FROM PENCIL … TO MODEL BASED SAFETY ASSESSMENT

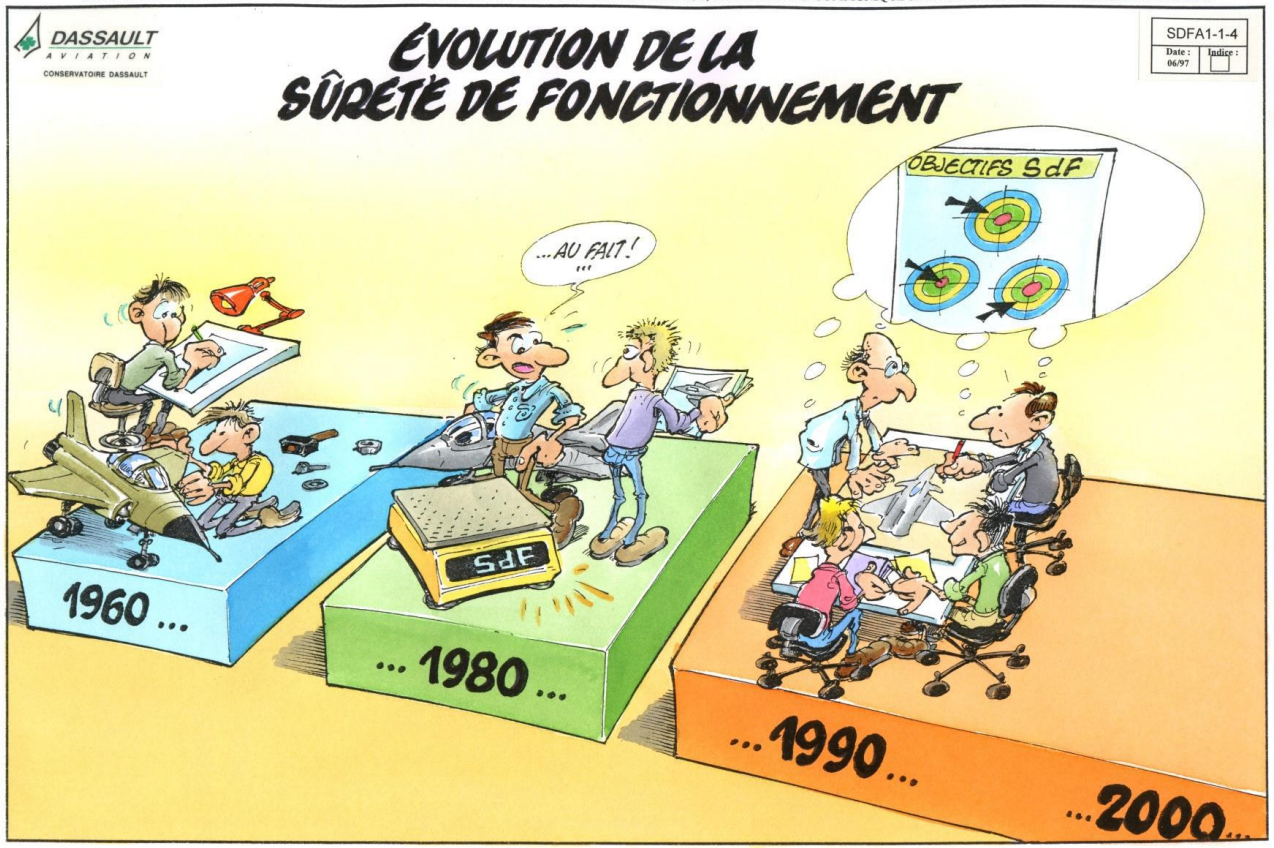
40 YEARS OF BRAINSTORMING AND SAFETY ANALYSIS METHODS IMPROVEMENT

TOULOUSE , JUNE 1RST, 2023

TABLE OF CONTENT

INTRODUCTION

BEFORE 1990



First Fault Tree analyses (mid 80's)

ESCAF^{tm} : tool developed by CEA (French Atomic Research Institute)

- Fault trees built using electronic components
  - All boolean operators available (and, or, not, nand, xor, nor,…)
- Minimal cut sets generated by
  1. injecting combinations of Failure Events
  2. monitoring the Boolean equation output
- Loops in boolean equations handled by the tool
  - Example : on military airplane, failures on one control surface may lead to disengage this control surface and the symmetrical control surface.

SAFETY STUDIES IN DASSAULT

Evolutions of Fault Tree Analysis tools

Since 1985, DASSAULT Research Department worked on a tool allowing to edit and compute Fault Trees

1992 : First industrial version of CECILIA

- Fault Tree editor including a Failure Rate Database
- Limitations
  - Boolean operators limited to: “and”, “or”, “n amongst m”
  - Loops not handled
  - Only small Fault Trees computed in an acceptable timescale
- Fault Trees managed in configuration and in a collaborative environment

In 1994 : Major improvement of computation engine (BDD technology)

- Large Fault Trees (at system level) computed in an acceptable timescale
- Order-truncated computation including probability
- Previously missing boolean operators added

SAFETY STUDIES IN DASSAULT

WHY we want to find an alternative method

- System are more complex. (more redundancy, integrated…)
- Large fault trees are not easily verifiable and so verified.
- When systems are complex, is the analyst-made abstraction correct ?
- Safety analysis is Highly Dependent on Skill of the Analyst
- Safety analysis is Based on Informal Specifications
- Time to produce Safety Analysis need to be reduced.
- How do we ensure consistency between fault tree (specially in case of system update) ?

Is Safety analysis using model a good solution?

- Need a better mean to communicate with the designer.

FIRST MBSA APPLICATION

1994 : only one tool available on the market

FIABEX tool (developed by ELF, COGEMA and CEP Systèmes)

1995 – 1997: Rafale FBW

Model Based Safety Assessment used in parallel with Fault Tree Analysis

Main improvement criteria are satisfied

- Less dependency with the practitioner skill
- Enhancement of communication with design team
  - Fault Tree produced from MBSA are correct
- Eased consistency amongst “Fault Trees”
- Timescale reduction

Improvements still required

- Fault Tree generation algorithms (e.g. loop treatment, …)
- Time efficiency for sequence (chronological failure combinations) generation

CECILIA OCAS

1997

- FIABEX development stopped (legal issue)
  - Industry (ELF, IXI, CEA, DASSAULT) academics (LABRI university) collaboration to develop a new safety analysis tool
  - Constraint: be based on a formal language for mathematical properties demonstration
- First version of AltaRica language

1998: First version of AltaRica-based modeling tool

- Result not satisfactory (regression vs. FIABEX)

2000: Dassault Aviation decision to create its own MBSA tool

2001: First version of CECILIA OCAS tool

- Decision to perform Falcon7X DFCS safety assessment using MBSA methodology only

MBSA AND CERTIFICATION

MBSA AND CERTIFICATION

- **2001 : First operational use of Cecilia OCAS**
  - Safety Studies are made on DFCS
  - During Preliminary Design Phase : 28 variants of architecture were studied in 2 months:
    - 35 Failure Conditions were evaluated.

- **2002**
  - First presentation of the methodology to EASA (June 24-25)
  - First presentation of the methodology to FAA (Oct 16-18)
  - The DFCS model is used as a support of this presentation
    - EASA position : No technical objection
    - FAA relies on EASA position

MBSA AND CERTIFICATION

- **2003 : Discussion with EASA on the MBSA methodology**
  - EASA has some concerns as generated Fault Tree are not easily readable.
  - Question raised were :
    - How DA can “demonstrate” that Safety outputs (Fault Trees) are correct ?
    - Does the tool comply with DO178b requirement?

  An agreement between EASA and DA has been obtained:
  - An audit of the model (June 2003)
  - A tool qualification in accordance with DO178b §12 (verification tool)

  Evidences of the tool qualification were presented to EASA in december 2006

MBSA AND CERTIFICATION

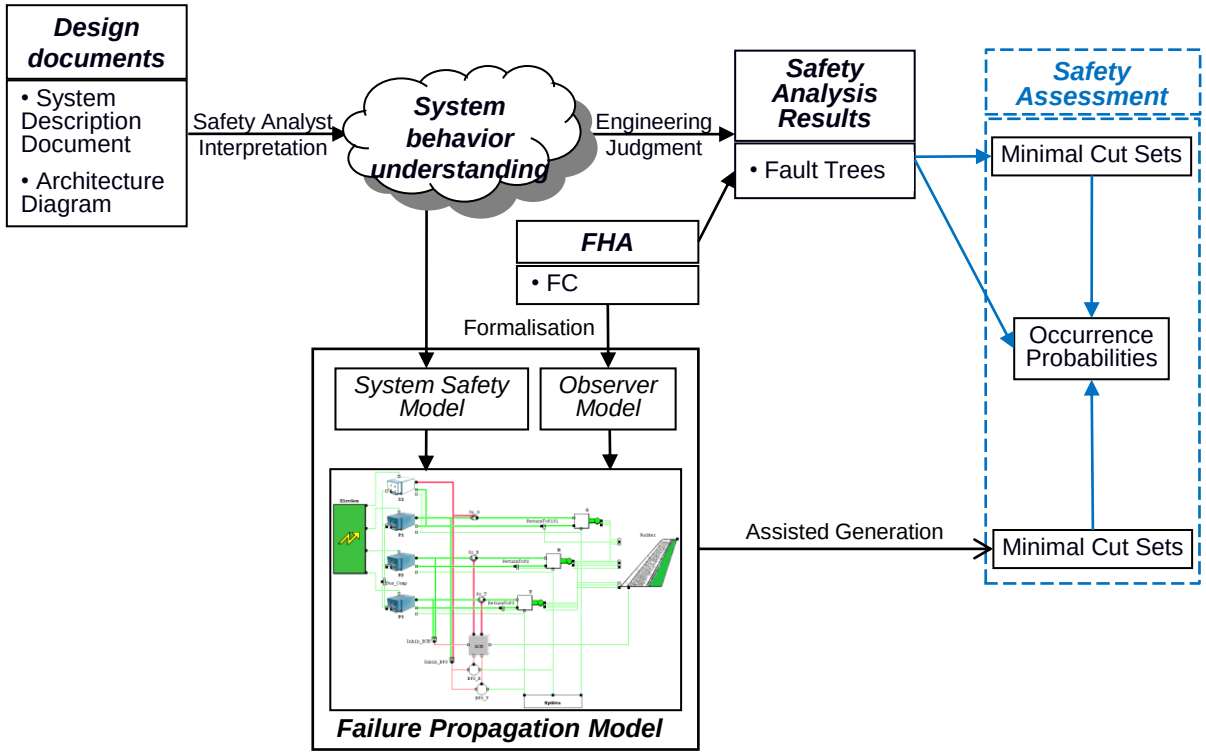
- F7X certification = 1st case of MBSA acceptance by EASA
  - But acceptance on future programs not guaranteed
- DA objective: MBSA acknowledgment at Industry level
  - MBSA allowed to be used in certification compliance activities
    - On any future program
    - With reduced certification effort compared to F7X
- Means: ARP 4761 update
  - Creation of a dedicated appendix
  - MBSA as an alternative to other analysis methods such as Fault Tree, Dependence Diagram or Markov Model
- ARP 4761A status
  - Final acceptance within full document publication frame

MBSA AND CERTIFICATION

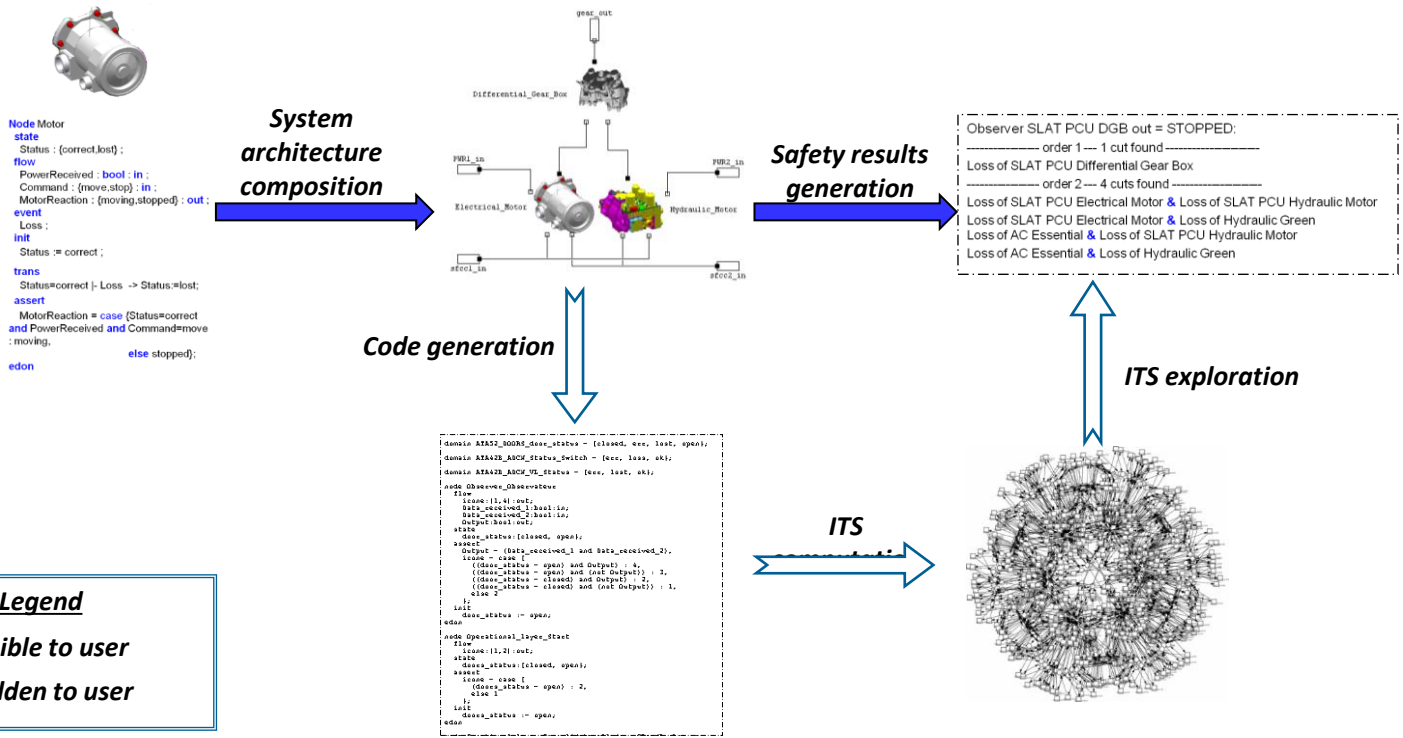
- Certified Airplane with MBSA
  - F7X
  - F8X
- MBSA used to perform safety studies
  - NEURON
- Certification in progress
  - F6X
  - F10X
- In discussion for :
  - MALE
  - FCAS

FTA VERSUS MBSA

FTA VS. MBSA - OVERVIEW



MBSA: FROM ITEM MODEL TO MCS



TODAY
MBSA USAGE

MULTI-SYSTEM DEPENDENCIES SAFETY MODEL– INTRODUCTION

Model Based Safety Assessment

Architecture modeling

- High level model of each system
  - System interconnections (functional data)
  - Connections to physical resources (MAU, electrical bus bars…)
  - Failures having an effect on downstream systems
    - Aircraft behavior in case of failure (cascading failures & reconfigurations)

FHA modeling

- Based on Top-Down FC previously identified

Objectives

Support Bottom-Up FHA
Support PASA

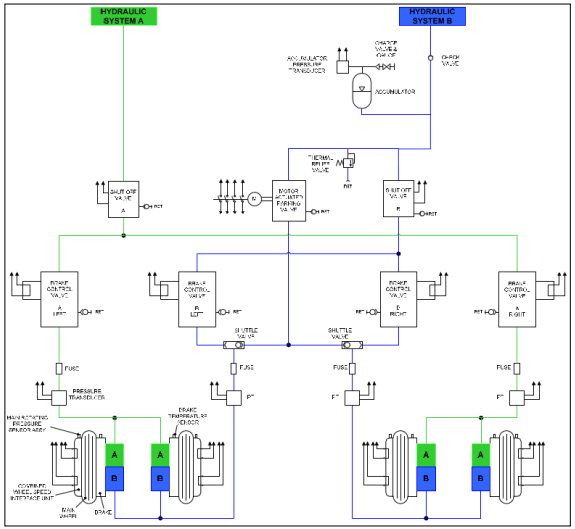
MSDSM – CONTENT

Architecture components

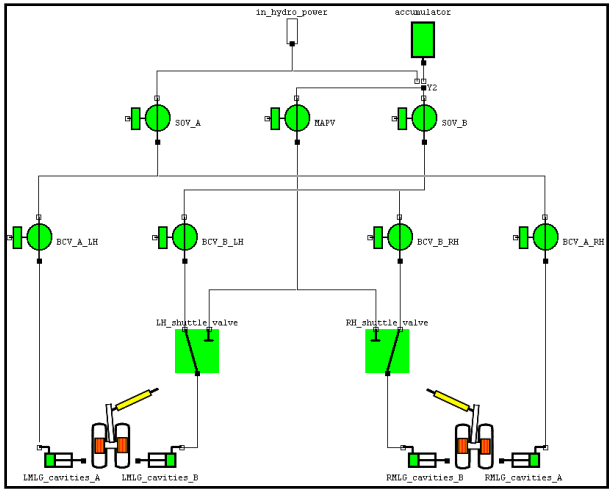
Main LRUs (fuel tank, engine, electrical bus bar…)

- LRUs whose failures have an impact at A/C level

Reconfiguration LRUs (switch, valves…)



Safety view of the Architecture



MSDSM – CONTENT

“Controllers”

Control logics

- Reconfiguration logics
- Data computation and broadcast

Monitoring logics

- Abstract CAS/Warning equations

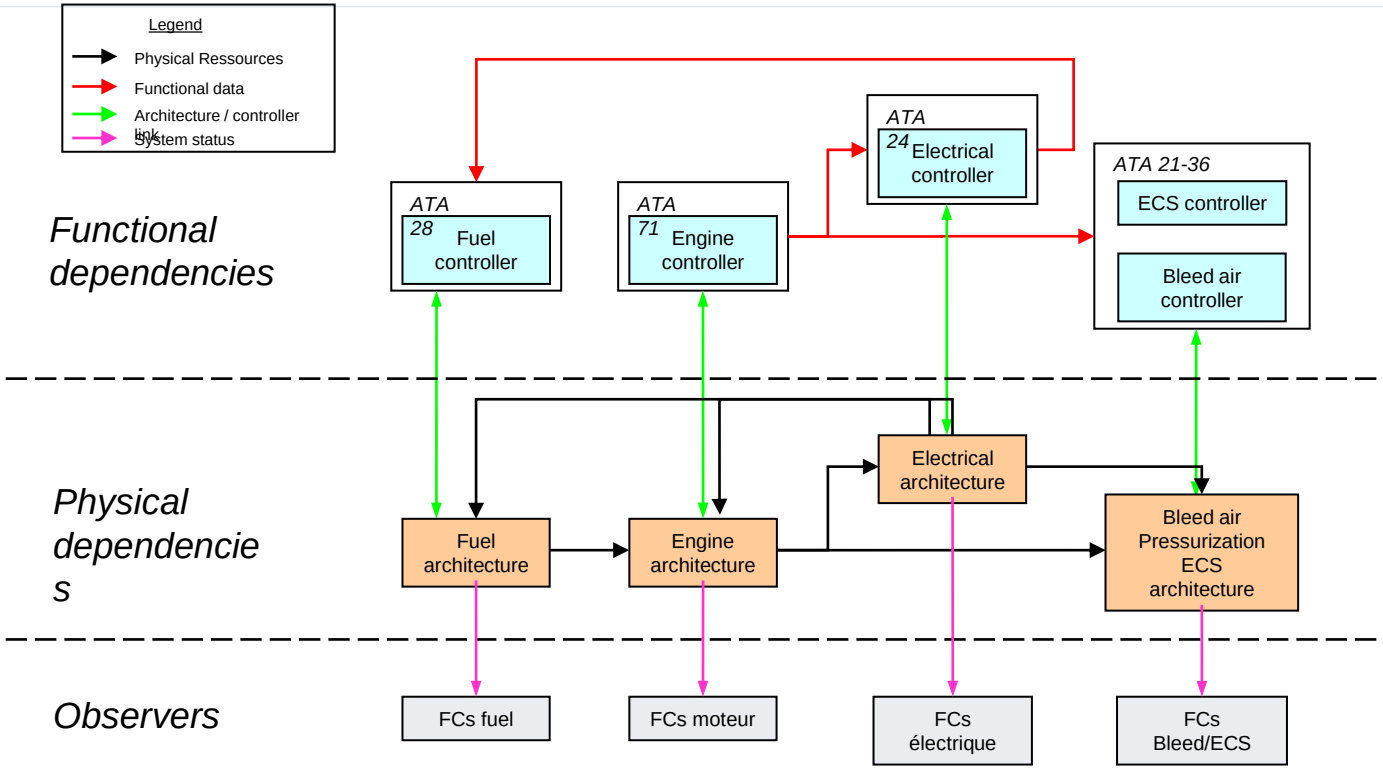
“Observers”

Failure Conditions formalization

- Each FC written as a Boolean equation
  - Based on system components status observation

Aircraft layout

MSDSM – MODEL STRUCTURE



MSDSM – SAFETY ANALYSIS MEANS

Interactive simulation

Observation of failure effects on downstream systems

- To validate the model behavior
- To understand failure scenarios given by the MCS analysis

Assisted Minimal Cut Set generation

Qualitative analysis of failure combinations
To validate the aircraft multi-system architecture (MCS of LRU)

SOME STATISTICS

MODEL COMPARISON (SIZING)

FALCON 7X (DFCS)

Before translate
- Define domain : 35
- Define function : 9
- Define node : 284 (hierarchical : 66)
- Node instance : 4204
- Hierarchical node instance : 871

After flatness
- Flow : 141920 (alias : 90659)
- State : 1135
- Event : 1294
- Trans : 1302
- Extern clause : 7239
- Expression : 323854

FALCON 6X (DFCS)

Before translate
- Define domain : 72
- Define function : 24
- Define node : 502 (hierarchical : 149)
- Node instance : 43682
- Hierarchical node instance : 4237

After flatness
- Flow : 920312 (alias : 730934)
- State : 2081
- Event : 3083
- Trans : 3091
- Extern clause : 35094
- Expression : 875153

MODEL COMPARAISON (SIZING)

FALCON 7X (DFCS)

Number of Failure condition : 105

FALCON 6X (DFCS)

Number of Failure condition : 200

CECILIA CONFIGURATION

CECILIA in 2007

Run on OS 32 Bits platform

BDD engine :

- **ARALIA 4 (64 GB of ram memory)**

CECILIA in 2023

Run on OS 64 Bits platform

BDD engine :

- **ARALIA 4 (512 GB of ram memory)**
- **Cecilia BDD (512 GB of ram memory)**

RESEARCH STUDIES

CHALLENGES FOR FUTURE RESEARCH

Algorithm improvement

- Boolean equation generator to be able to handle loop system.
- BDD engine (allowing to find MCS of order 4 for big and complex system)
- New Computing cluster

- Merging results coming from MBSA/FTA Studies

Connection with Requirements tools or MBSE tool

- 3D exp connector

Improving the methodology to build model

- Defining the criteria for the deepness of the model
- What kind of information have to be included in the model.