


STPA-Sec: System-Theoretic Process Analysis for Security - Flight Management System

STAMP Workshop 2017, MIT

Daniel Patrick Pereira, daniel.patrick@embraer.com.br

Celso Massaki Hirata, hirata@ita.br

Rodrigo Martins Pagliares, pagliares@bcc.unifal-mg.edu.br

Francisco Luiz de Lemos flemos@ipen.br

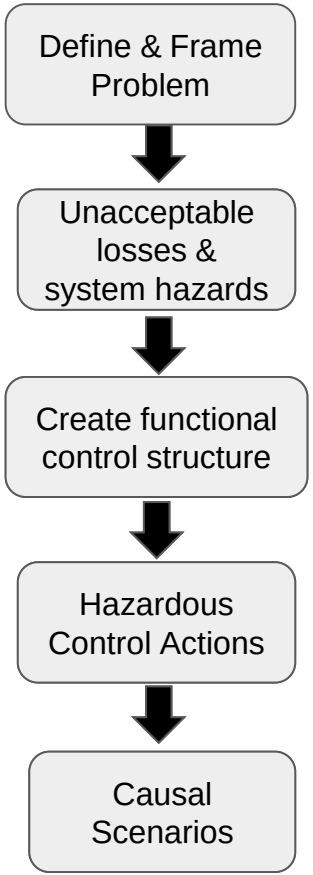
Introduction

- **Motivation**
  - Current **aeronautic standard** (e.g. ED-202A/DO-326A) defines **data requirements** and **compliance objectives** to perform the **airworthiness security process**;
  - The **methods** and **guidelines** that may be used within the **airworthiness security process** are still under development (e.g. DO-356).
    - In addition to that, **ED-202A/DO-326A** considers use of alternative practices.

- **Purpose**
  - The **main purpose** of this work is to present the **application** of **STPA-Sec**, in the aerospace area, for a **F**ictitious **A**irline operating in **B**razil (**FBA**).
  - The system we analyze is a **FMS** (**F**light **M**anagement **S**ystem);

Outline

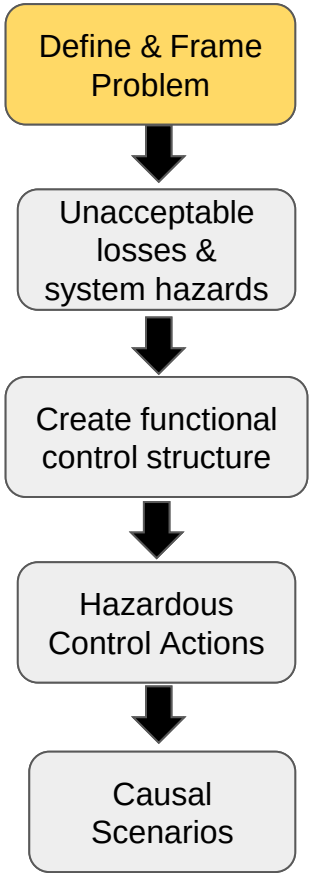
1. **STPA-Sec**
   - Define & frame problem
   - Unacceptable losses & system hazards
   - Create functional control structure
   - Hazardous control actions
   - Causal scenarios
2. **Conclusion**



Outline

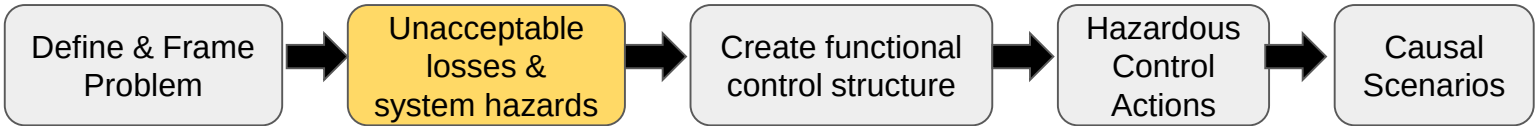
Define & frame problem

- Consists of defining the **scenario** of operation of an **airline**; identifying its **mission** and key **stakeholders**, in addition to defining the **system purpose** and **goal**;
  - **Scenario**: Assure a safe and secure flight. Nowadays there is an increasing risk of cyber-attacks on flight operations, including maintenance. The attacks might be caused by many sources, including terrorism.
  - **Mission**: Valuing and respecting relationships with our customers and, through operational excellence, making our airline their carrier of choice.
  - **Key stakeholders**: Airline, shareholder, passengers.
  - **System purpose and goals**: Civil aviation system to provide secure and safe flight through aircraft maintenance and flight operation in order to support the airline mission.



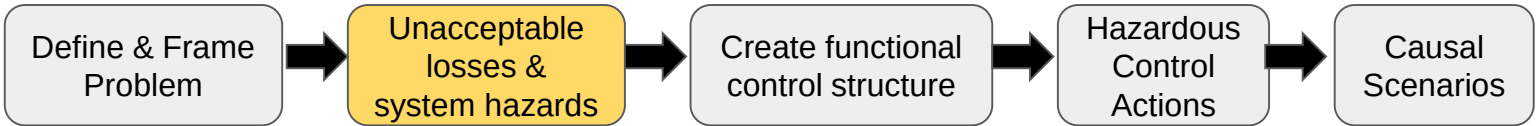
Losses/accidents and Hazards

#ID	Unacceptable losses/accidents
L1	Loss of life/serious injury
L2	Loss of personal identifiable information (PII)
L3	Loss of credibility in the air transportation industry
L4	Mission delay



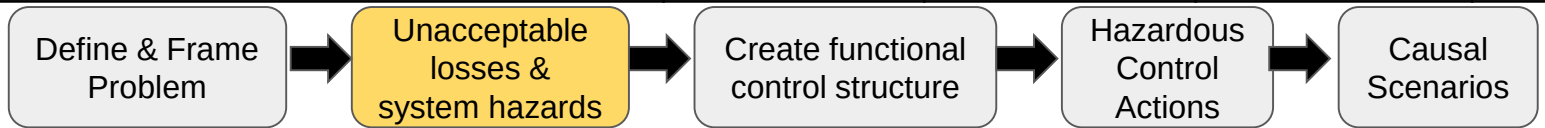
Losses/accidents and Hazards

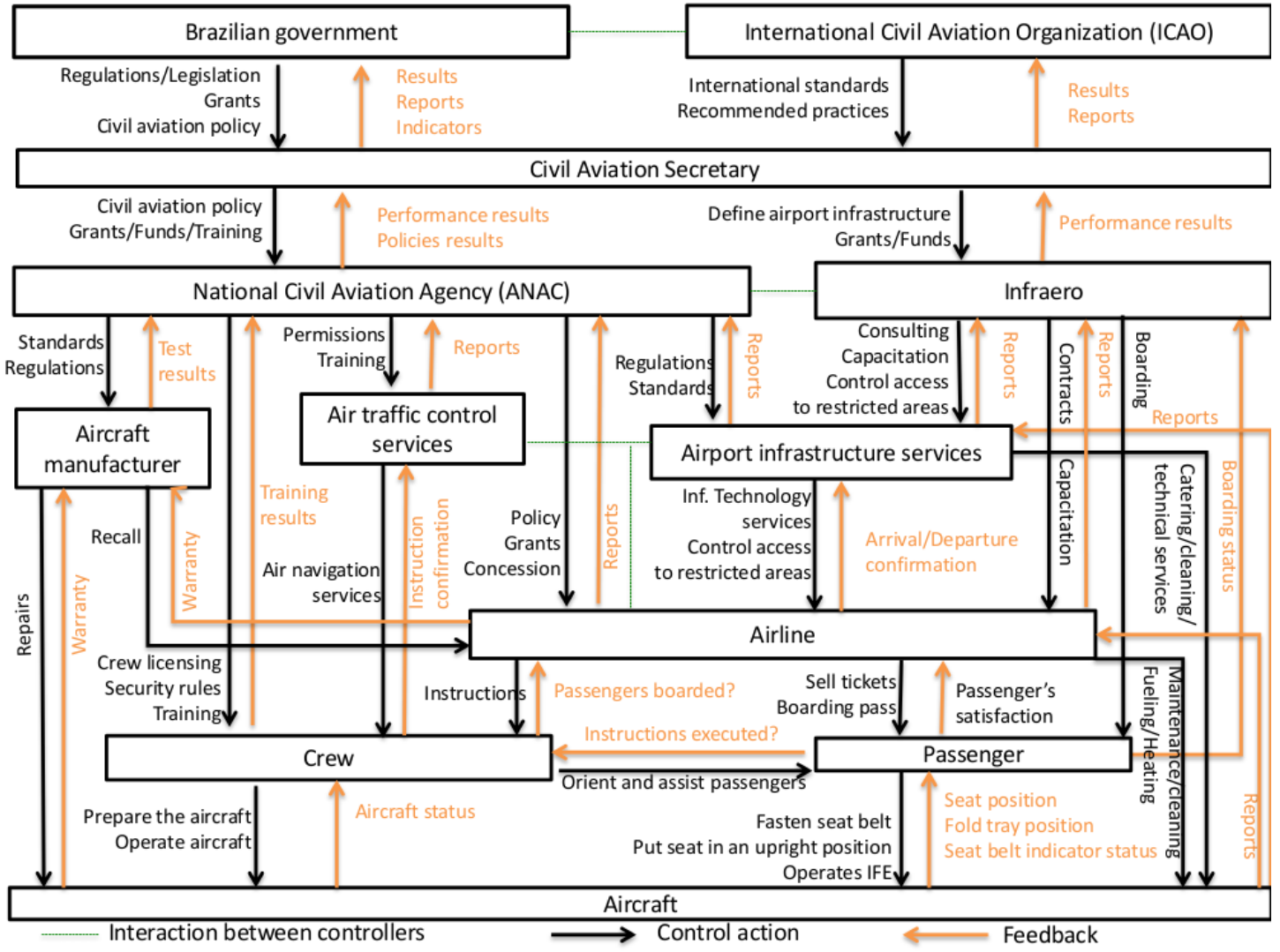
System hazards	System constraints
H1: Violation of minimum/maximum altitude	**SC1**: The flight crew must never violate predetermined minimum/maximum altitude
H2: Violation of minimum distance to other aircraft	**SC2**: The flight crew must never violate the minimum distance to other aircraft
H3: Uncontrolled aircraft	**SC3**: The flight crew must have control of the aircraft all the time.
H4: Aircraft flying off the route specified at flight plan	**SC4**: The aircraft must never fly off the route specified at the flight plan
H5: Unauthorized access to aircraft equipment (electronic and physical)	**SC5**: No access to aircraft equipment (electronic or physical) shall be allowed without authorization
H6: Unable to dispatch aircraft	**SC6**: Aircraft must be dispatched

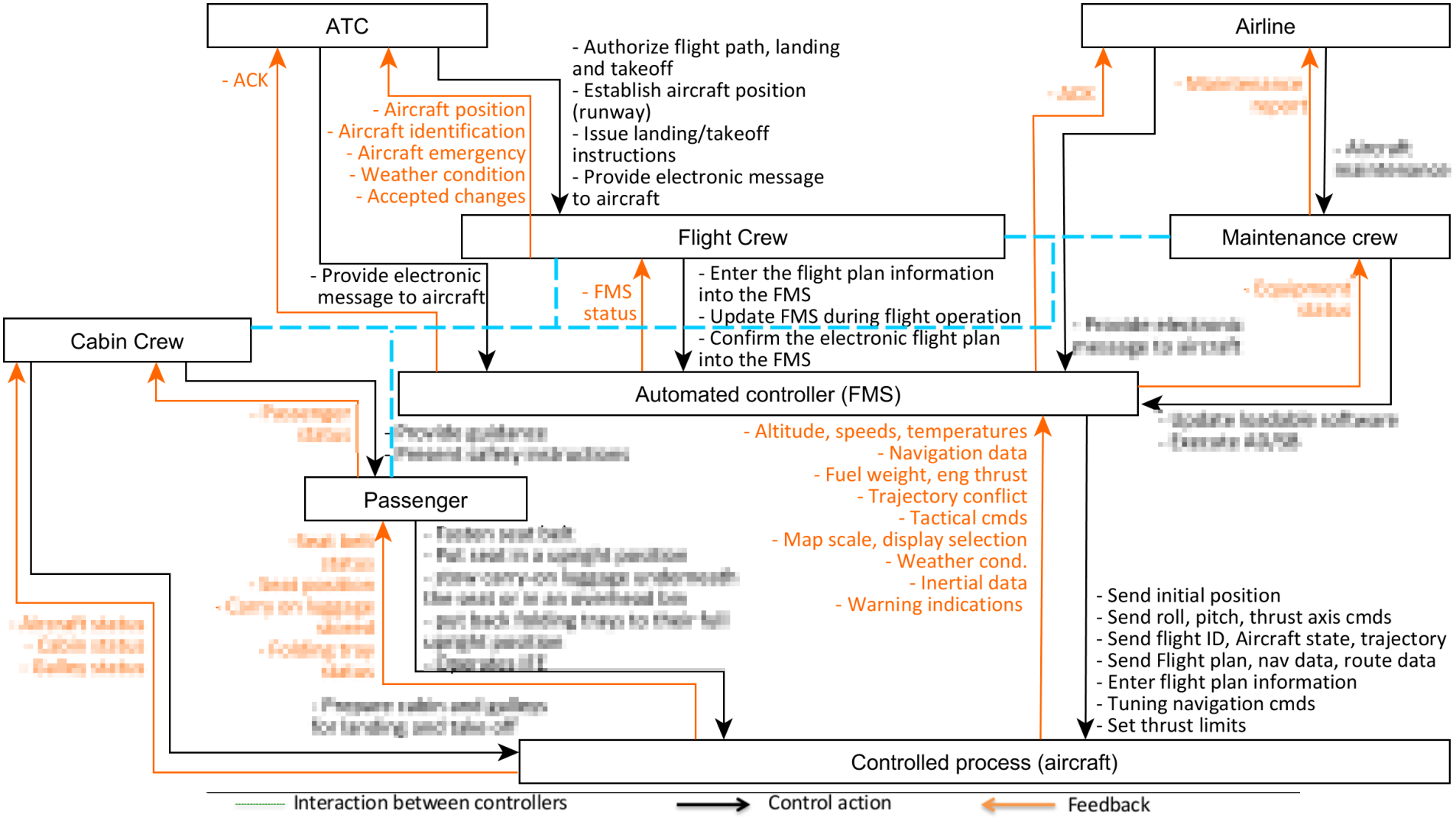


Losses/accidents and Hazards

	L1: Loss of life/serious injury	**L2:** Loss of personal identifiable information (PII)	**L3:** Loss of credibility in the air transportation industry	**L4:** Mission delay
H1: Violation of minimum/maximum altitude	x		x	
H2: Violation of minimum distance to other aircraft	x		x	
H3: Uncontrolled aircraft	x		x	
H4: Aircraft flying off the route specified at flight plan	x		x	
H5: Unauthorized access to aircraft equipment (electronic and physical)	x	x	x	
H6: Unable to dispatch aircraft			x	x




Brazilian government
International Civil Aviation Organization (ICAO)
Regulations/Legislation
Grants
Civil aviation policy
Results
Reports
Indicators
International standards
Recommended practices
Results
Reports
Civil Aviation Secretary
Civil aviation policy
Grants/Funds/Training
Performance results
Policies results
Define airport infrastructure
Grants/Funds
Performance results
National Civil Aviation Agency (ANAC)
Infraero
Standards
Regulations
Test results
Permissions
Training
Reports
Regulations
Standards
Reports
Consulting
Capacitation
Control access
to restricted areas
Reports
Contracts
Reports
Boarding
Reports
Aircraft manufacturer
Air traffic control services
Airport infrastructure services
Training results
Air navigation services
Instruction confirmation
Policy
Grants
Concession
Reports
Inf. Technology services
Control access
to restricted areas
Arrival/Departure confirmation
Capacitation
Catering/cleaning/technical services
Boarding status
Recall
Warranty
Repairs
Warranty
Airline
Crew licensing
Security rules
Training
Instructions
Passengers boarded?
Sell tickets
Boarding pass
Passenger's satisfaction
Maintenance/cleaning
Fueling/Heating
Instructions executed?
Crew
Passenger
Orient and assist passengers
Prepare the aircraft
Operate aircraft
Aircraft status
Fasten seat belt
Put seat in an upright position
Operates IFE
Seat position
Fold tray position
Seat belt indicator status
Reports
Aircraft
Interaction between controllers
Control action
Feedback

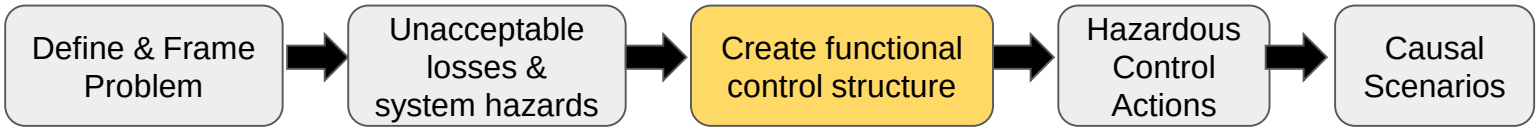

ATC
Airline
- ACK
- Aircraft position
- Aircraft identification
- Aircraft emergency
- Weather condition
- Accepted changes
- Authorize flight path, landing and takeoff
- Establish aircraft position (runway)
- Issue landing/takeoff instructions
- Provide electronic message to aircraft
Flight Crew
Maintenance crew
- Provide electronic message to aircraft
- FMS status
- Enter the flight plan information into the FMS
- Update FMS during flight operation
- Confirm the electronic flight plan into the FMS
Cabin Crew
Automated controller (FMS)
Passenger
- Altitude, speeds, temperatures
- Navigation data
- Fuel weight, eng thrust
- Trajectory conflict
- Tactical cmds
- Map scale, display selection
- Weather cond.
- Inertial data
- Warning indications
- Send initial position
- Send roll, pitch, thrust axis cmds
- Send flight ID, Aircraft state, trajectory
- Send Flight plan, nav data, route data
- Enter flight plan information
- Tuning navigation cmds
- Set thrust limits
Controlled process (aircraft)
Interaction between controllers
Control action
Feedback

Model elements, responsibilities and control actions

Activity: Flight operation		
Element	**Responsibilities**	**Required control actions**

Element	Element	Process Model Variable	Process Model Variable values
Flight crew	Flight crew	FMS status	[Alert, Advisory, Warning, Performance Info, Unknown]
		IsAircraftOn	[Yes, No, Unknown]
		IsFlightPlanPrepared	[Yes, No, Unknown]
		IsFlightCrewCockpit	[Yes, No, Unknown]
		IsFlightPlanReceived	[Yes, No, Unknown]

Model descriptions and variables



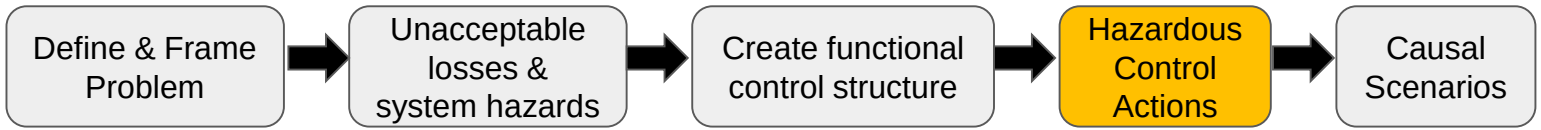
STPA-Sec (Step 1)

Flight crew				
Control actions	**Hazardous Control Actions**			
	Not providing CA causes hazard	**Providing CA causes hazard**	**Providing CA too soon or Applying too long causes hazard**	**Providing CA in the wrong sequence or order (too early/late) causes hazard**
CA01: Enter flight plan information into the FMS	[13] Not providing CA when flight plan information is available **[H6]**	[14] Providing CA when flight plan information is tampered or faked **[H1] [H2] [H3] [H4] [H6]**	[15] Providing CA too late when flight plan information is available [H6]	NA
CA03: Confirm the electronic flight plan into the FMS	[19] Not providing CA when an electronic flight plan is received **[H1] [H2] [H4][H6]**	[20] Providing CA when flight plan is tampered or faked **[H1] [H2] [H4]**.	NA	

H1: Violation of minimum/maximum altitude
H2: Violation of minimum distance to other aircraft
H3: Uncontrolled aircraft
H4: Aircraft flying off the route specified at flight plan
H5: Unauthorized access to aircraft equipment (electronic and physical)
H6: Unable to dispatch aircraft

Security constraints

Hazardous Control Actions	Security Constraints
[13] Not providing “Enter **flight plan** information into the FMS” when flight plan information is available.	**Cockpit crew** must be able to enter flight plan information.
[14] Providing “Enter **flight plan** information into the FMS” when flight plan information is tampered or faked.	**Flight Plan** information must not be tampered or faked.
[15] Providing “Enter **flight plan** information into the FMS” too late when flight plan information is available	**Cockpit crew** must be able to enter flight plan information.
[19] Not providing CA when an electronic flight plan is received.	**Electronic Flight Plan** must be confirmed by Flight Crew.
[20] Providing “Confirm the **electronic flight plan** into the FMS” when flight plan is tampered or faked.	**Electronic Flight Plan** must not be tampered or faked.



STPA-Sec (Step 2)

HCA 19: Flight crew does not provide "**Confirm the electronic flight plan into the FMS**" when an electronic flight plan is received.

Scenarios	**Security Causal Factors**	**D4 Evaluation (Goal impact)**	**Design recommendations**
Ground station (Airline or ATC) is infected by a virus and flight plan confirmation is not received.	10. There is no antivirus in the ground station. 11. Outdated antivirus on ground station computers	**Duration**: Permanent **Extent**: Total (**Destroy**)	All ground station computer should have an updated antivirus installed and at least once a week the antivirus must run in all computers
Ground station (Airline or ATC) is unable to receive a message (ACK) from aircraft due to jammed communication.	12. There is interference/ noise in the communication channel.	**Duration**: Temporary **Extent**: Total (**Deny**)	Communication channel should be able to use different frequencies.
Flight crew cannot confirm the electronic flight plan because FMS is frozen.	13. FMS system has received many requests.	**Duration**: Temporary **Extent**: Total (**Deny**)	FMS system should discard/ ignore many requests according to source, type, timestamp ...

Conclusions

- The application of STPA-Sec, in the aerospace area (FMS), was a good example of its potential to identify design recommendations;
- We identified design recommendations that cover not only the FMS itself but also the ground station (ATC and Airline);
- STPA-Sec shows to be an alternative method to current ED-203/DO-356 implementations;
  - Identification of **security environment** and **security perimeter** is addressed during elaboration of the **functional control structure**;
  - **Security Risk Assessment** activity is covered during Step1 and Step 2 of STPA-Sec.
- Embraer has proposed STPA-Sec as an alternative means of compliance to ED-202A/DO-326A (in progress).