High	High	Medium
Scenario Analysis	High	Medium	Medium	Low	Medium	Limited
Requirements/Constraints	High	Low	Limited	Medium	Low	Limited

QUESTIONS?

Capt. Diniz – dinizavdm@fab.mil.br
Dr. Carlos Lahoz – carloslahoz@univap.br

LASW - 2nd Latin American STAMP Workshop 2024

September 03-05

https://www1.univap.br/la-stamp-workshop