Massachusetts Institute of Technology

EMBRAER

MIT AEROASTRO

FOR THE JOURNEY S7VEN

STPA application
Air Management System
Commercial Aviation

DISCLAIMER: The technical information contained in this presentation is for illustrative purposes only.

STPA – The process

1 **Identify Accidents and Hazards**

2 **Draw Functional Hierachical Control Structure**

3 **Identify Accident Scenarios**

- STEP 1: Identify Unsafe Control Actions
- STEP 2: Identify Causal Factors and Create Scenarios

4 **Generate Recommendations**

STPA – The process

1 **Identify Accidents and Hazards**

2 Draw Functional Hierachical Control Structure

3 Identify Accident Scenarios

- STEP 1: Identify Unsafe Control Actions
- STEP 2: Identify Causal Factors and Create Scenarios

4 Generate Reccomendations

1 Identify Accidents and Hazards

ACCIDENTS

An accident is defined as "an undesired and unplanned event that results in a loss, including a loss of human life or human injury, property damage, environmental pollution, mission loss, financial loss, etc."

A-1: Loss of Life / Injury (suffocation, eye/ear irritation etc.);
A-2: Loss/damage to aircraft and its equipment
A-3: Mission Interruption or delay

1 Identify Accidents and Hazards

HAZRDS

STPA defines a hazard as "a system state or set of conditions that together with a worst-case set of environmental conditions will lead to an accident (loss)."

Hazard
H1: High/Low Air Temperature
H2: High/Low Air Pressure
H3: Inappropriate Air Transport (bleed and distribution)
H4: Unacceptable Air Contamination
H5: H2O/Ice (other) Accumulation

1 Identify Accidents and Hazards

SAFETY CONSTRAINTS

STPA helps identifying safety constraints to provide guidance to systems designers. This will serve as input to define lower level requirements.

Safety Constraint
SC1: The AMS must not let the air temperature reach values out of the prescribed limits for the destination environment
SC2: The AMS must not let the air pressure reach values out of the prescribed limits for the destination environment
SC3: The AMS must not extract air from from the inappropriate sources at the inappropriate time
SC4: The AMS must not transport air to inappropriate environments at inappropriate times
SC5: The AMS must not distribute air inside the aircraft which is unacceptably contaminated
SC6: The AMS must avoid H2O/Ice accumulation

STPA – The process

1 Identify Accidents and Hazards

2 Draw Functional Hierachical Control Structure

3 Identify Accident Scenarios

- STEP 1: Identify Unsafe Control Actions
- STEP 2: Identify Causal Factors and Create Scenarios

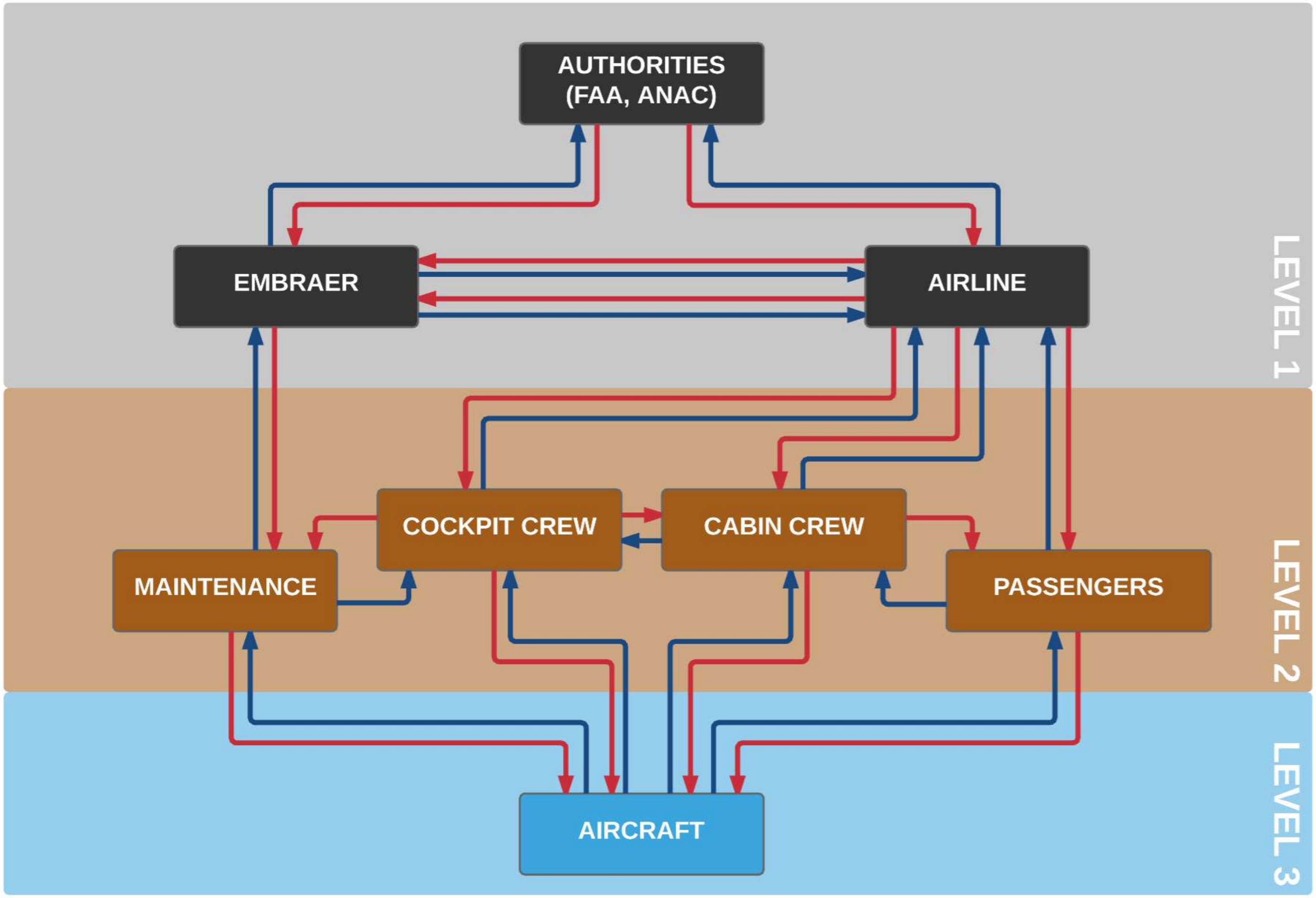
4 Generate Reccomendations

Massachusetts Institute of Technology

EMBRAER

2

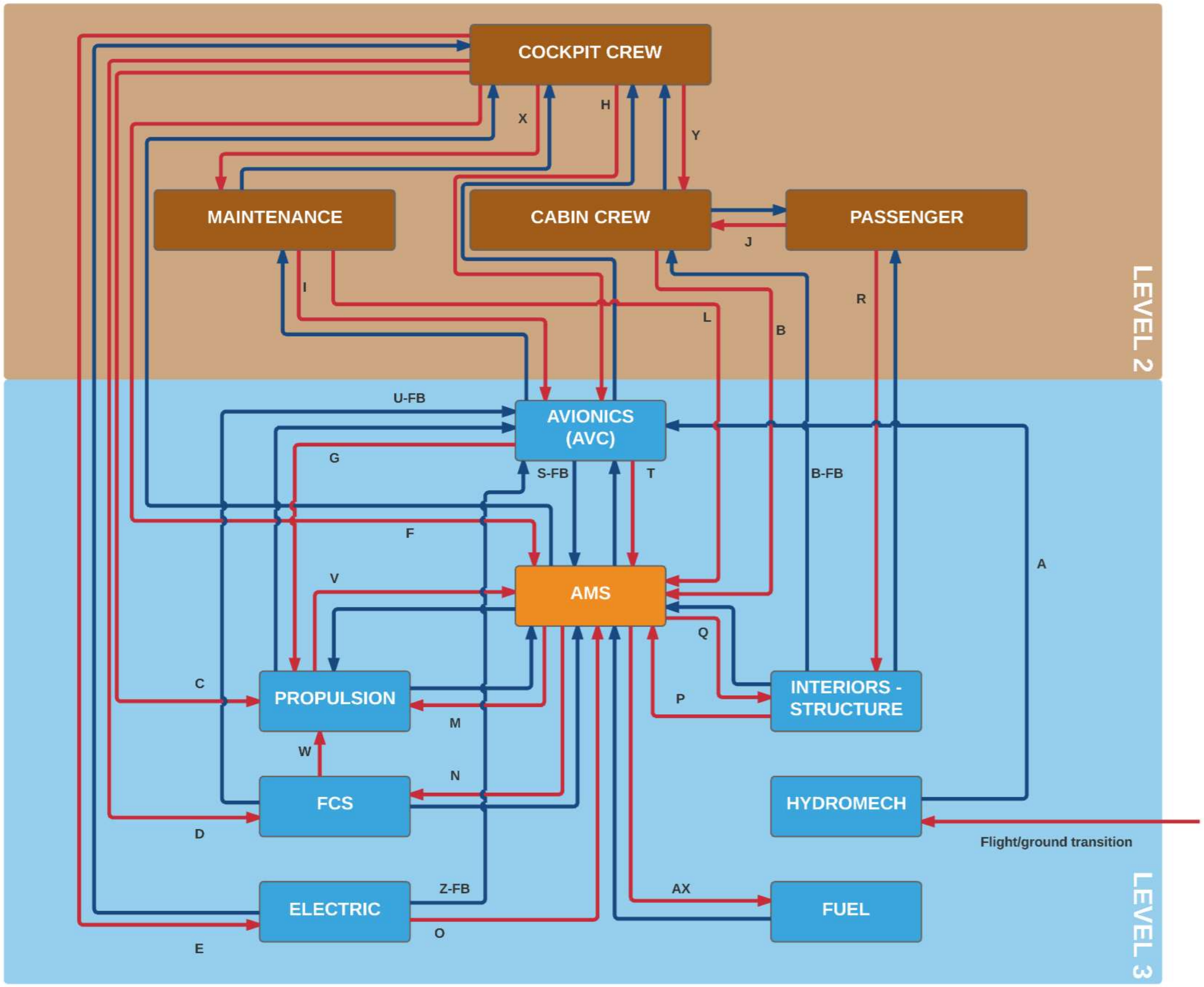
Draw Control Structure



Massachusetts Institute of Technology

EMBRAER

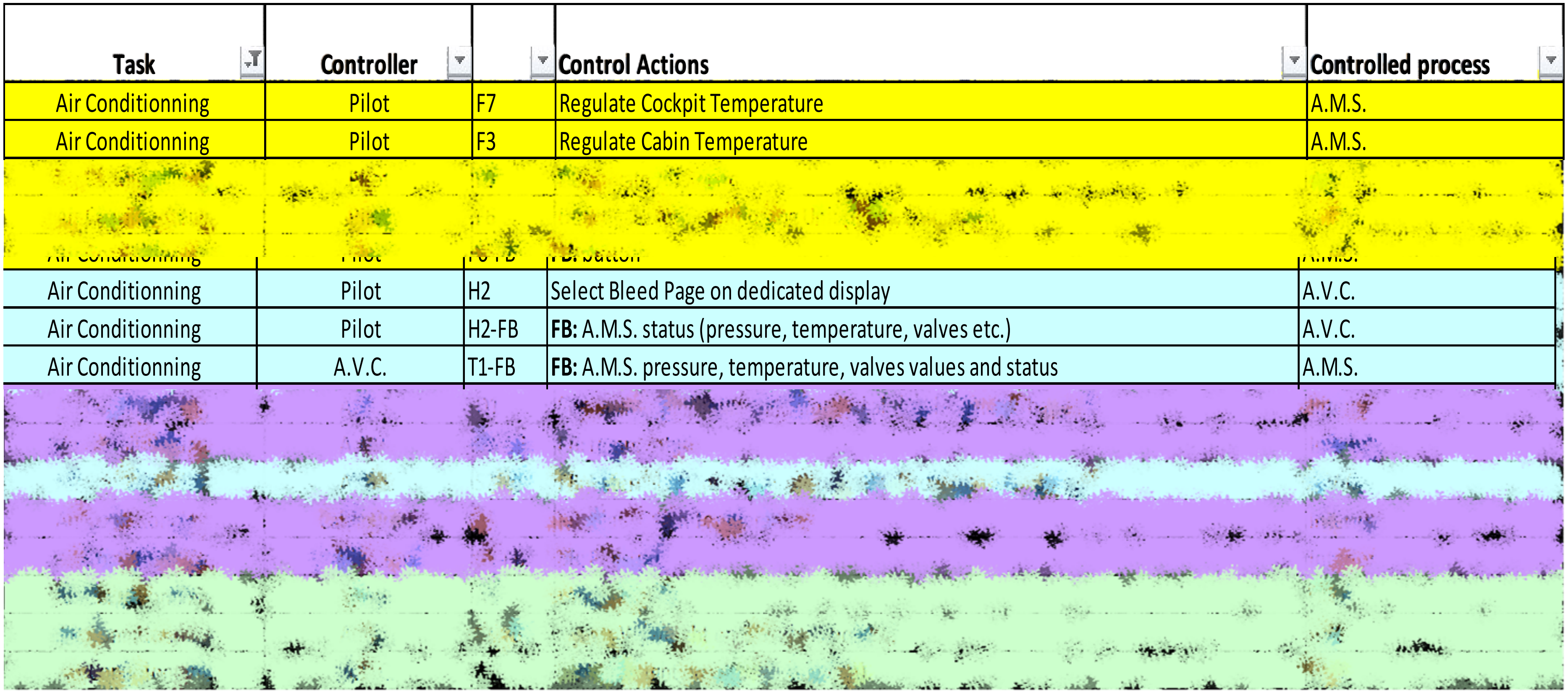
2 Draw Control Structure



Massachusetts Institute of Technology

EMBRAER

2 Draw Control Structure



Task	Controller		Control Actions	Controlled process
Air Conditionning	Pilot	F7	Regulate Cockpit Temperature	A.M.S.
Air Conditionning	Pilot	F3	Regulate Cabin Temperature	A.M.S.
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Air Conditionning	Pilot	[illegible]-FB	**FB:** button	A.M.S.
Air Conditionning	Pilot	H2	Select Bleed Page on dedicated display	A.V.C.
Air Conditionning	Pilot	H2-FB	**FB:** A.M.S. status (pressure, temperature, valves etc.)	A.V.C.
Air Conditionning	A.V.C.	T1-FB	**FB:** A.M.S. pressure, temperature, valves values and status	A.M.S.
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

STPA – The process

1 Identify Accidents and Hazards

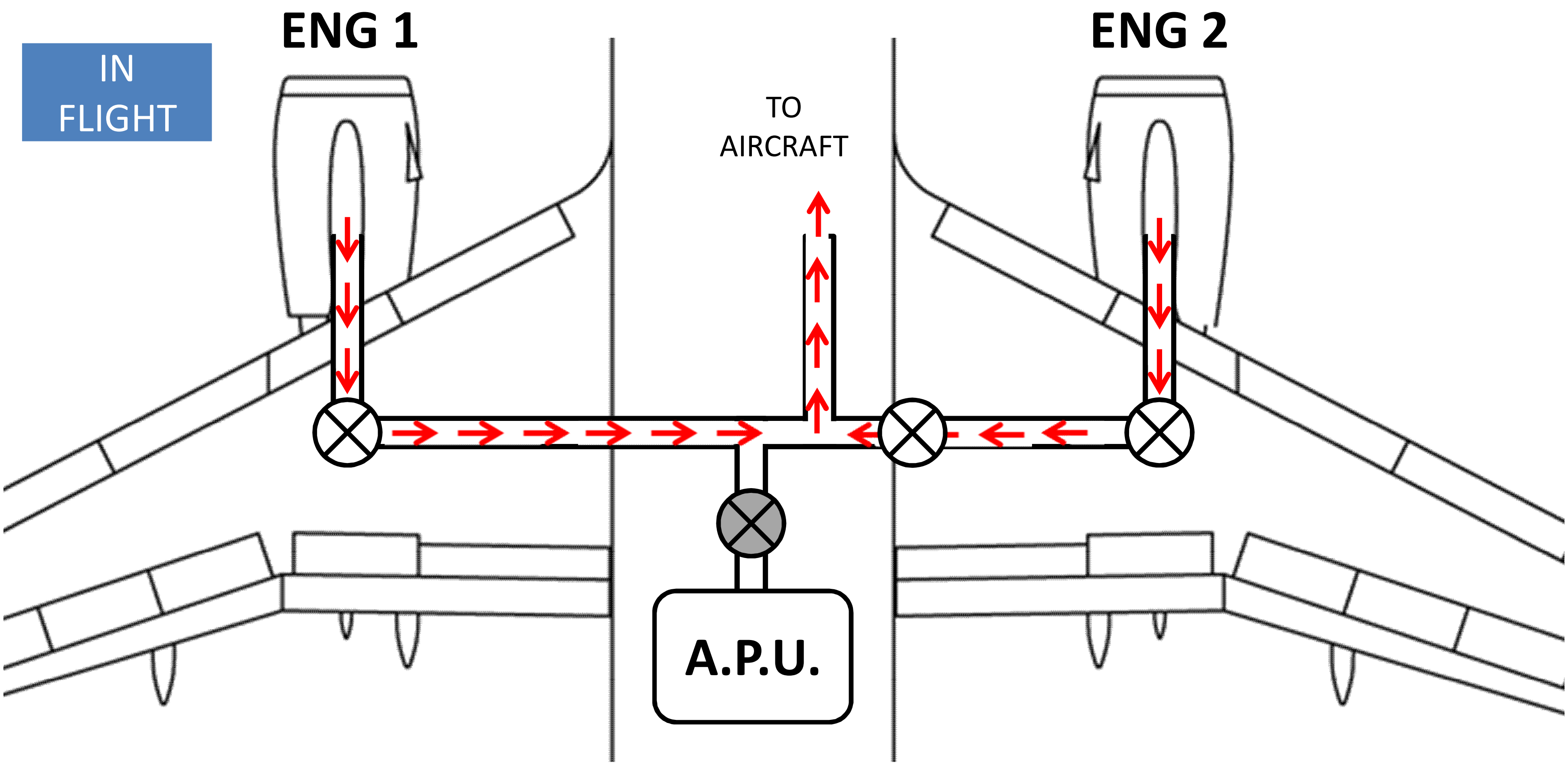
2 Draw Functional Hierachical Control Structure

3 **Identify Accident Scenarios**

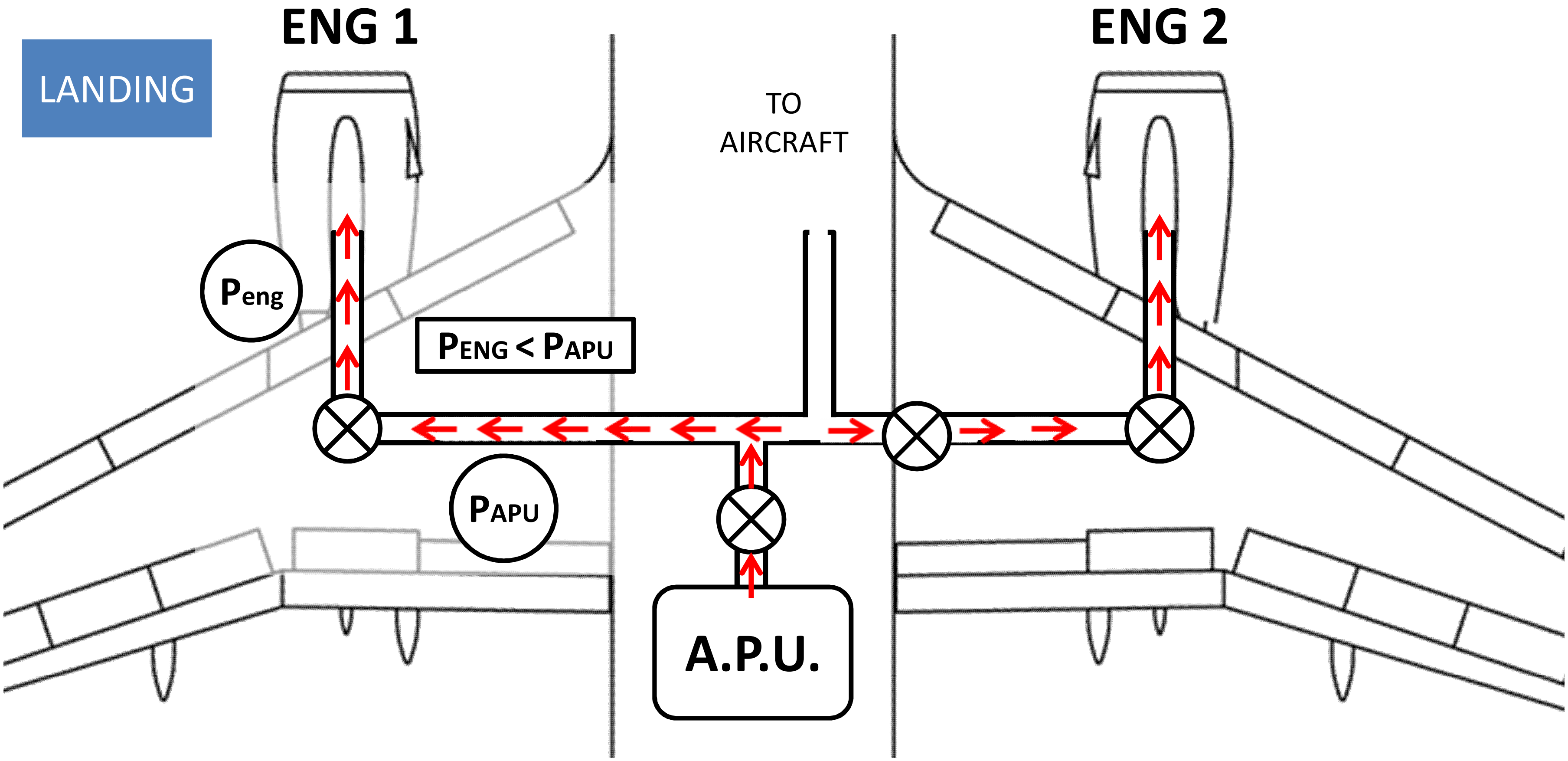
- STEP 1: Identify Unsafe Control Actions
- STEP 2: Identify Causal Factors and Create Scenarios

4 Generate Reccomendations

3 Identify Accident Scenarios



3 Identify Accident Scenarios

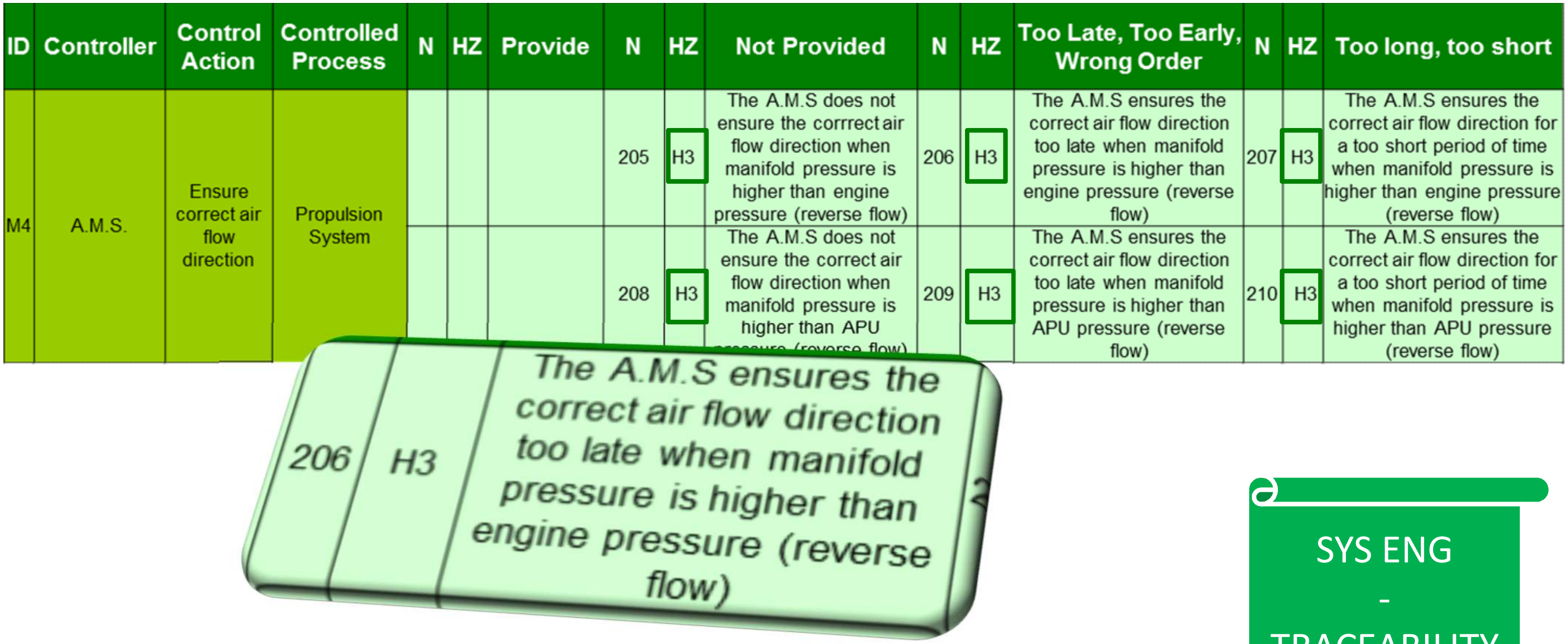


Massachusetts Institute of Technology

EMBRAER

3 Identify Accident Scenarios

STEP 1: Identify Unsafe Control Actions



ID	Controller	Control Action	Controlled Process	N	HZ	Provide	N	HZ	Not Provided	N	HZ	Too Late, Too Early, Wrong Order	N	HZ	Too long, too short
M4	A.M.S.	Ensure correct air flow direction	Propulsion System				205	H3	The A.M.S does not ensure the corrrect air flow direction when manifold pressure is higher than engine pressure (reverse flow)	206	H3	The A.M.S ensures the correct air flow direction too late when manifold pressure is higher than engine pressure (reverse flow)	207	H3	The A.M.S ensures the correct air flow direction for a too short period of time when manifold pressure is higher than engine pressure (reverse flow)
							208	H3	The A.M.S does not ensure the correct air flow direction when manifold pressure is higher than APU pressure (reverse flow)	209	H3	The A.M.S ensures the correct air flow direction too late when manifold pressure is higher than APU pressure (reverse flow)	210	H3	The A.M.S ensures the correct air flow direction for a too short period of time when manifold pressure is higher than APU pressure (reverse flow)

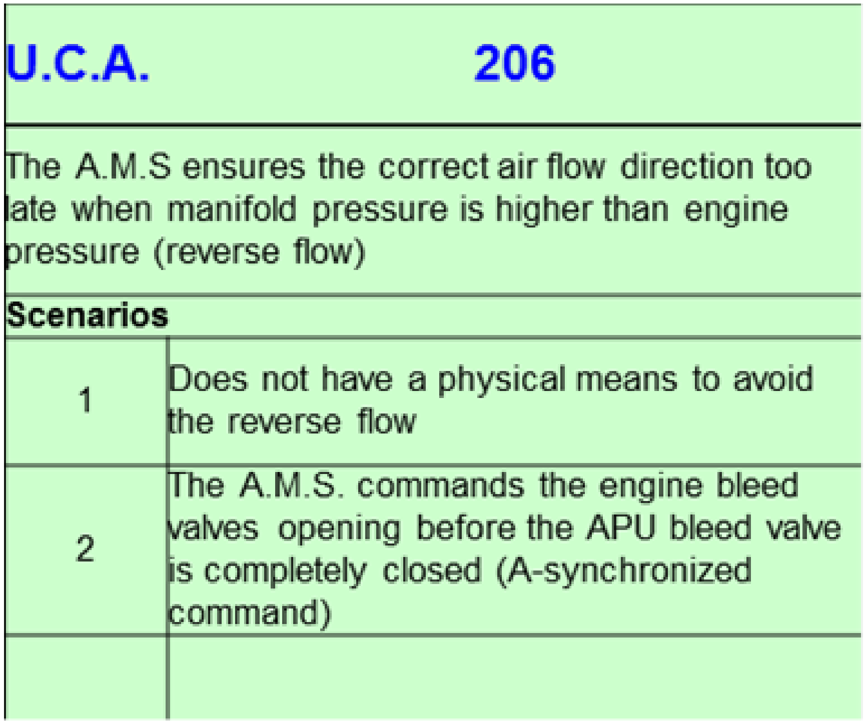
206	H3	The A.M.S ensures the correct air flow direction too late when manifold pressure is higher than engine pressure (reverse flow)

SYS ENG
-
TRACEABILITY

3

Identify Accident Scenarios

STEP 2: Identify Causal Factors and Create Scenarios



U.C.A.	206
The A.M.S ensures the correct air flow direction too late when manifold pressure is higher than engine pressure (reverse flow)	
Scenarios	
1	Does not have a physical means to avoid the reverse flow
2	The A.M.S. commands the engine bleed valves opening before the APU bleed valve is completely closed (A-synchronized command)

STPA – The process

1 Identify Accidents and Hazards

2 Draw Functional Hierachical Control Structure

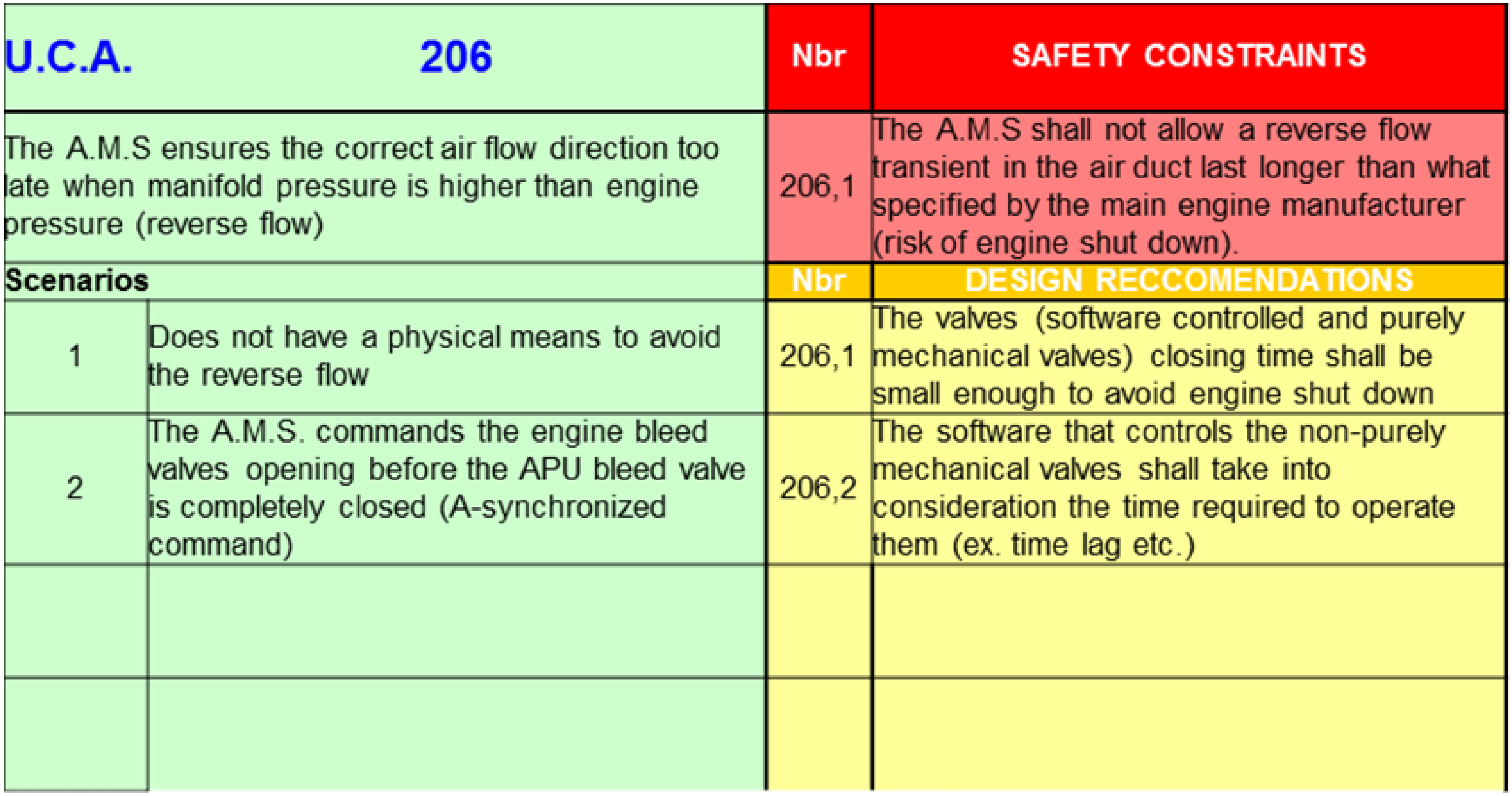
3 Identify Accident Scenarios

- STEP 1: Identify Unsafe Control Actions
- STEP 2: Identify Causal Factors and Create Scenarios

4 **Generate Reccomendations**

4

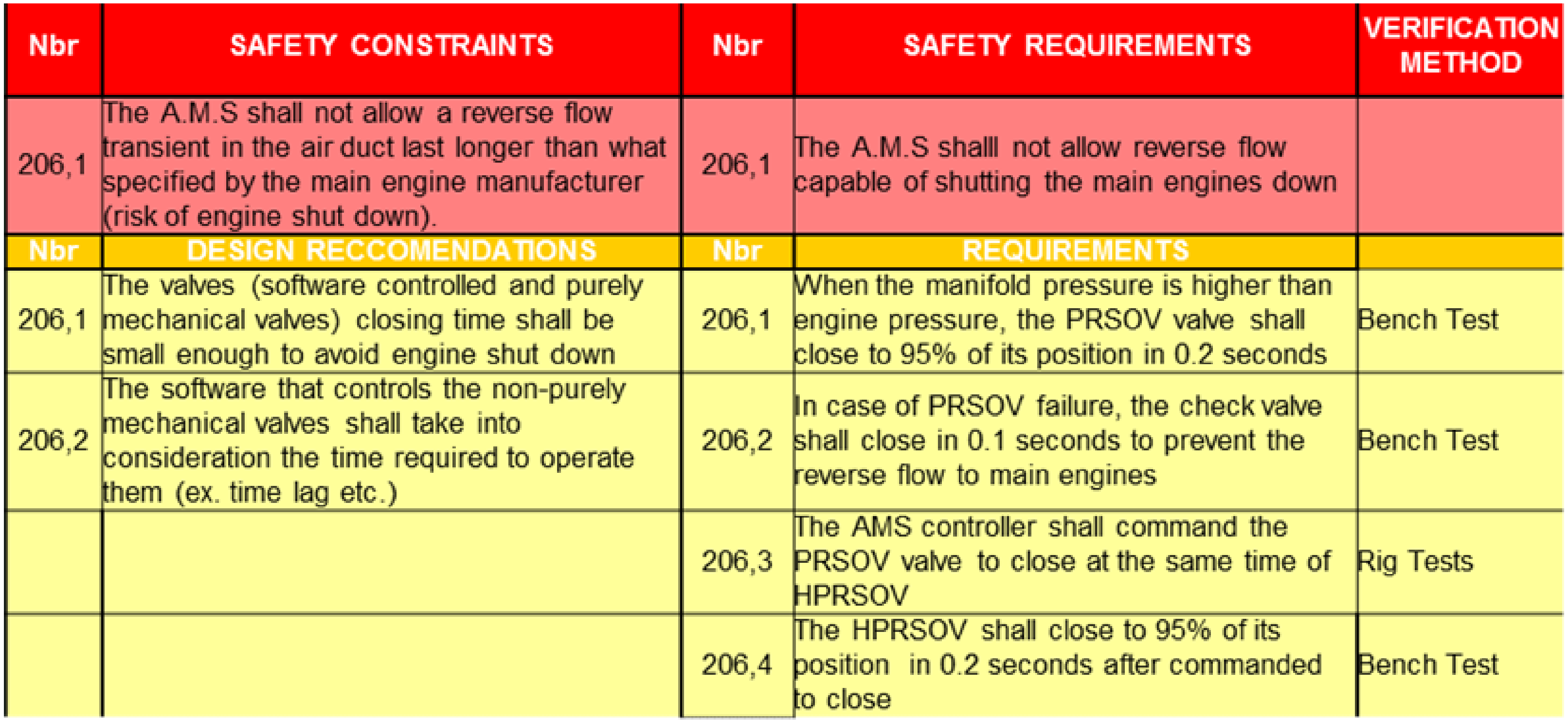
Generate Recommendations and safety constraints



U.C.A.	206	Nbr	SAFETY CONSTRAINTS
The A.M.S ensures the correct air flow direction too late when manifold pressure is higher than engine pressure (reverse flow)		206,1	The A.M.S shall not allow a reverse flow transient in the air duct last longer than what specified by the main engine manufacturer (risk of engine shut down).
Scenarios		Nbr	DESIGN RECCOMENDATIONS
1	Does not have a physical means to avoid the reverse flow	206,1	The valves (software controlled and purely mechanical valves) closing time shall be small enough to avoid engine shut down
2	The A.M.S. commands the engine bleed valves opening before the APU bleed valve is completely closed (A-synchronized command)	206,2	The software that controls the non-purely mechanical valves shall take into consideration the time required to operate them (ex. time lag etc.)

Is it possible to generate requirements from STPA outputs?

Yes, indeed…



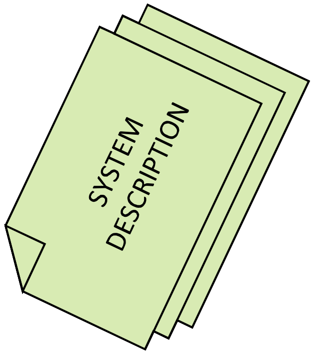
Nbr	SAFETY CONSTRAINTS	Nbr	SAFETY REQUIREMENTS	VERIFICATION METHOD
206,1	The A.M.S shall not allow a reverse flow transient in the air duct last longer than what specified by the main engine manufacturer (risk of engine shut down).	206,1	The A.M.S shalll not allow reverse flow capable of shutting the main engines down	
Nbr	DESIGN RECCOMENDATIONS	Nbr	REQUIREMENTS	
206,1	The valves (software controlled and purely mechanical valves) closing time shall be small enough to avoid engine shut down	206,1	When the manifold pressure is higher than engine pressure, the PRSOV valve shall close to 95% of its position in 0.2 seconds	Bench Test
206,2	The software that controls the non-purely mechanical valves shall take into consideration the time required to operate them (ex. time lag etc.)	206,2	In case of PRSOV failure, the check valve shall close in 0.1 seconds to prevent the reverse flow to main engines	Bench Test
		206,3	The AMS controller shall command the PRSOV valve to close at the same time of HPRSOV	Rig Tests
		206,4	The HPRSOV shall close to 95% of its position in 0.2 seconds after commanded to close	Bench Test

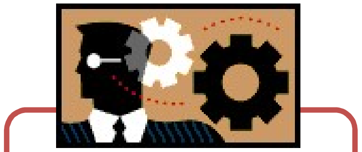
Massachusetts Institute of Technology

EMBRAER

Our project in a snapshot…

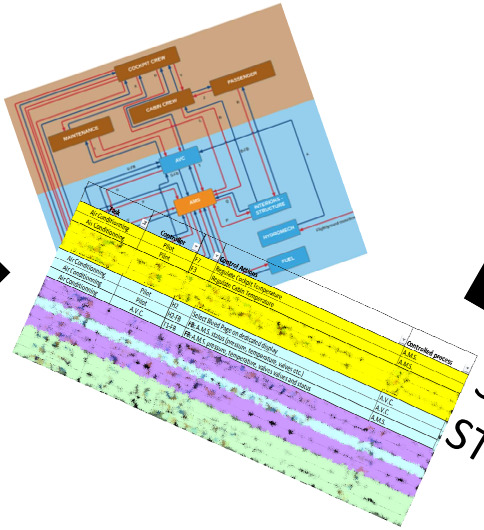
July 2016 | August 2016 | September 2016





SYSTEM SPECIALIST

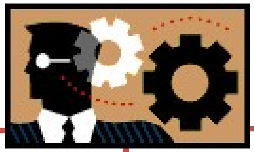
INTEGRATION/SAFETY ENGINEER



Task	Controller		Control Actions	Controlled process
Air Conditionning	Pilot	F7	Regulate Cockpit Temperature	A.M.S.
Air Conditionning	Pilot	F3	Regulate Cabin Temperature	A.M.S.
Air Conditionning	Pilot	H2	Select Bleed Page on dedicated display	A.V.C.
Air Conditionning	Pilot	H2-FB	**FB:** A.M.S. status (pressure, temperature, valves etc.)	A.V.C.
Air Conditionning	A.V.C.	T1-FB	**FB:** A.M.S. pressure, temperature, valves values and status	A.M.S.

STEP 1

STEP 2



SYSTEM SPECIALIST | PILOT

INTEGRATION/SAFETY ENGINEER | MECHANICS

200+
Safety Constraints
(high level design drivers)

700+
Design recommendations

Massachusetts Institute of Technology

EMBRAER

Our project in a snapshot...

- TOP-DOWN APPROACH
- STRUCTURED/SYSTEMATIC METHOD
- MULTIDISCIPLINARY ENGINEERING
- REQUIREMENTS TRACEABILITY
- REQUIREMENTS RE-USE
- SOLID REQUIREMENT SET SINCE BEGINNING

STEP 1
STEP 2

SYSTEM SPECIALIST

INTEGRATION/SAFETY ENGINEER

(high level design drivers)

700+
Design recommendations

Massachusetts
Institute of
Technology

EMBRAER

Andrea
Scarinci

Amanda
Quilici

Danilo
Ribeiro

Felipe
Oliveira

Ricardo
Moraes

Daniel
Pereira

Andrea Scarinci

**PhD candidate and
Research Assistant**

scarinci@mit.edu

Felipe Oliveira

**System Integration
and Safety**

felipe.oliveira@embraer.com.br