A Systems Approach to the Development of an Aircraft Smoke Control System

Danilo da Costa Ribeiro

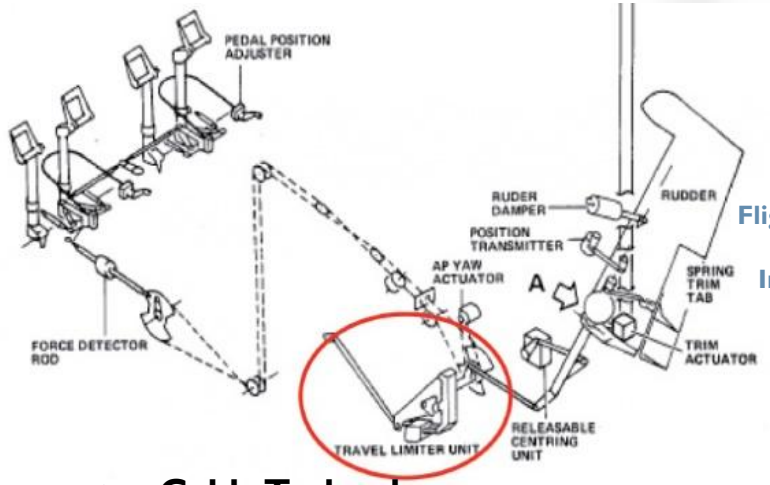
danilo.costa@embraer.com.br

March 2016

Motivation

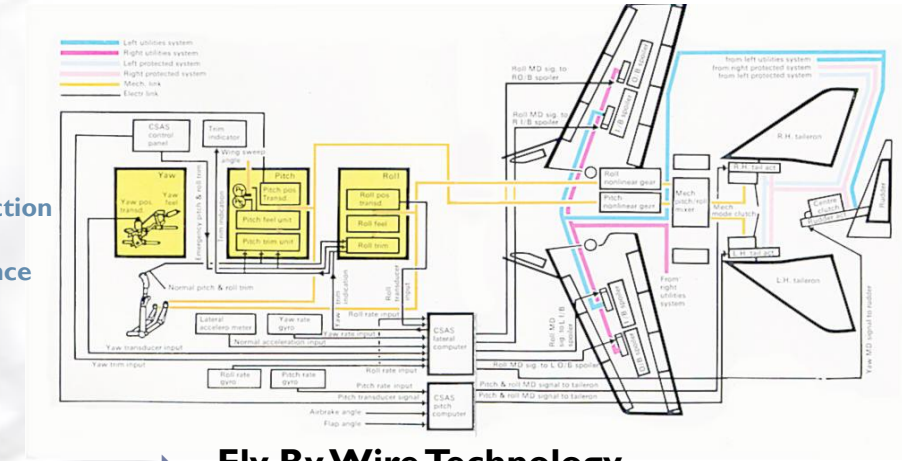
Motivation

- Technology Evolution
  - Flight Control System



- **Cable Technology**
  - **90s**

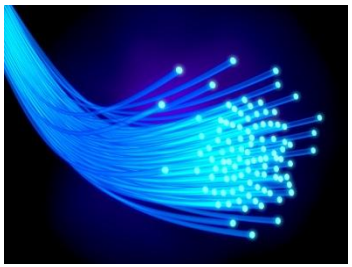
Flight Envelope Protection
Gain scheduling
Improved Performance
Less Weight
(…)



- **Fly By Wire Technology**
  - **2000s**

Flight Envelope Protection
EMI/HIRF shielding
Large bandwith
Less Weight
(…)

Flight By Light Technology

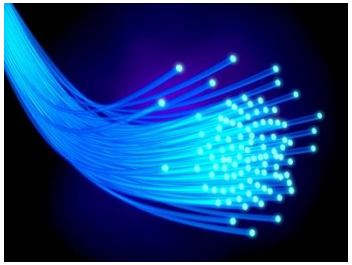


Motivation

- Technology Evolution
  - Flight Control System

Less Time to Market

Flight By Light Technology

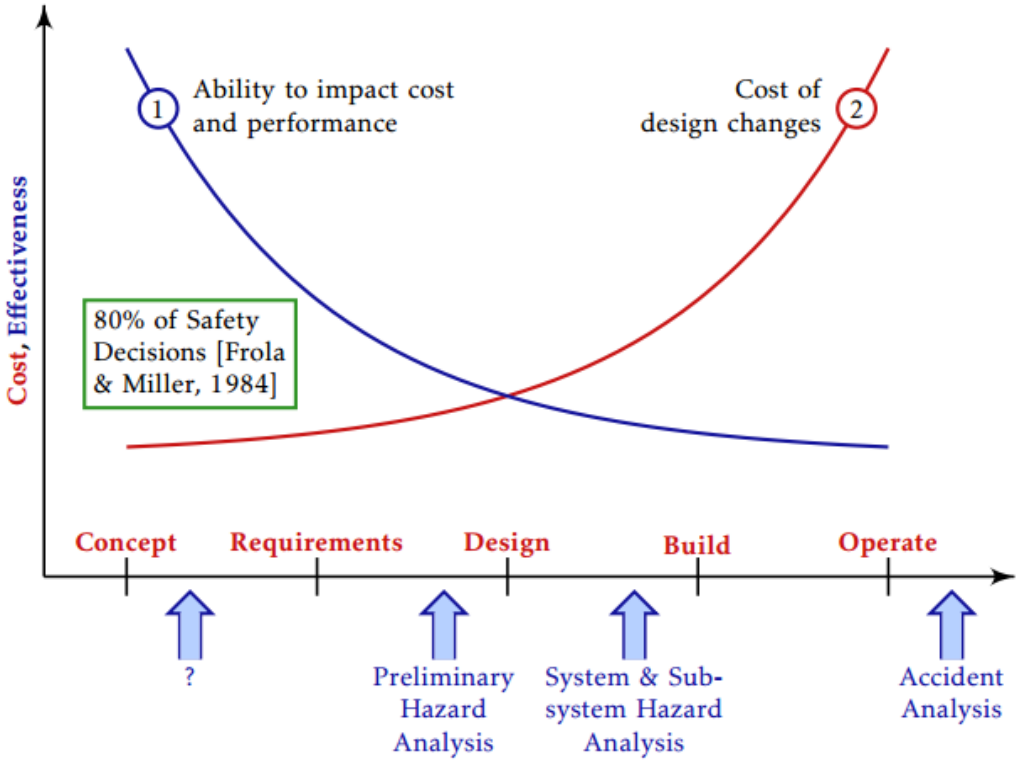


Motivation

- Safety often considered expensive
  - Cost
  - Parameters constraints

Motivation

- Safety often considered expensive
  - Cost
  - Parameters constraints



(Fleming, 2015)

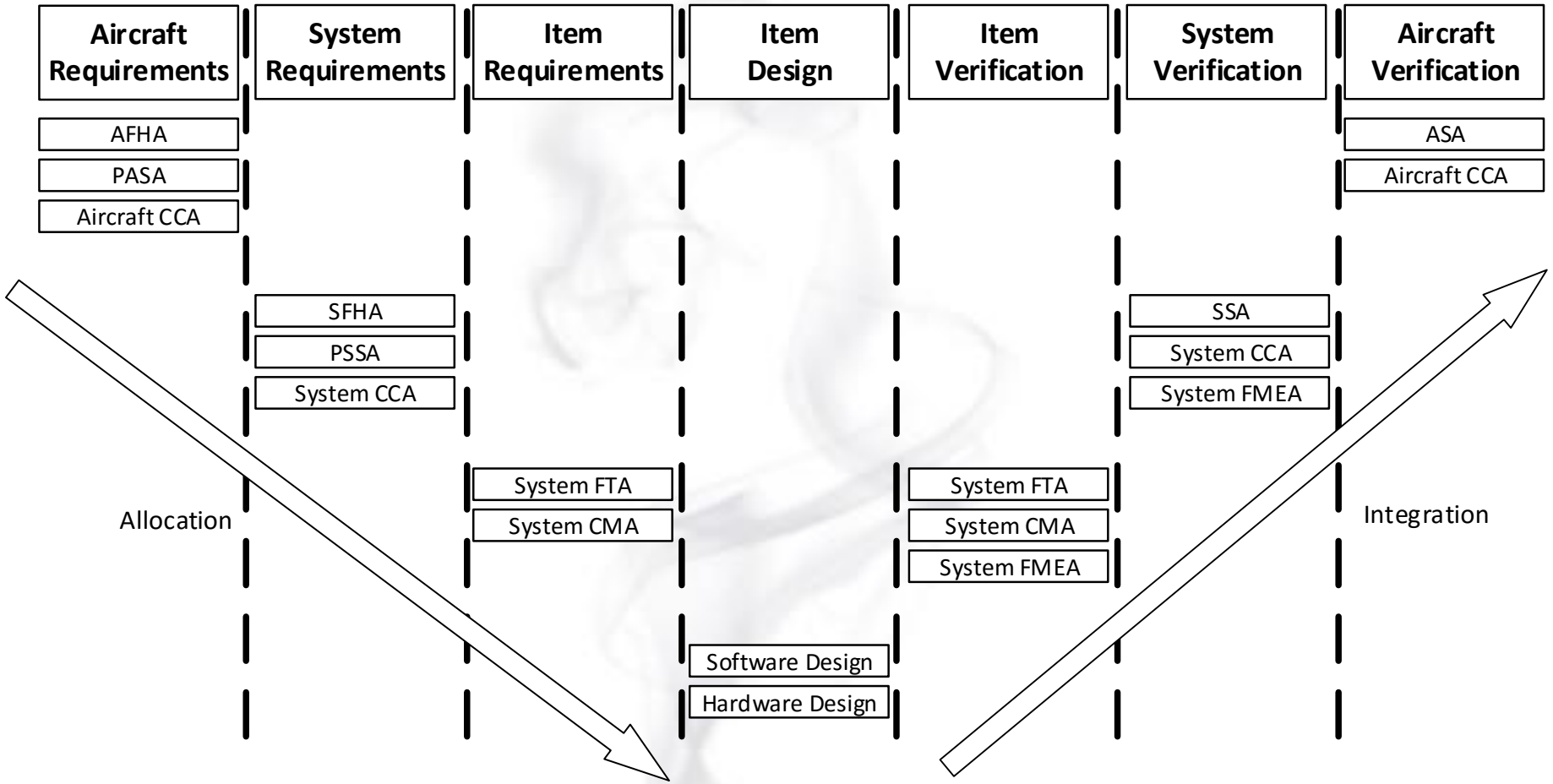
Motivation

- Component Interaction Accidents
  - Increasing with the systems' complexity and integration
  - Not covered by Component Failure Analysis

Motivation

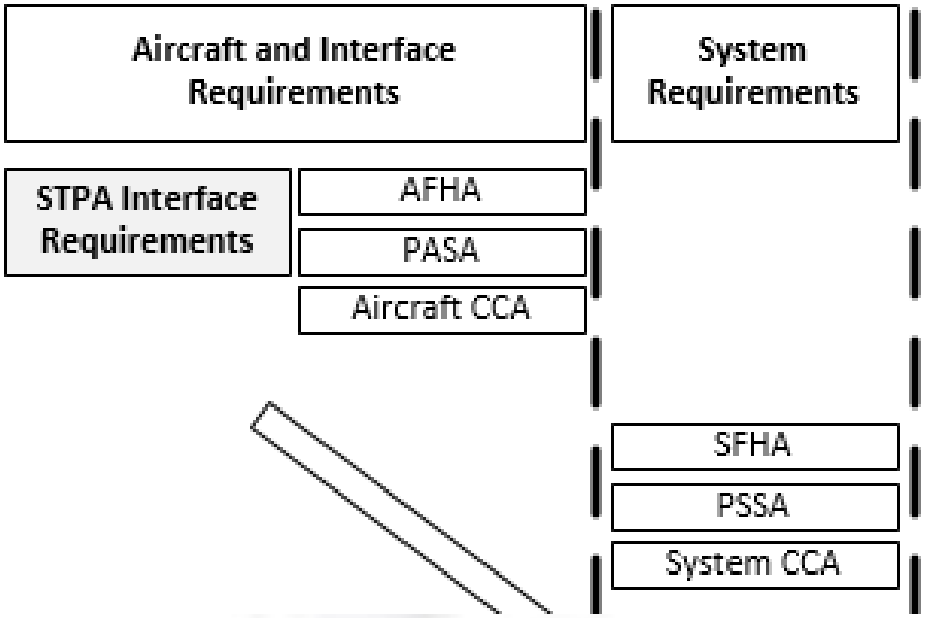
- Traditional Assessment
  - Failure oriented
  - Assess many Interfaces at a later stage
  - Experience plays a significant role
- STPA
  - Function oriented
  - Systemically assess Interfaces at an early stage
  - Experience allied to a systemic process

Motivation



(Adapted from ARP 4754A, 2010)

Motivation



(Adapted from ARP 4754A, 2010)

Complexity

- A “complex system” is a group or organization which is made up of many interacting parts (...) In such systems the individual parts—called “components” or “agents”—and the interactions between them often lead to large-scale behaviors which are not easily predicted from a knowledge only of the behavior of the individual agents. Such collective effects are called “emergent” behaviors.

(Mitchell and Newman, 2002)

Systems Thinking and Safety

Aircraft System

- Avionics (...)
- Electrical System (...)
- Flight Controls (...)
- **AMS**
  - Bleed Control System (...)
  - Ice and Rain Protection (...)
  - **Environmental Control System**
    - **Air Conditioning**
    - **Smoke Control System**
    - **Ventilation**
  - Pressurization System (...)
  - Oxygen System (...)
- Hydromechanics (...)
- Propulsion (...)
- Interior Systems (...)

Complexity

Smoke Control System

- Functions:
  - Detect smoke on board
  - Prevent smoke from entering an occupied zone
  - Prevent fire on board

STPA: Accidents and Hazards

- Accidents
  - A-1 Multiple fatalities
  - A-2 Loss of aircraft
  - A-3 Loss of mission

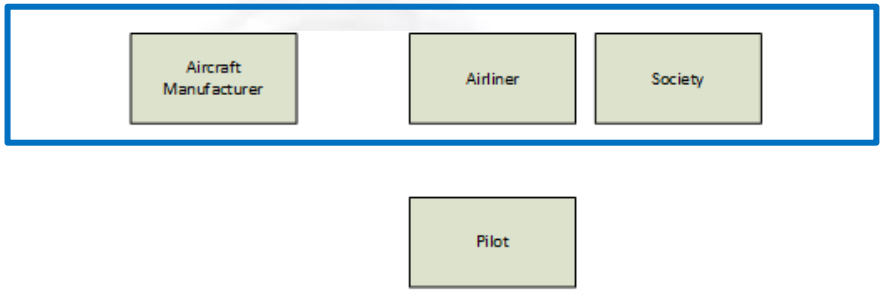
- Hazards

Hazards		Associated Accident
H-1	Smoke inside the cabin	A-1
H-2	Uncontrolled fire on board	A-2
H-3	Unnecessary loss of relevant functions	A-3

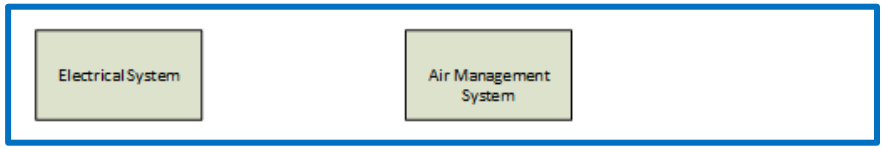
STPA: Level 0 Safety Constraints

- Safety Constraints to avoid Hazards
  - L0-01 - There shall never be smoke inside the cabin
  - L0-02 - There shall never be uncontrolled fire on board
  - L0-03 - No relevant function shall be lost when not required

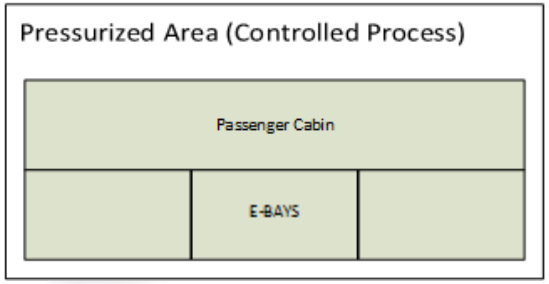
STPA: Functional Control Structure



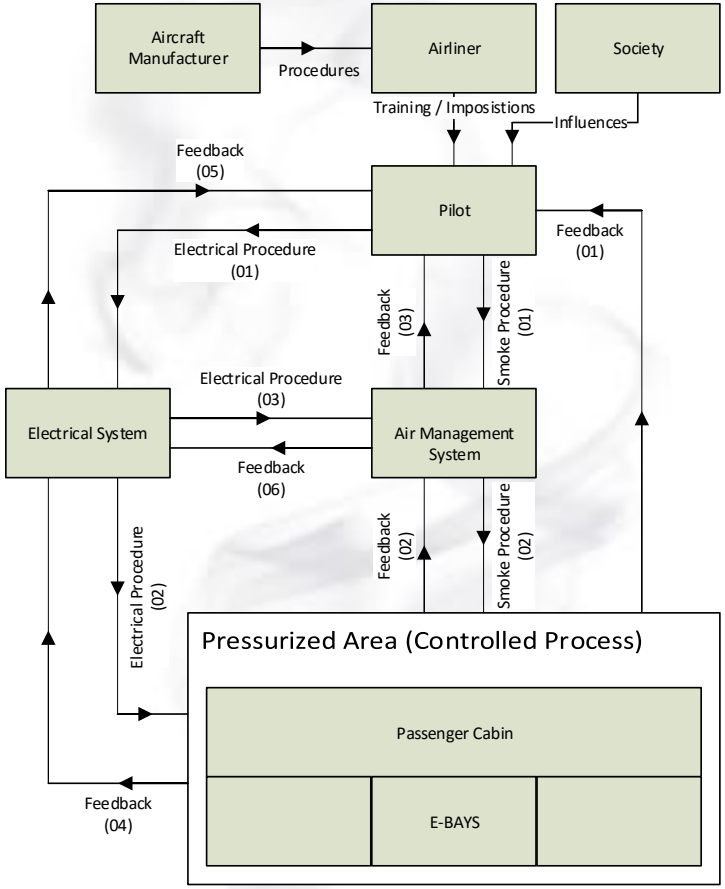
External Inputs



Subsystems



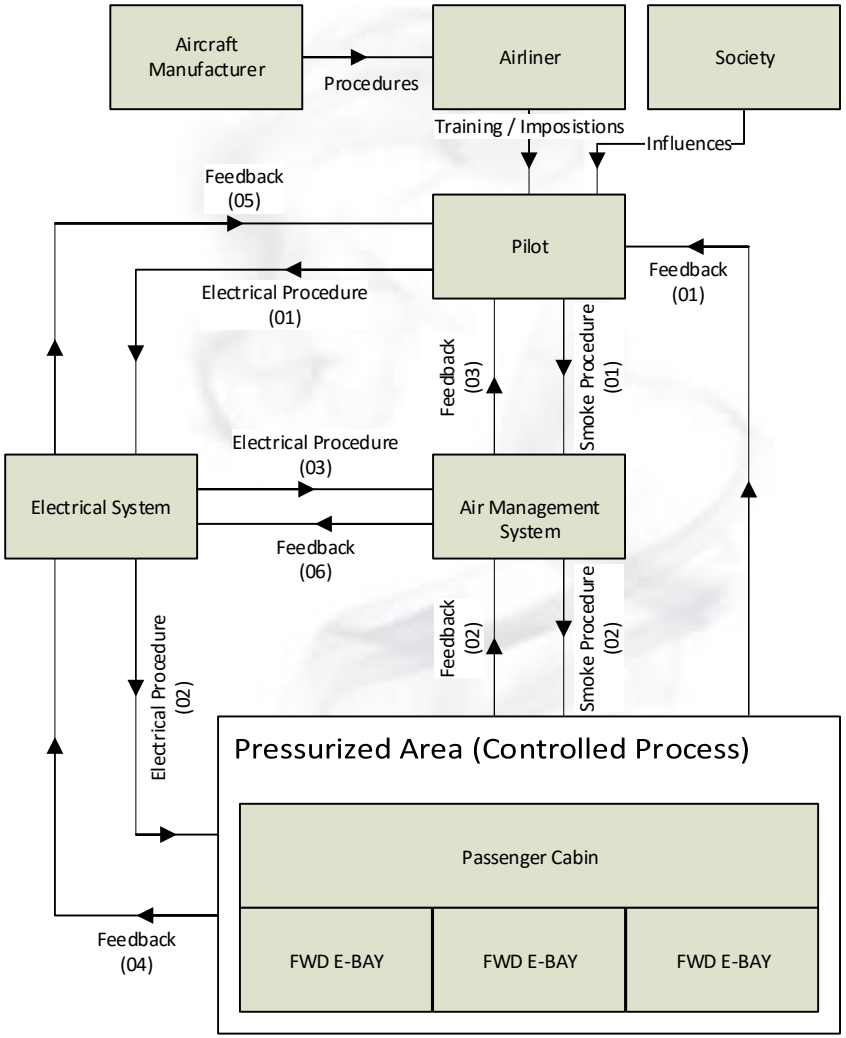
STPA: Functional Control Structure



STPA: Step 01 – Unsafe Control Actions

- According to Leveson, there are four ways for a control action to be hazardous:
  - A safety required control action is not followed.
  - An unsafe control action is provided.
  - A safety required control action is provided too late or too early or out of sequence.
  - A safety required control action is stopped too soon or applied too long.

STPA: Step 01 – Unsafe Control Actions (UCA)



STPA: Step 01 – Unsafe Control Actions (UCA)

Control action	Safe control action not provided	Unsafe control action provided	Wrong timing/order	Stopped too soon or applied too long
Smoke procedure from the Pilot to Air Management System	Smoke procedure not executed in case of smoke on board [UCA21]	Smoke procedure executed when there is no smoke on board [UCA22]	Smoke procedure executed too late [UCA23]	Too soon: smoke procedure not fully executed in case of smoke on board [UCA24]

Accidents		Hazards		Unsafe control actions
A-1	Multiple fatalities	H-1	Smoke inside the cabin	21;23;24
A-3	Loss of mission	H-3	Unnecessary loss of relevant functions	22

STPA: Step 01 – Safety Constraints

- **Safety Constraints to avoid Unsafe Control Actions**
  - L1-04a: The pilot shall execute completely on time the smoke procedure to the AMS (UCA 21, 23 and 24)
  - L1-05a: The pilot shall execute the smoke procedure only when there is smoke on board (UCA 22)

(…)

STPA: Step 02

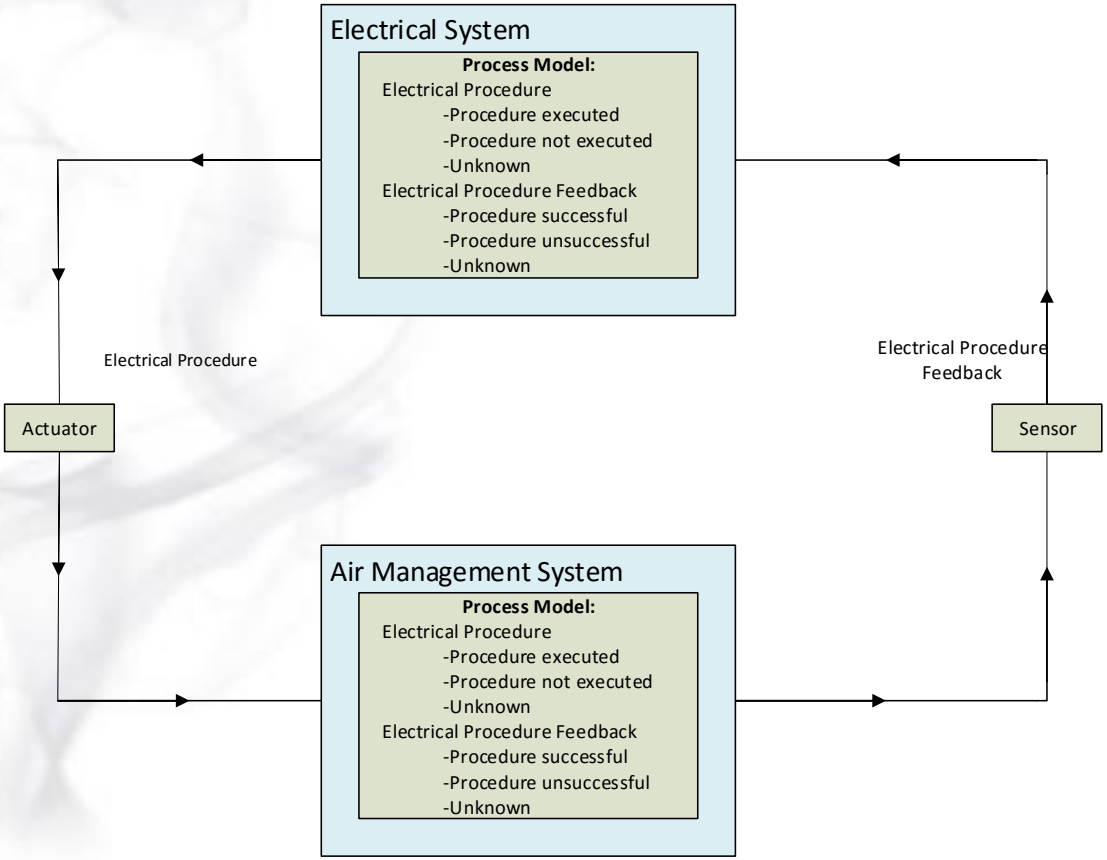
- Causal Factors

- Process Models

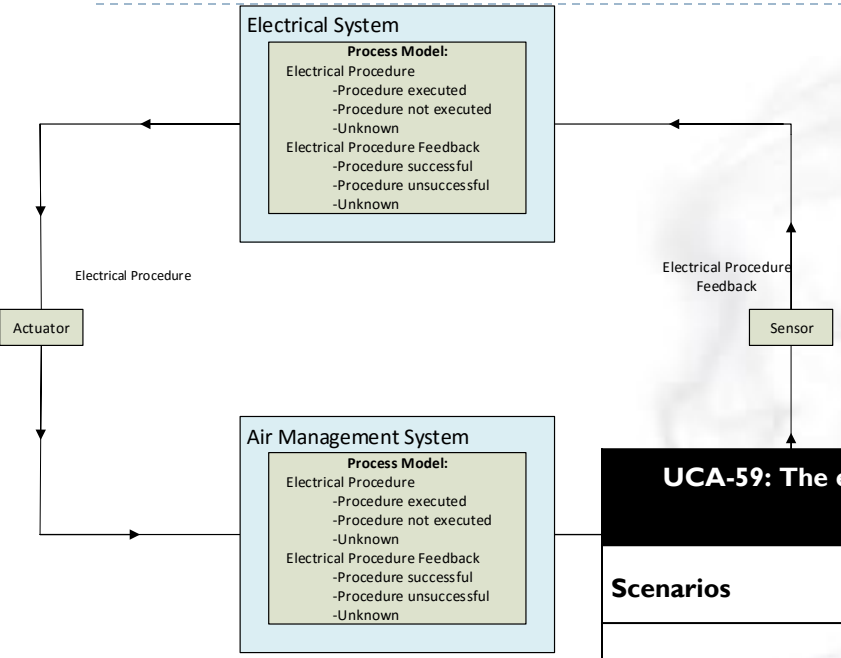
STPA: Step 02

- Process Models

UCA-59: The electrical procedure affects the effectiveness of the smoke procedure, when it is performed at the AMS



STPA: Step 02

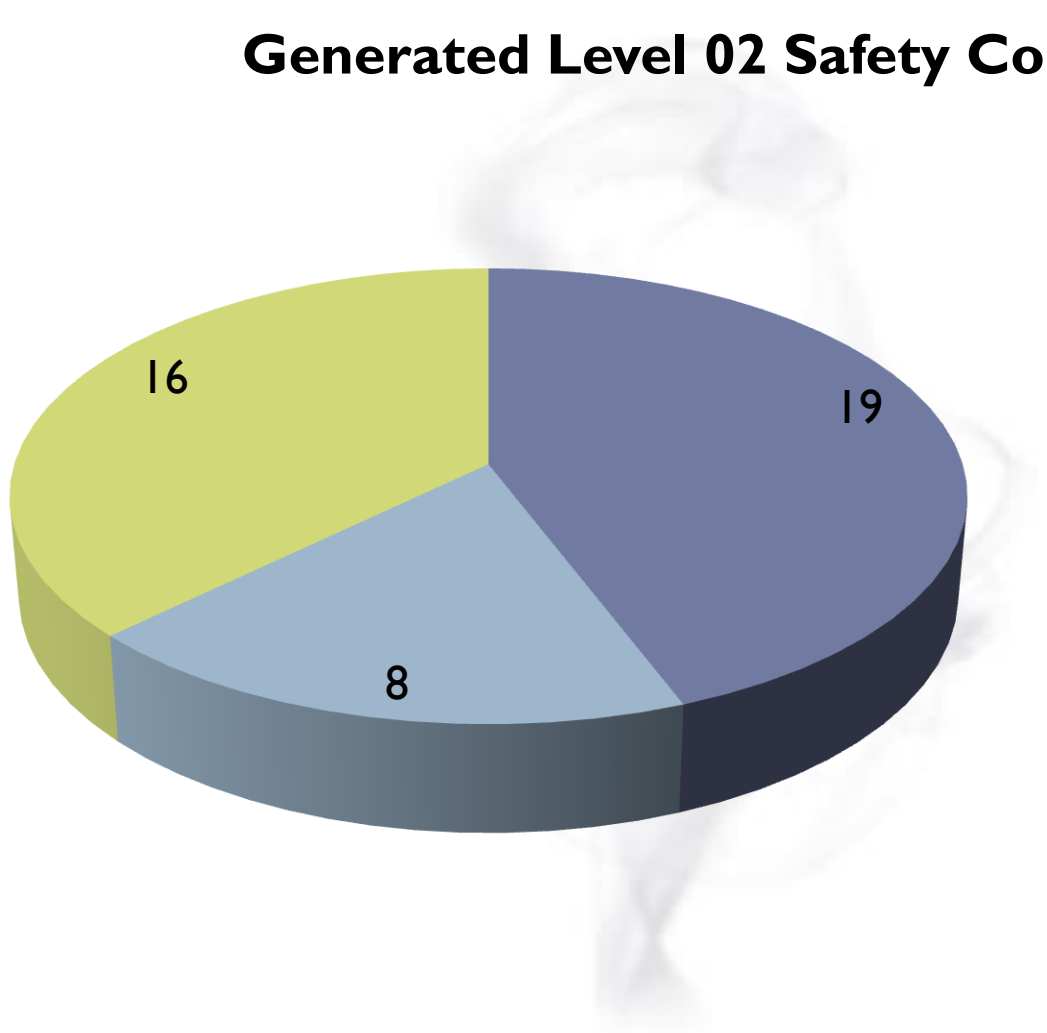


UCA-59: The electrical procedure affects the effectiveness of the smoke procedure, when it is performed at the AMS			
Scenarios	Associated causal factors	Safety Constraint	Allocated to
[Process Model Flaw: Electrical / Air Management Systems]: The smoke procedure has its efficiency reduced by the electrical procedure	The electrical procedure was defined incorrectly and turn some AMS components off, which reduces the smoke procedure efficiency	The electrical procedure shall not affect the smoke procedure efficiency (L2-42)	Aircraft manufacturer
	The electrical procedure is executed with an incorrect timing and affect the smoke procedure	The electrical procedure shall not affect the smoke procedure efficiency (L2-42)	Aircraft manufacturer
	The communication between the electrical and air management systems is flawed	The communication between the electrical and air management systems shall be assured (L2-43)	Aircraft manufacturer

Safety Constraints

- 03 Safety Constraints - Hazards
- 21 Safety Constraints - Unsafe Control Actions
- 43 Safety Constraints - Causal Factors
- Requirements
  - Multi-disciplinary Team

Conclusion


Generated Level 02 Safety Constraints
16
19
8
Traditionally captured by requirements
Traditionally captured in an advanced stage
Captured only with STPA

Conclusion

- STPA
  - 23 Socio-technical safety constraints generated
  - 13 Socio-technical safety constraints not addressed as a requirement by nowadays regulations
  - Systemically generate requirements
- Traditional Hazard Analysis
  - Does not address the socio-technical aspect of system
  - Some requirements were created after some accident

An accident must occur to make flying safer?

EMBRAER

Thank you!