Massachusetts Institute of Technology

EMBRAER

MIT AEROASTRO

STPA in the Aeronautical Industry

Roles, resources and best practice

Massachusetts Institute of Technology

EMBRAER

1 - The roles. Who should do what?

2 –Best Practice

3 – Resources

Massachusetts Institute of Technology

EMBRAER

1 - The roles. Who should do what?

1.1 Who conducts the analysis?

STPA FACILITATOR

1.2 Who should be involved in the analysis?

INFORMATION FEEDERS

1.3 Who should review the analysis?

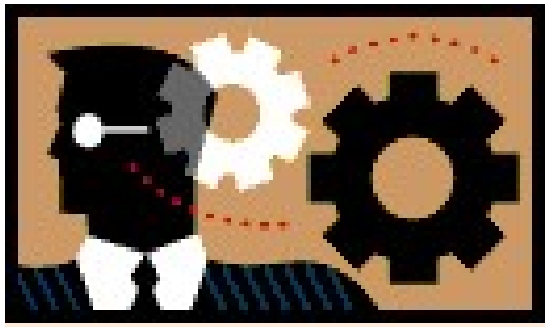
REQUIREMENT VALIDATOR

Massachusetts Institute of Technology

EMBRAER

1 - The roles. Who should do what?

1.1 Who conducts the analysis?



STPA FACILITATOR

PROFILE - TASKS

- Systems Integrator;
- STPA knowledge;
- Multidisciplinary background required;
- Good communication/relational skills;
- Knowledge of product/system development process, requirements and standards;

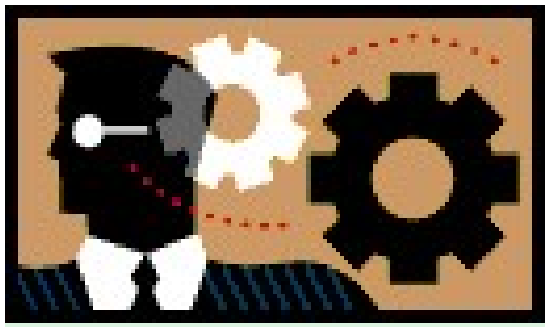
Translate STPA results into suitable material for certification (means of compliance)

Massachusetts Institute of Technology

EMBRAER

1 - The roles. Who should do what?

1.2 Who should be involved in the analysis?



INFORMATION FEEDERS

PROFILE - TASKS

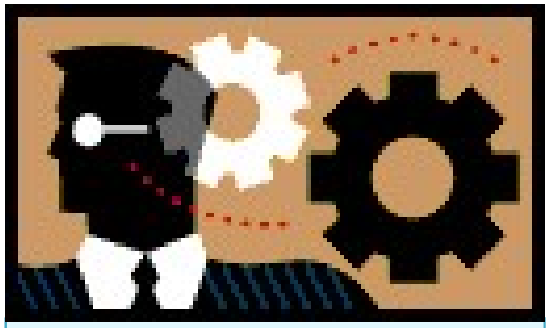
- Systems Specialists;
- Systems operators (ex. Pilots, Cabin crew);
- Maintenance engineers and personnel;
- Manufacturing engineers;
- Production line personnel;
- Customer service;
- Customers;
- Do NOT need to know STPA;
- Will define requirements.

Massachusetts Institute of Technology

EMBRAER

1 - The roles. Who should do what?

1.3 Who should review the analysis?



REQUIREMENT VALIDATOR

PROFILE - TASKS

- Process assurance engineer;
- Needs to be an expert in how requirements have to be written for certification purposes;
- Needs to know certification requirements;
- Needs NOT to be involved in the STPA analysis nor know the technique.

Massachusetts Institute of Technology

EMBRAER

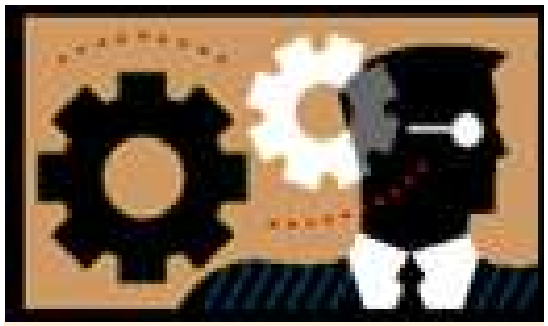
1 - The roles. Who should do what?

1.3 Who should review the analysis?

INFORMATION FEEDERS

REQUIREMENT VALIDATOR

+



STPA FACILITATOR

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.1 How to "get going" with the analysis

At the very beginning

- A lot of information;
- Many different levels of abstraction;
- Difficult to mentally define the scope of the analysis;

TAKE A BREATH!

STPA is there exactly to help manage complexity, if you were able to do it all in your mind, we would not need this technique

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.1 How to "get going" with the analysis

- **A** Spend time (some days or 1 or 2 weeks) reading documentation and understanding the system;
- **B** Underline and list possible candidates for ***controllers***, ***controlled process*** and ***control actions***;
- **C** Attempt a first draft of the control structure;
- **D** Check whether the level abstraction is correct, if not reiterate.

Massachusetts Institute of Technology

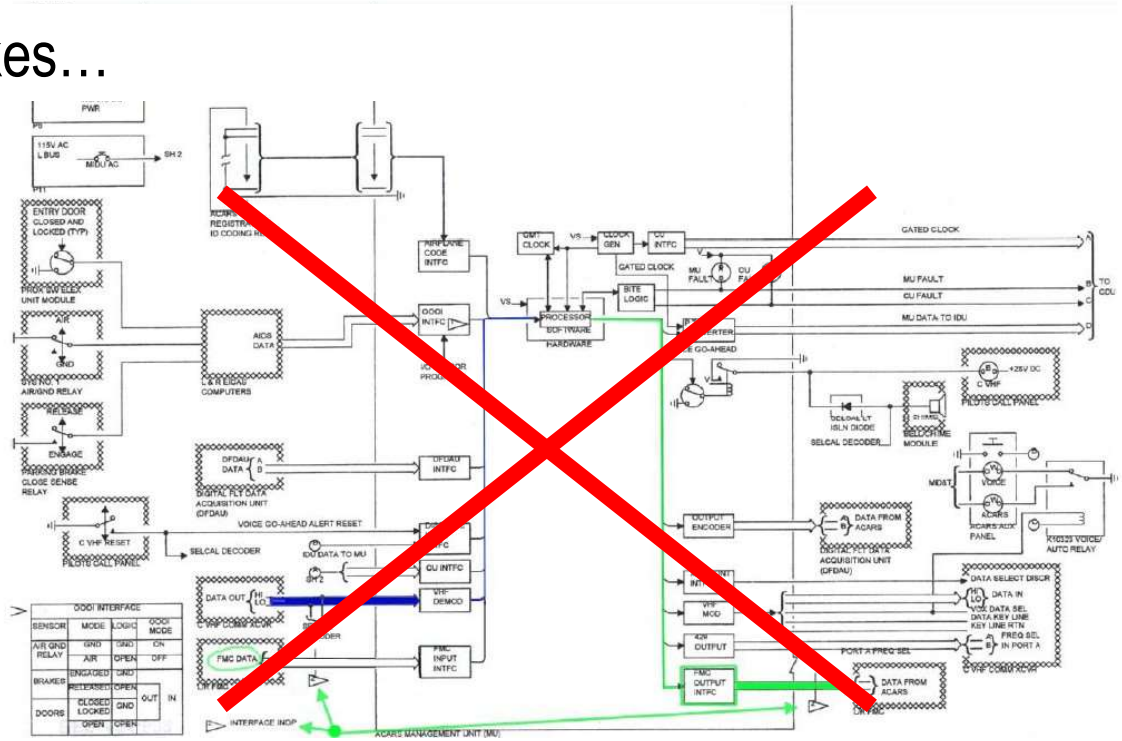
EMBRAER

2 –Best Practice

2.1 How to "get going" with the analysis

Tips and common mistakes…

If the control structure looks too detailed, choose a higher level of abstraction



Massachusetts Institute of Technology

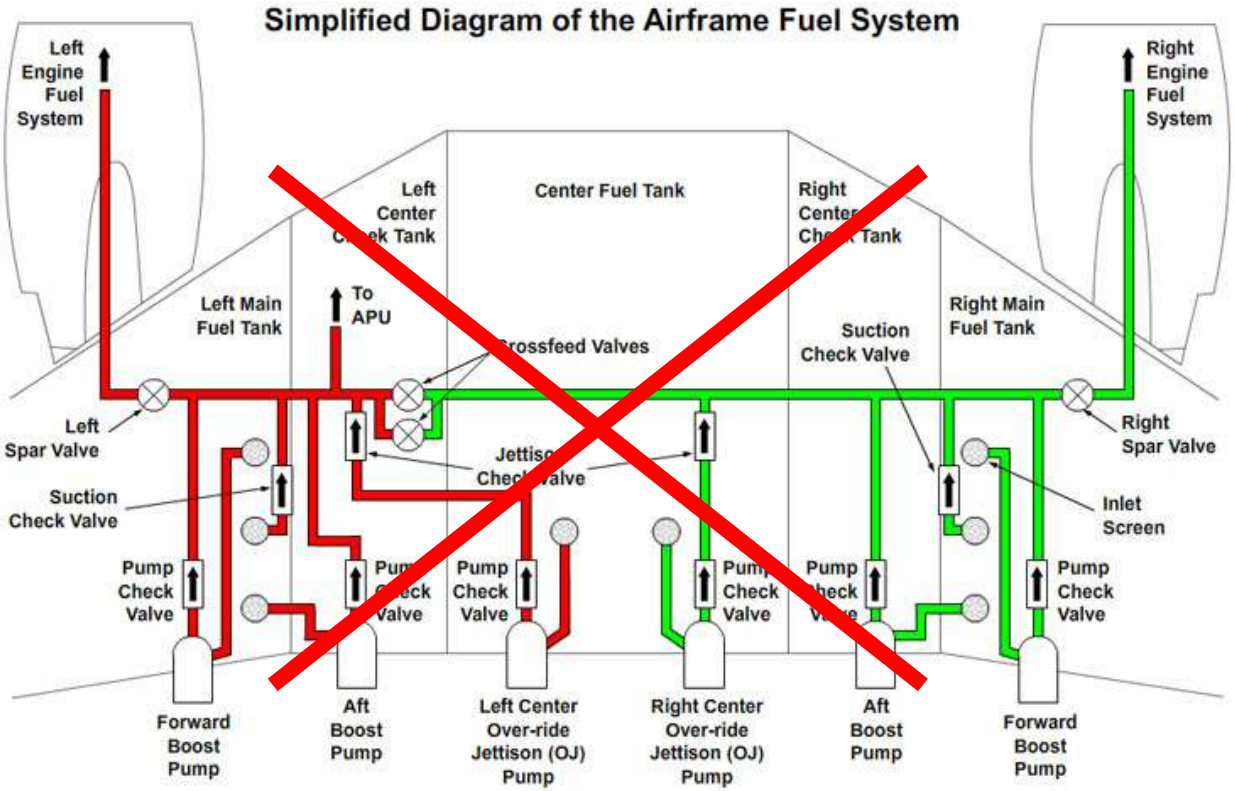
EMBRAER

2 –Best Practice

2.1 How to "get going" with the analysis

A control structure is NOT a physical schema of the system.

Functional relations determine the hierarchy of controller-controlled process, NOT container-content



Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.1 How to "get going" with the analysis

If you can't identify a feedback for a control action… it's not necessarily because the diagram is wrong. Something may be missing from the design of the actual system.

REMEMBER:

The STPA analysis starts with the control structure. The control structure itself already gives some insight on possible design flaws or inconsistencies. Do not rush to get to STEP 1!

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

- HAZARDS - ACCIDENTS
- CONTROL STRUCTURE
- STEP 1
- STEP 2
- DESIGN RECCOMENDATIONS AND REQUIREMENTS

- *Who?*
- *How?*
- *Tips*

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

HAZARDS - ACCIDENTS

Who?

How?

- The STPA facilitator can define a list of hazards and accidents before meeting with the information feeders;
- This list can be validated and refined during the meetings held with information feeders for the controls structure definition, STEP 1, STEP 2 etc.

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

HAZARDS - ACCIDENTS

Tips

- Avoid writing down many hazards and many accidents (usually 3-4 accidents with 4-5 hazards is a good number);
- Keep the level of hazards and accidents relatively high with respect to the level of the analysis → This avoids losing some possible scenarios;
- Specialists and other information feeders may fear such a high level will not “cover” all possible hazards/accidents → Try to map all their scenarios to the hazards to check for completeness

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

CONTROL STRUCTURE

Who?

How?

- After preparing the first draft, the STPA facilitator should ask the information feeders to check the correctness of the control structure;
- This should be performed through short meetings (~1h) with each of the information feeders groups;

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

CONTROL STRUCTURE

Tips

- Specialists may criticize the usefulness of a high level of abstraction and push to insert details in the control structure.

  → Explain details will be incorporated at a later stage, but that the scope of the technique is to deal with complexity step by step by the means of abstraction.

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

STEP 1

Who?

How?

- The STPA facilitator should prepare the STEP 1 table and a couple of examples;
- The UCAs should be identified during meetings of with each of the information feeders groups:
  - Do not exceed 2h-2h½ duration;
  - 2/3 information feeders maximum from one category (ex. pilot, system specialist etc.);
  - Inter-category meeting when needed.

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

STEP 1

Tips

- Explain that the meaning of a UCA is to identify the ***CONTEXT*** in which a specific control action can become unsafe;
- Information feeders, operators especially, may have a tendency to consider certain lapses or mistakes as “impossible” (“the pilot will never forget/do…”). → Insist that if a certain unsafe action is physically possible someday, somehow, someone, *will* do it;
- Remember STEP 1 is only meant to identify unsafe contexts, not the reasons behind them occurring (STEP 2): avoid implicit likelihood bias.

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

STEP 2

Who?

How?

- The STPA facilitator should prepare the STEP 2 table and a couple of examples;
- The causal scenarios should be identified during meetings of about 2h with each of the information feeders groups:
  - Do not exceed 2h-2h½ duration;
  - 2/3 information feeders maximum from one category (ex. pilot, system specialist etc.);
  - Inter-category meeting when needed.

Massachusetts Institute of Technology

EMBRAER

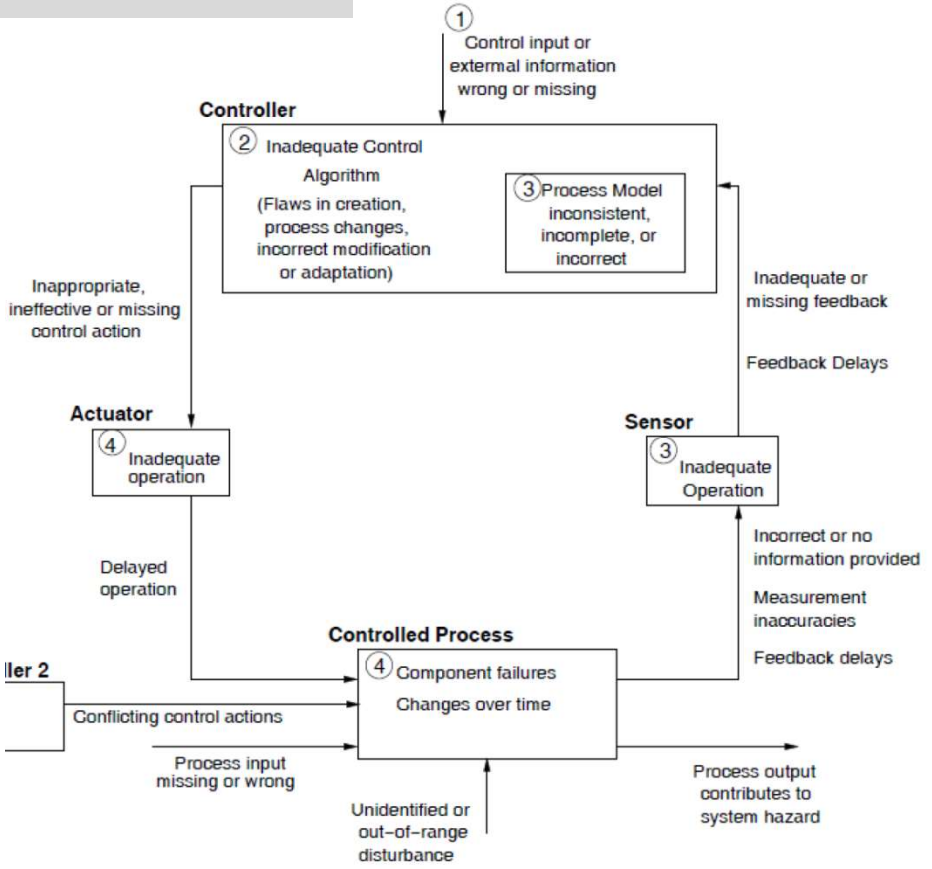
2 –Best Practice

2.2 How to carry out the analysis

STEP 2

Tips

- Do not use checklists to perform this step as an FMEA;
- Try to look for broad scenarios: the reasons why a certain UCA may occur can come from any point in the control structure. Do NOT narrow down.



Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

STEP 2

Tips

- Do not forget process model issues;
- Do not overlook higher level controller inputs;
- Look at previous accidents/incidents when available to make sure they are included in the analysis;
- The scenarios can be high level at first and then refined according to the objective of the analysis (reuse?) and level of detail available on current design.

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

REQUIREMENTS AND RECCOMENDATIONS

Who?

How?

- Dedicated meetings with information feeders should be held to identify possible design recommendations to the problems identified;
- Design recommendations are a first “draft” of possible requirements;
- Formal requirements should be written by the information feeders and reviewed by the requirement validator with the support of the STPA facilitator.

Massachusetts Institute of Technology

EMBRAER

2 –Best Practice

2.2 How to carry out the analysis

REQUIREMENTS AND RECCOMENDATIONS

Tips

- Keep good traceability of requirements to UCAs and Hazards;
- Usually: # requirements > # design recommendations;
- Adjust the level of abstraction of the design recommendations according to re-use purposes;
- Requirements can also be articulated across different abstraction levels;
- Requirements can be safety, operational, design etc.

Massachusetts Institute of Technology

EMBRAER

3 –Resources

People

- STPA Facilitator;
- Designers;
- Process Engineers;
- Pilots;
- Human Factor Specialist;
- Maintenance etc.

Documents

- Specifications;
- Manuals;
- Standards;
- Schematics etc.

Software

- Simple Graphic Software (Control Structure);
- Simple Database (Control Actions, UCAs, Scenarios, Requirements);
- Ex. Open Office.

Massachusetts Institute of Technology

EMBRAER

3 –Resources

OUR CASE...

AIR MANAGEMENT SYSTEM

- 12 controllers/controlled processes;
- 100+ Control Actions;
- 200+ Safety Constraints;
- 700+ Design Recommendations.

RESOURCES	Engagement %
STPA Facilitator	100 %
Information feeders:	
Designers;	50%
Interface Designers	30%
Pilots;	20%
Human Factor Specialists	20%
Maintenance Specialists	10%

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