Feedback on application of an MBSE Approach to an Avionics Subsystem following SAE ARP4754 practices

SSSE

13 January 2021 - Raphael Faudou

Agenda

- Context of the mission
- MBSE approach overview
  - Motivations and Principles
  - Structure of functional needs
  - Definition of functional interfaces and functions
  - Refinement of functions down to components
  - Functional simulation of operational scenarios
- Lessons learned from applying MBSE approach
  - Lessons learned on following approach step by step
  - Drawbacks of MBSE over document centric approach
  - From MBSE learning to adoption challenges
- Conclusion

SAMARES ENGINEERING
Accelerate Systems Design

Context

COMAC and MBSE…

- Mission was initiated by the Commercial Aircraft Corporation of China

- Goal : learn and apply an MBSE approach on an avionics subsystem
  - With one constraint: comply with the SAE ARP4754A

SAE Aerospace An SAE International Group	AEROSPACE RECOMMENDED PRACTICE	SAE ARP4754	REV. A
		Issued 1996-11 Revised 2010-12	
		Superseding ARP4754	
(R) Guidelines for Development of Civil Aircraft and Systems			

- COMAC hired MBSE experts including *ColleSys* and *Samares Engineering*
  - *ColleSys* defined the initial state of the art on MBSE and mission scope
  - *ColleSys* captured the current engineering practices and defined the Use Case
  - *Samares Engineering* provided training, coaching and support on MBSE approach

SAMARES ENGINEERING
Accelerate Systems Design

The Commercial Aircraft Corporation of China, Ltd (COMAC)

COMAC
中国商飞

- Founded in 2008 in Shanghai
- Registered capital of RMB 23 Billion.

- Headquarters in Shanghai Expo Park

SHAREHOLDERS

- State-owned Assets Supervision and Administration Commission of the State Council
- Aviation Industry Corporation of China
- China Aluminum Corporation
- Shanghai Guosheng (Group) Co., Ltd
- Baosteel Group
- Sinochem Group

Main Products

- **ARJ21-700 Regional Jet Program**
- Range: 1200-2000 nm
- Max Takeoff Weight: 40500kg
- Seat Capacity: 78 – 90
- Orders: 473 from 22 customers
- First Deliver to Chengdu Airline: 29th Nov. 2015

- **C919 Program**
- Range: 2200 - 3000 nm
- Max Takeoff Weight: 72500kg
- Seat Capacity: 156 – 174
- Orders: 815 from 28 customers
- Maiden Flight: 5th May. 2017

- **CR929 Program**
- Range: 8000 - 10000 nm
- Max Takeoff Weight: 240000kg
- Seat Capacity: 280 – 320

Beijing Aeronautical Science and Technology Research Institute(BASTRI)

Establishment time: 26th Feb, 2010

Vision: World-class research institution for civil aviation

Mission:

- Strategic planning research
- Future product planning
- Key technology research
- Technology integration verification
- Foresight technology exploration

Samares Engineering in a few words…(1)

- Activities
  - Methods and tools for engineering
  - Research and technologies with publications: ERTSS, CSDM, ASTC, CJA,
  - Initial and continuous training

- Expertise domains
  - Systems Engineering for critical and complex systems including **requirement engineering** and **architecture definition**
  - **Model-Based Systems Engineering** (method, process and tooling) –customization / deployment / coaching / support
  - Simulation and co-simulation
  - Product Line Engineering (PLE) with models

Certified SE Professionals

Capella

pure::variants

SAMARES ENGINEERING
Accelerate Systems Design

Samares Engineering in a few words…(2)

Research

GROUPE ISAE
World leader in aerospace engineering higher education and research

IRT SAINT EXUPERY

AFIS Association Française d'Ingénierie Système

INP ENSEEIHT

Industry

AIRBUS

中国商飞 COMAC

SAFRAN

OBEO Honeywell

LATECOERE

Rockwell Collins

AVIC

RENAULT

NAVAL GROUP

EDF

Schneider Electric

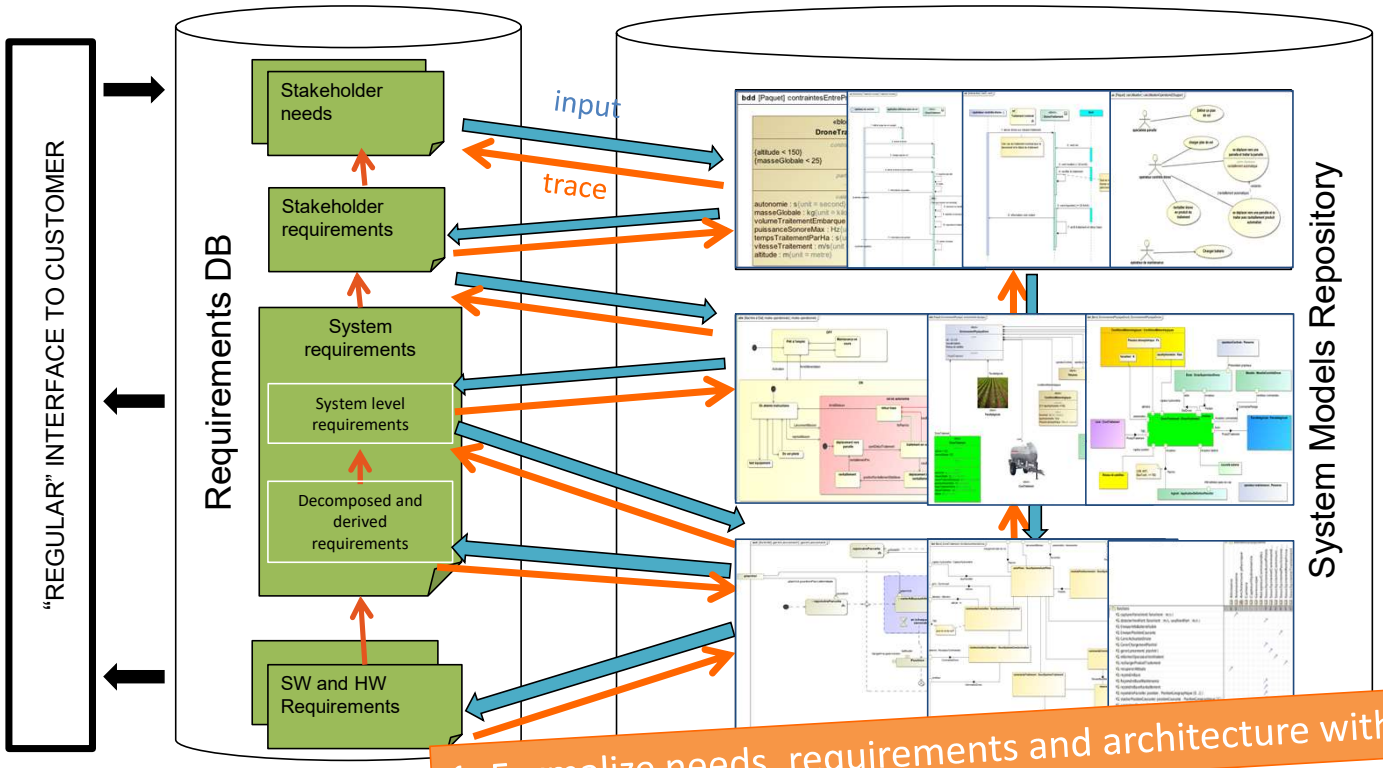
AIRBUS DEFENCE & SPACE

CIRTEM POWER OPTIMISED

- Located in Toulouse

SAMARES ENGINEERING
Accelerate Systems Design

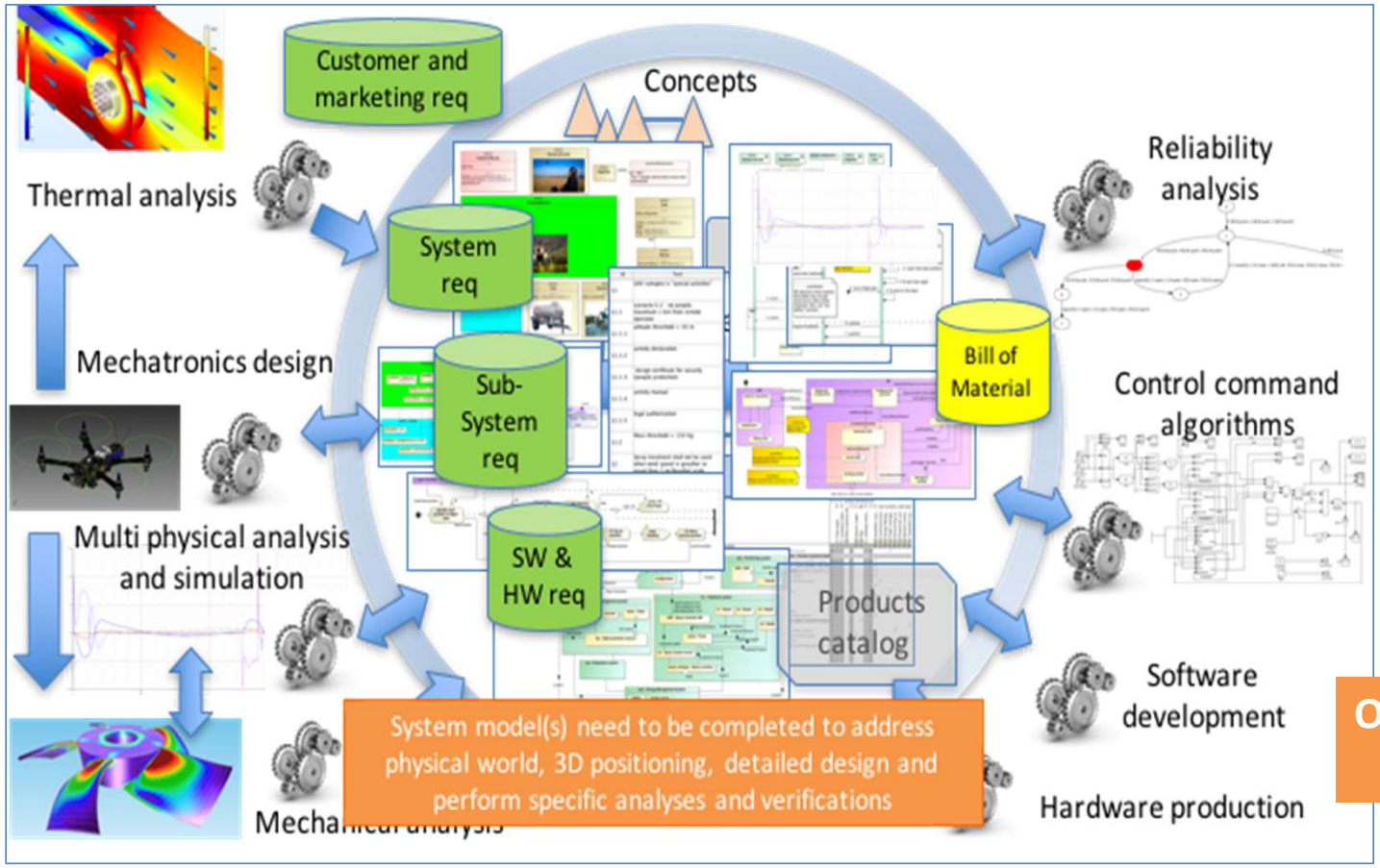
Our vision of MBSE…(1)



1. Formalize needs, requirements and architecture with models
2. Derive requirements from models (for SW and HW)
3. Ensure consistency and end to end traceability through models

SAMARES ENGINEERING
Accelerate Systems Design

Our vision of MBSE…(2)



Our focus: digital continuity and co-simulation

SAMARES ENGINEERING
Accelerate Systems Design

MBSE approach overview

Motivation for transitioning to MBSE

- MBSE can be used for many purposes…
  - Improve communication, better description of architectures, ease analysis…

- Main motivation in this mission was in fact to « *accelerate requirements maturity* » = reach good-quality requirements at first iteration

SAE Aerospace
An SAE International Group

AEROSPACE RECOMMENDED PRACTICE

SAE ARP4754 | REV. A

Issued 1996-11
Revised 2010-12

Superseding ARP4754

(R) Guidelines for Development of Civil Aircraft and Systems

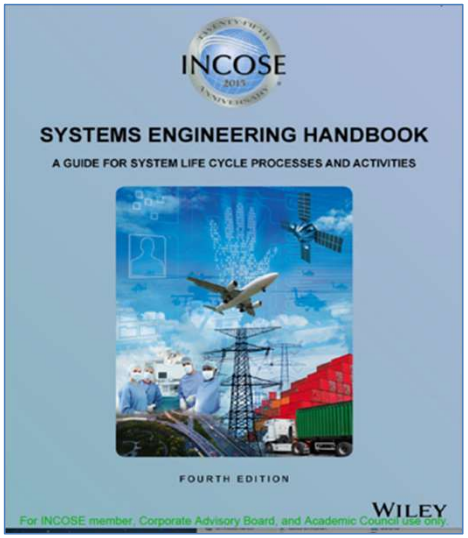
Correctness *is the degree to which an individual requirement is unambiguous, verifiable, consistent with other requirements and necessary for the requirement set.*

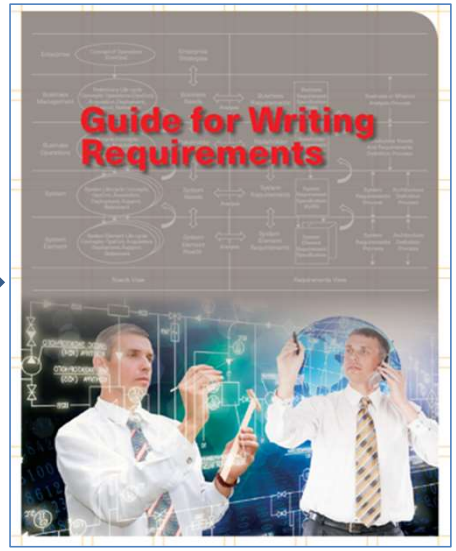
Completeness *is the degree to which a set of correct requirements, when met by a system, satisfy the interests of customers, users, maintainers, certification authorities as well as aircraft, system and item developers under all modes of operation and lifecycle phases for the defined operating environment*

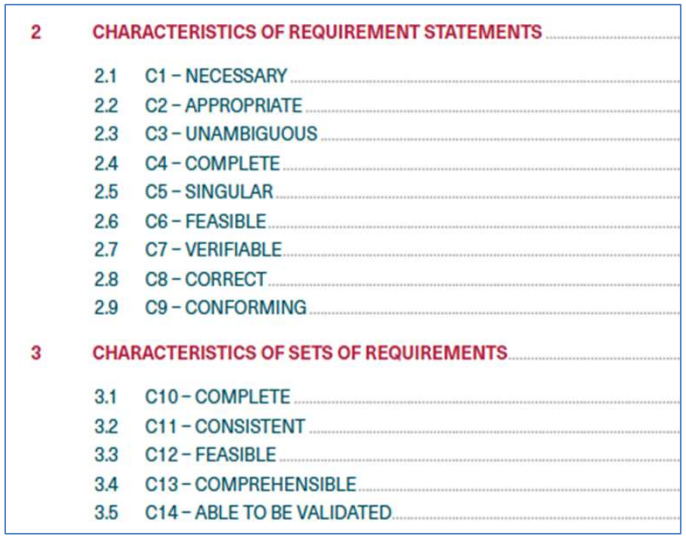
SAMARES ENGINEERING
Accelerate Systems Design

Motivation for transitioning to MBSE

- Note: even when SAE ARP4754A is not applicable (others domains), this motivation about “requirement quality” remains valid…







2 CHARACTERISTICS OF REQUIREMENT STATEMENTS

2.1 C1 – NECESSARY
2.2 C2 – APPROPRIATE
2.3 C3 – UNAMBIGUOUS
2.4 C4 – COMPLETE
2.5 C5 – SINGULAR
2.6 C6 – FEASIBLE
2.7 C7 – VERIFIABLE
2.8 C8 – CORRECT
2.9 C9 – CONFORMING

3 CHARACTERISTICS OF SETS OF REQUIREMENTS

3.1 C10 – COMPLETE
3.2 C11 – CONSISTENT
3.3 C12 – FEASIBLE
3.4 C13 – COMPREHENSIBLE
3.5 C14 – ABLE TO BE VALIDATED

Why would MBSE help to mature requirements?

- Because MBSE relies on using a standardized notation (language) with semi-formal semantics and graphical support, that helps highlighting issues early in the cycle

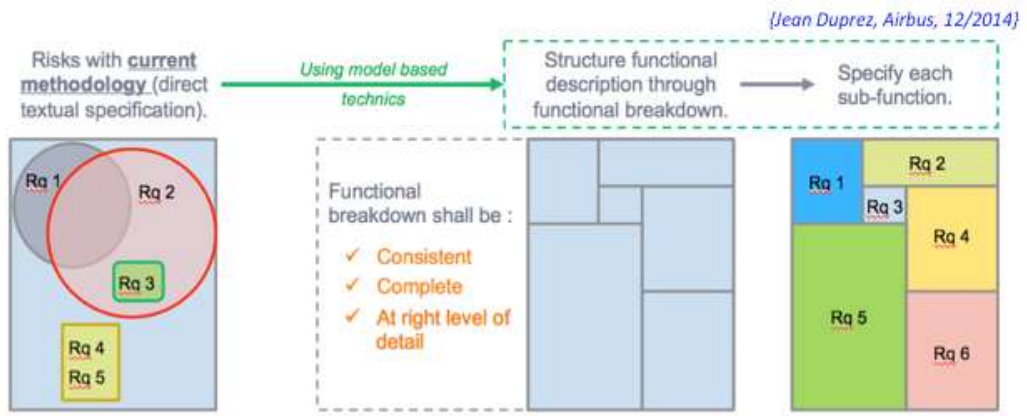
- Let us focus on consistency, which is one of the hardest challenges
  - Can you ensure that there is no conflict between 1,000 requirements?
  - Can you afford to review the total combinatory of requirements?
  - Think about numbers: 1,000 req mean 1,000,000 checks…… so you will check consistency partially.

- Can a modeling language help on consistency?
  - YES ! Diagrams provide local consistency of concepts (by construction)
  - But a language/notation is not enough reach global consistency…

- We need more than a language: an MBSE methodology, or at least an MBSE approach !

Key principles of our recommended MBSE approach

1. Based on System Modeling Language (Standard and powerful notation)
2. Function-based definition (prescribed by ARP4754A)
3. Support of functional simulation to ease early validation
4. Support of bidirectional traceability (Certification & Change Management)
5. Consistent-by-construction (all elements are connected)



SAMARES ENGINEERING
Accelerate Systems Design

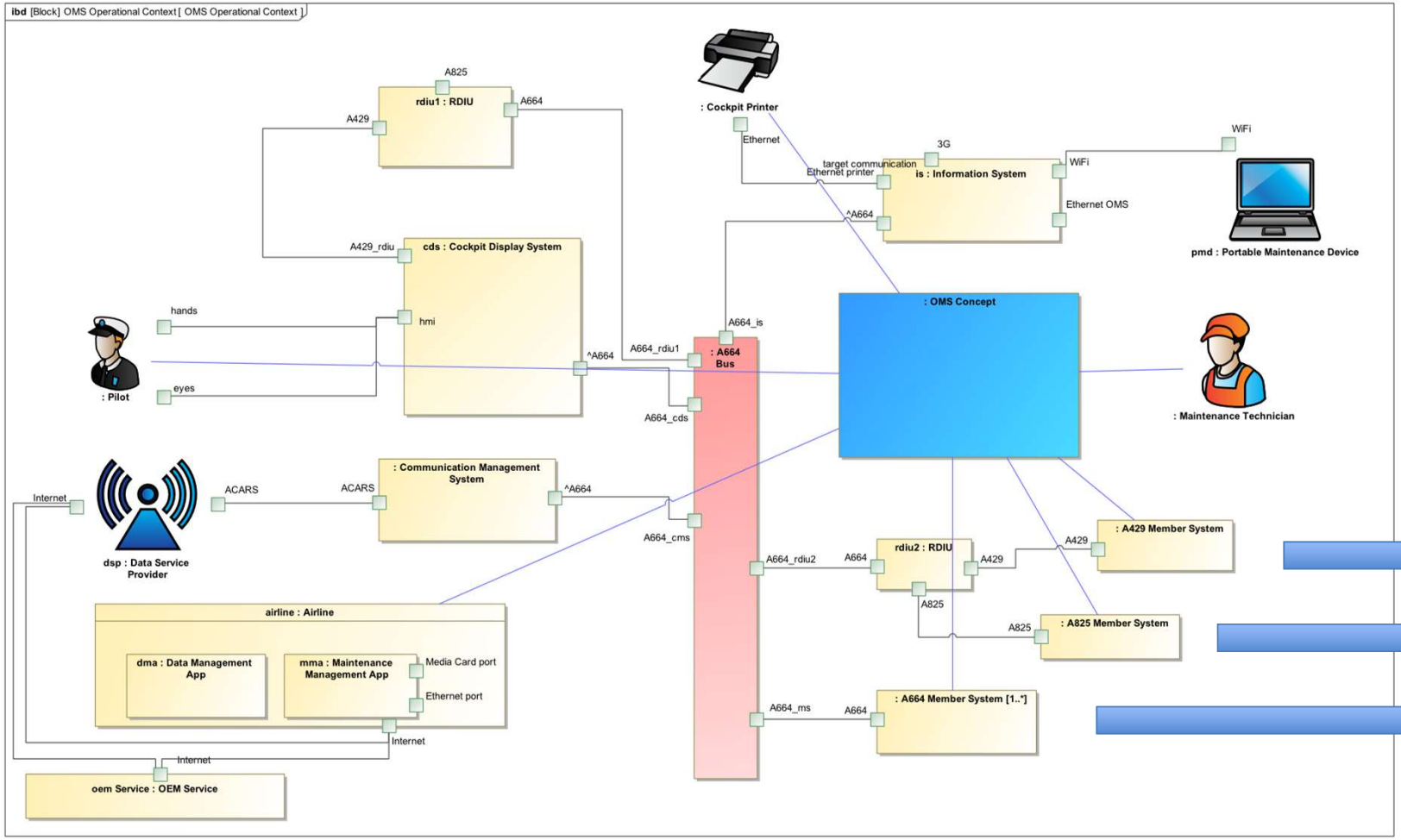
Quick overview of the pilot case (1)

- The OMS is a software intensive avionics system that monitors the health of the aircraft during the flight.

- **Expected functions**
  - Monitor continuously aircraft avionics during flight
  - Analyze faults and diagnosis of the root cause
  - Perform fault correlation and alert crew
  - Inform maintenance crew of needed repairs
  - Perform on-ground testing on aircraft avionics

- **Connected systems (called “Member Systems”)**
  - Flight Control, FMS, DOORS, APU, IMA, Oxygen System, Propulsion, Landing Gear, Fuel & Hydraulics, Water & Waste, Lighting,...

Quick overview of the pilot case



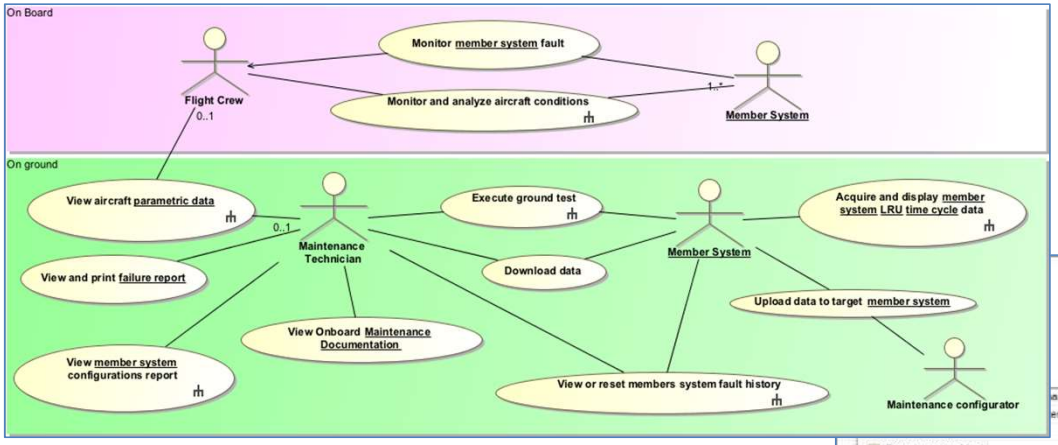
“Member Systems”

- DOORS
- APU
- Flight Control
- FMS
- IMA
- Oxygen System
- Propulsion
- Landing Gear
- Fuel & Hydraulics
- Water & Waste
- Lighting
- ...

SAMARES ENGINEERING
Accelerate Systems Design

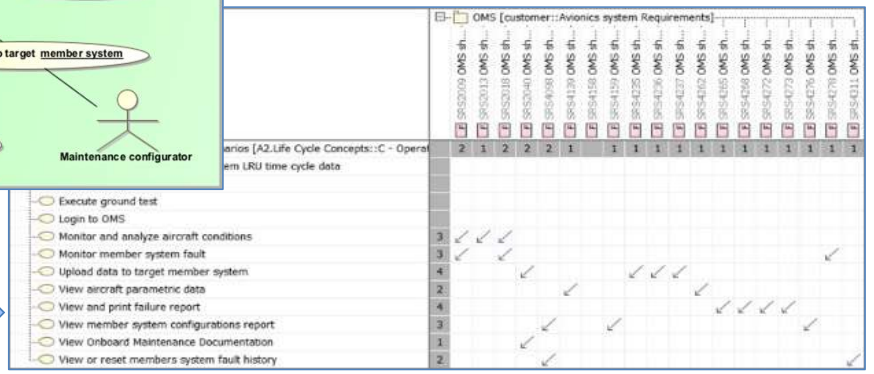
Structure of functional needs (1)

- Use Cases (UC) structure input requirements
  - A UC ensures completeness of a functionality and will be used as container to organize validation scenarios ➔ useful for both definition and validation activities
  - Actors provide functional boundaries (functional scope of the **S**ystem **o**f **I**nterest)



Note: as UC are independent of each other, a UC is a good unit for collaborative work

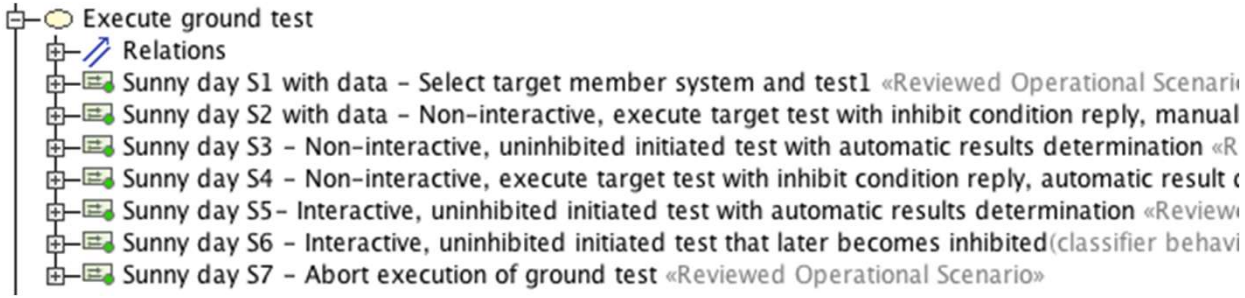
Traceability to input (textual) requirements

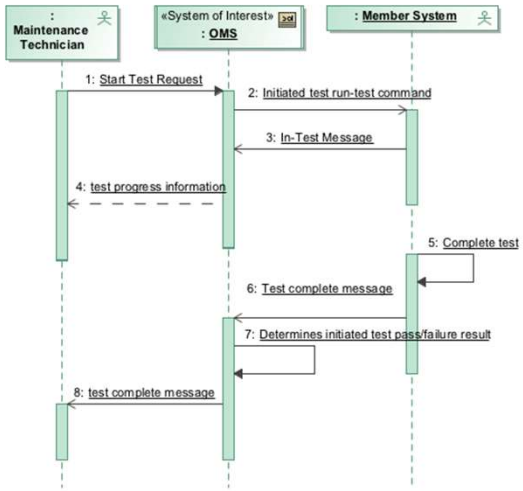


SAMARES ENGINEERING
Accelerate Systems Design

Structure of functional needs (2)

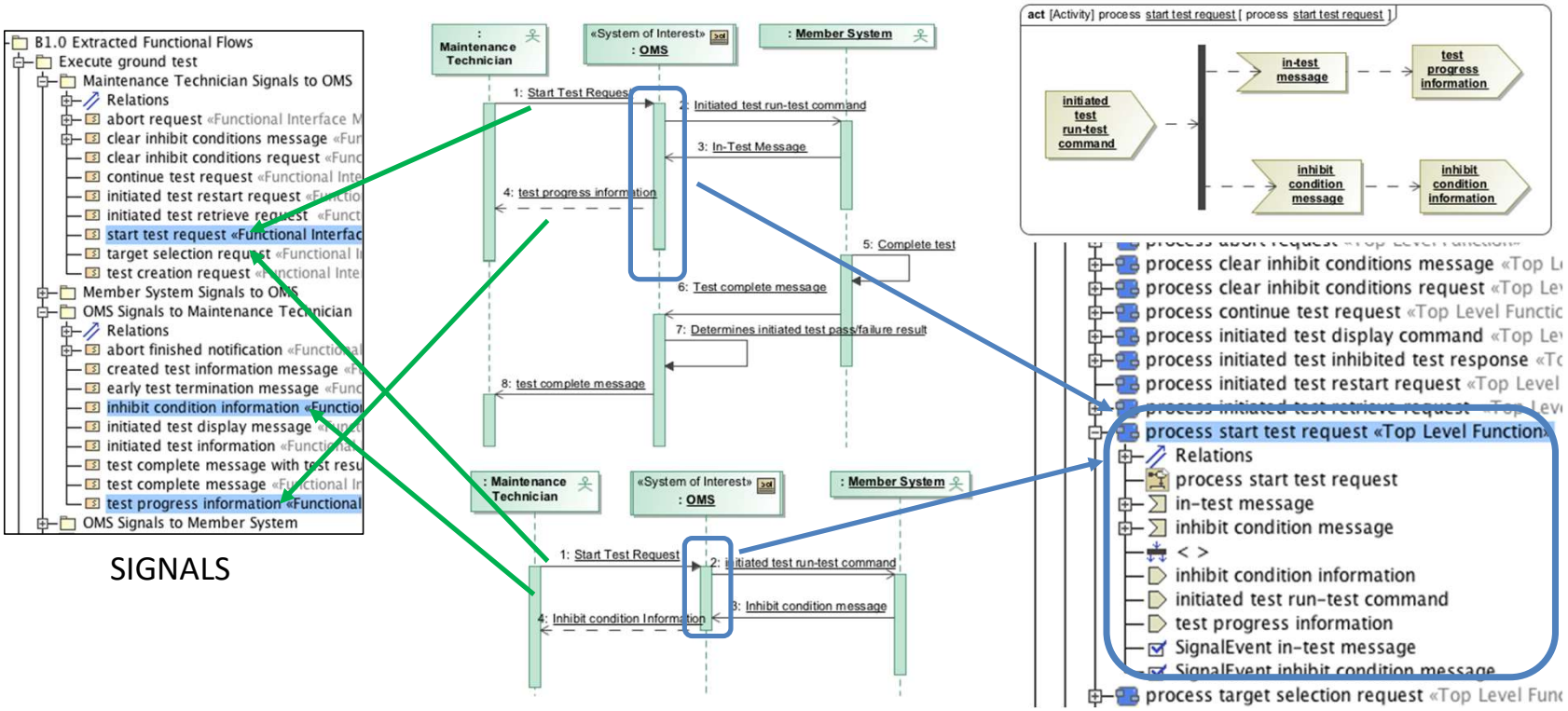
- UC is a scenarii umbrella and provides guidance
  - Same scope and same start for all scenarii => can detect inconsistencies
- Scenarii capture all nominal and non-nominal behaviors (completeness) with focus on interactions, that will lead to external interfaces…
  - Easy to validate by users
  - Straight forward translated into validation scenario skeletons
  - Can be completed at any time





SAMARES ENGINEERING
Accelerate Systems Design

Definition of functional interfaces and top-level functions (1)



SIGNALS

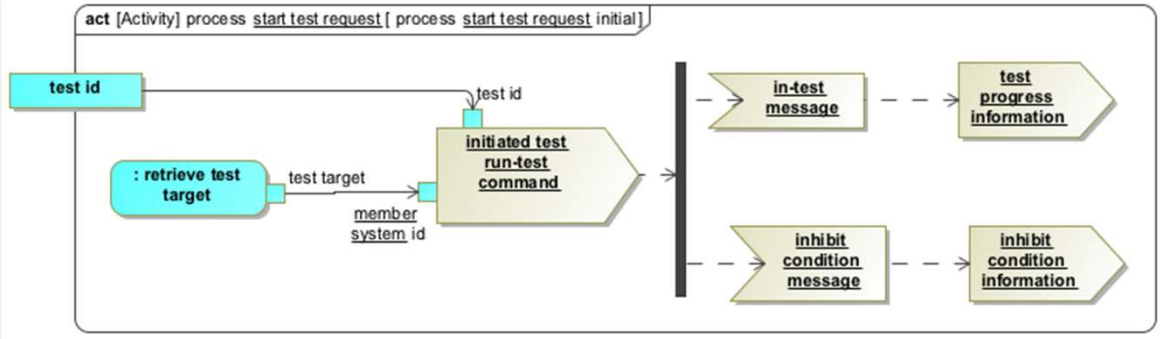
We use a pattern to identify top-level functions and system functional interfaces from intended scenarii (usages)

- Scenario is focused on capture of top-level functions and interactions
- We do not consider logics at this stage
- Idea is to ensure it remains simple enough to be validated by end users

SAMARES ENGINEERING
Accelerate Systems Design

Definition of functional interfaces and top-level functions (2)

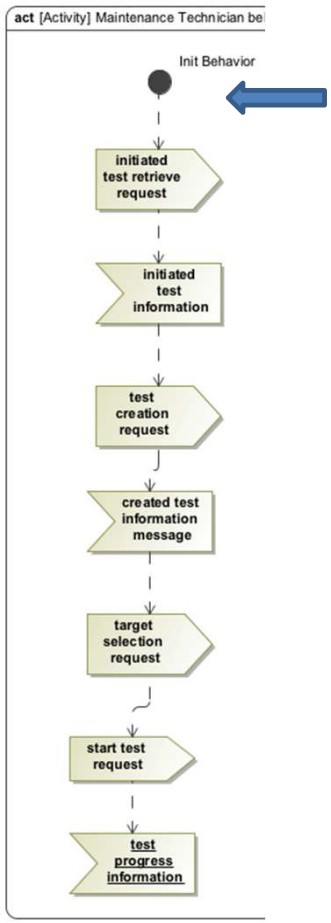
- Once identified, top-level functions are completed
  - Definition of their inputs and outputs
  - Functional flows between elements
- Data continuity principle:
  - each function input either comes from parent function input or from another function output

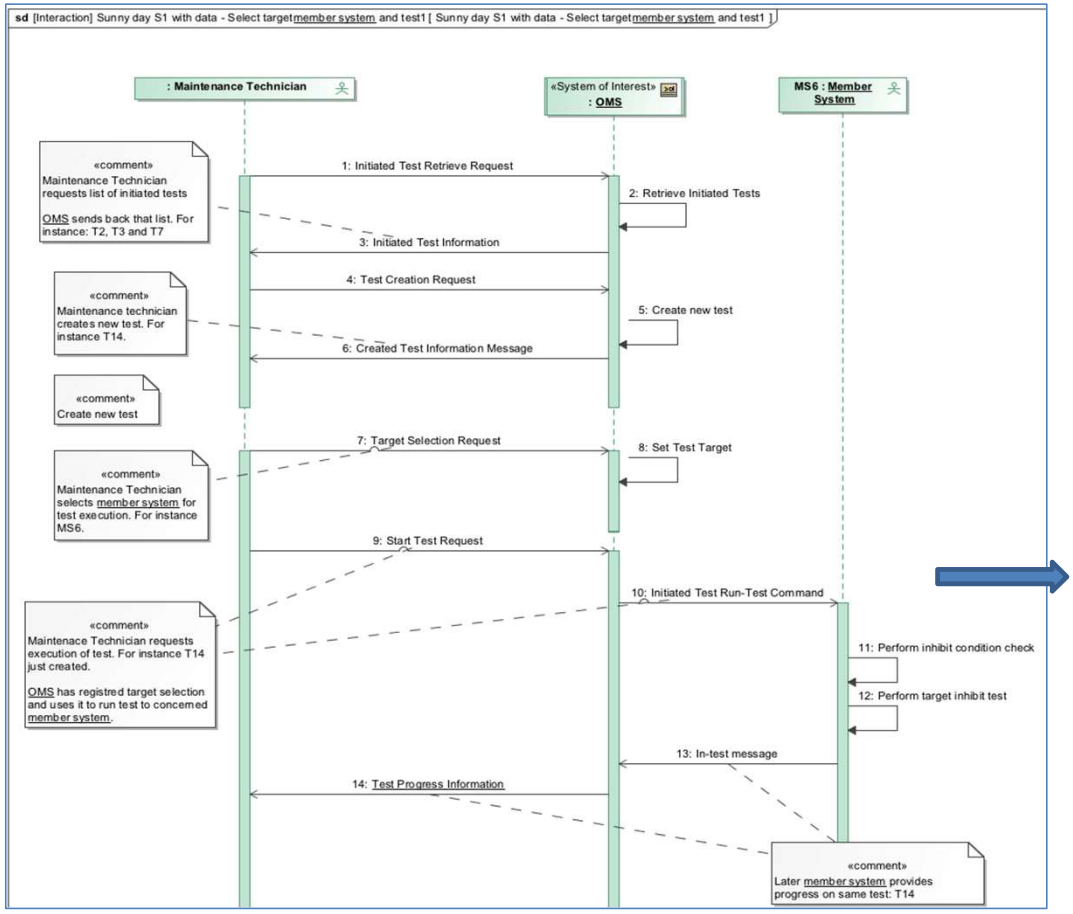


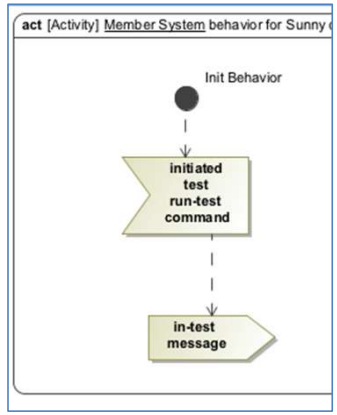
Tool (plugins) can helps detecting holes and inconsistencies in data continuity

SAMARES ENGINEERING
Accelerate Systems Design

Scenarii can be simulated at any time- example (1)



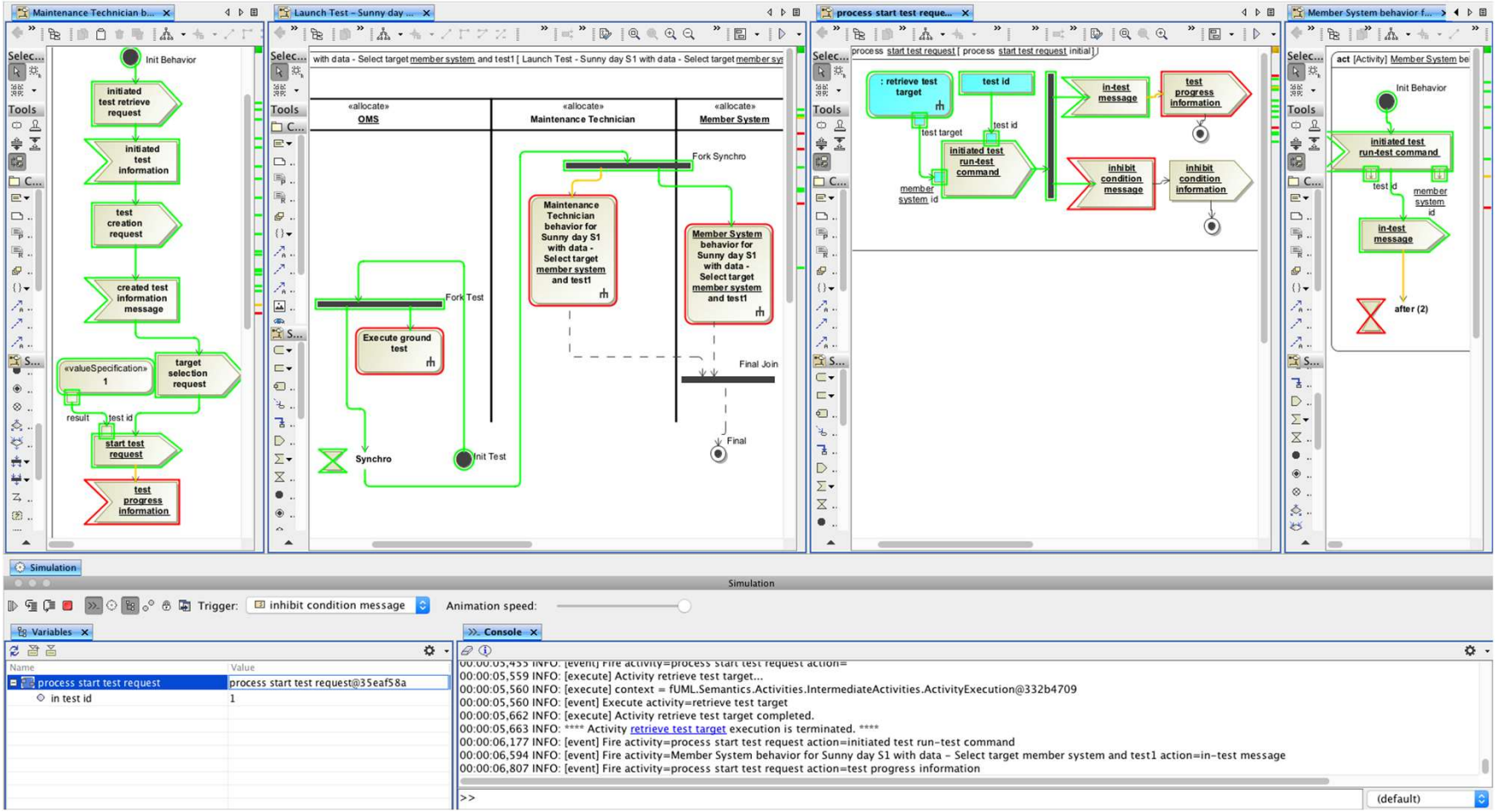




Each scenario is translated to emulate actor interactions: each actor interaction is translated into the senging or reception of a signal

SAMARES ENGINEERING
Accelerate Systems Design

Scenarii can be simulated at any time- example (2)



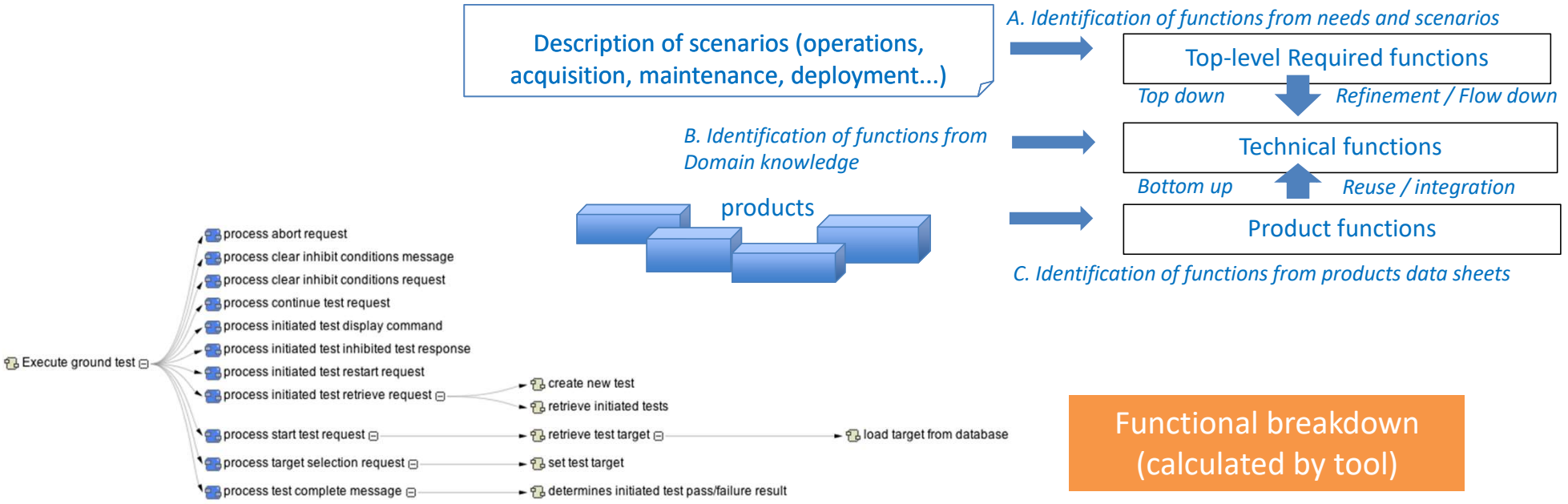
Each scenario can now be run to “stimulate” the functional behaviour of the system.

Here we see a snapshot or simulation with a scenanario almost ended

SAMARES ENGINEERING
Accelerate Systems Design

Refinement of functions down to allocation on products

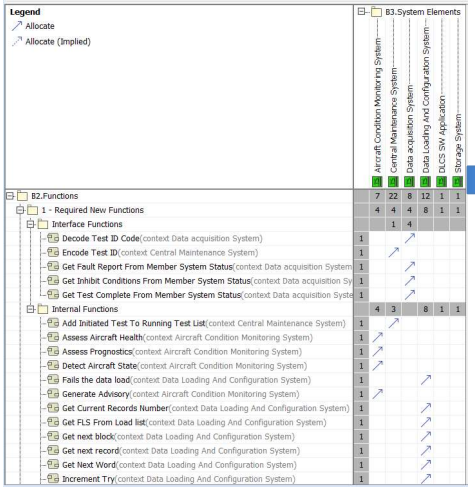
- Each function behavior is refined with calls to lower-level functions until:
  - Either the function can be fully allocated to a product available on the market
  - Or it is fully understood from its specification (and can be sub-contracted)



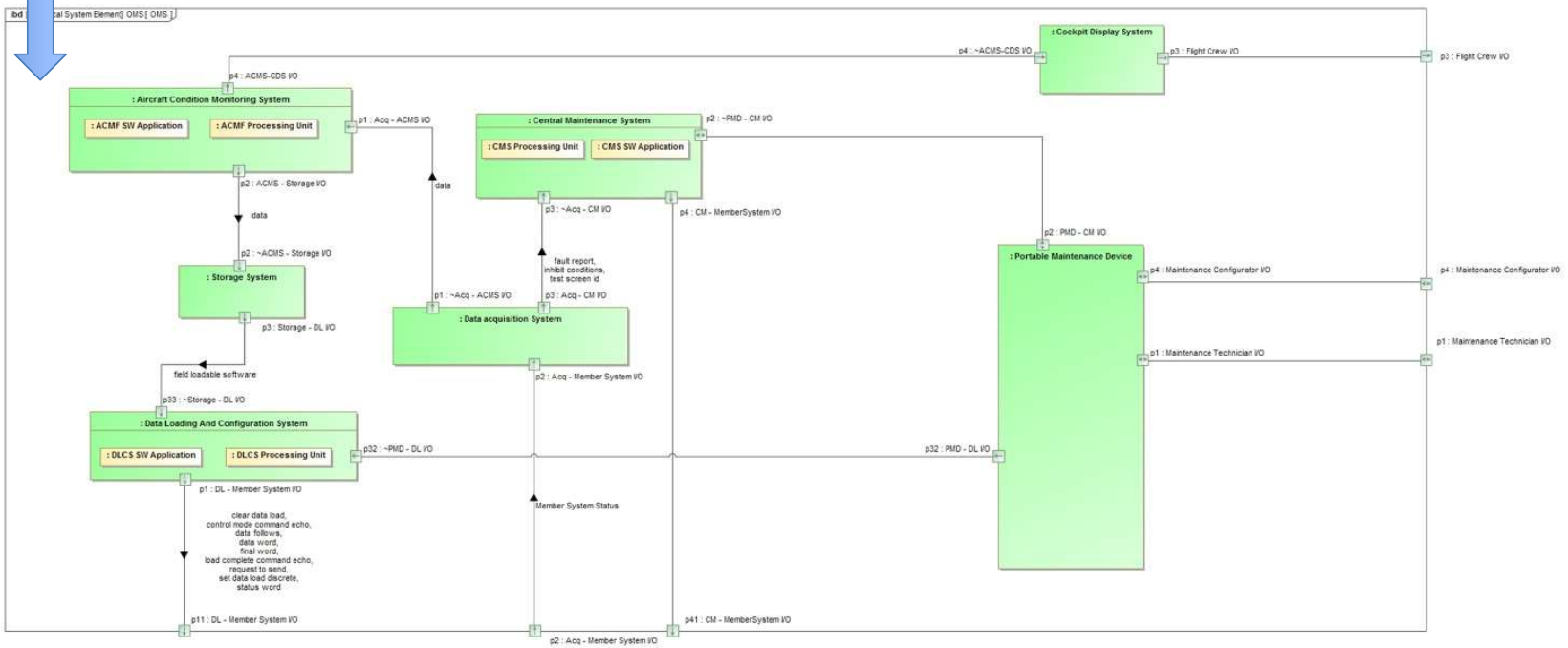
Functional breakdown (calculated by tool)

SAMARES ENGINEERING
Accelerate Systems Design

Derivation of functional flows into component flows



Some component flows can be deduced from functional architecture and allocation on system elements- **partially automated**

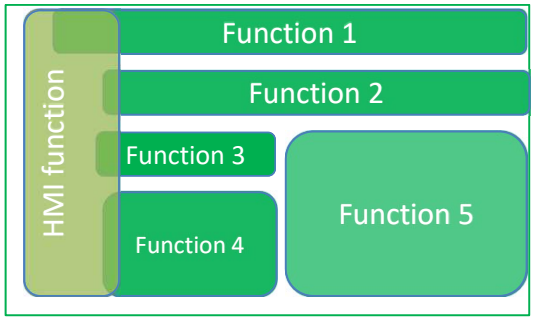


SAMARES ENGINEERING
Accelerate Systems Design

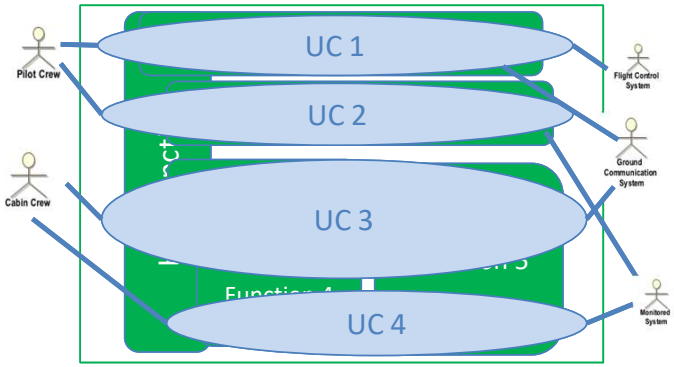
Lessons learned

1. Take your time to identify the “GOOD” use cases (right grain)

- Starting from aircraft-level functions allocation does not necessarily help in finding right Use Cases...
- ... as those functions may have not the right UC properties (“complete” and “user-oriented functionality”)



Functions are organized from technical point of view and must collaborate to provide services

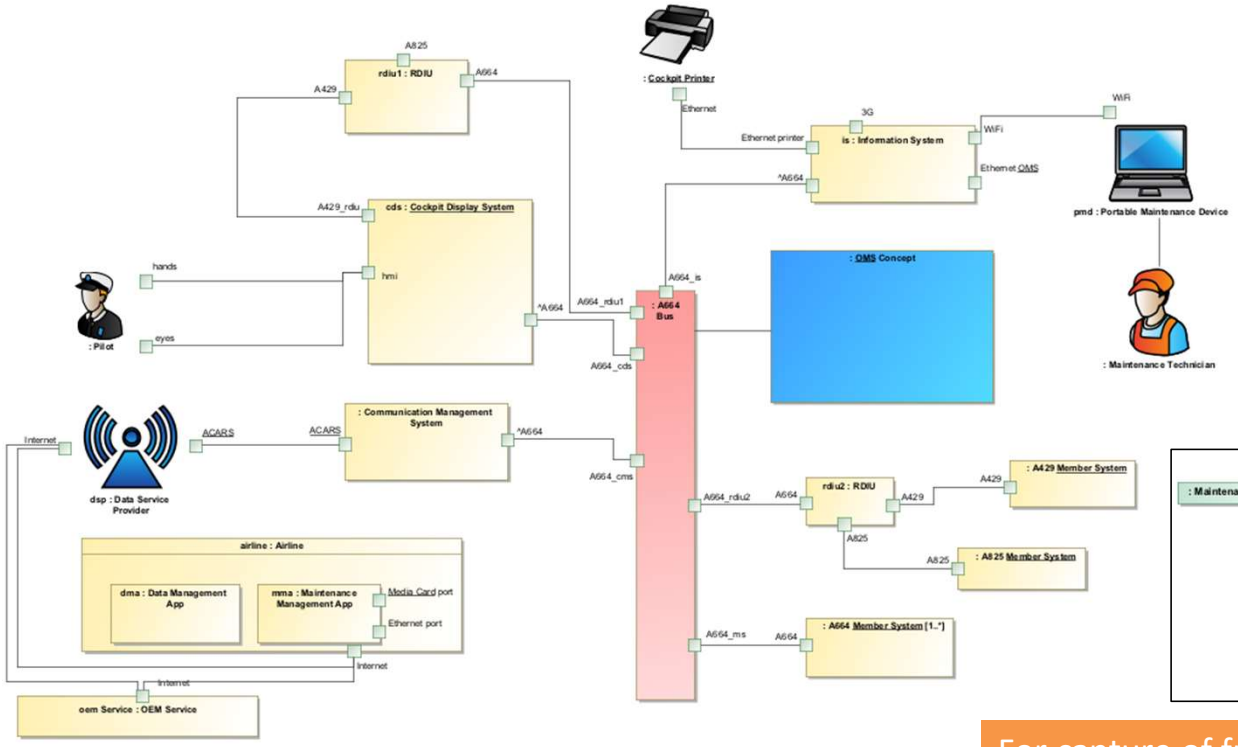


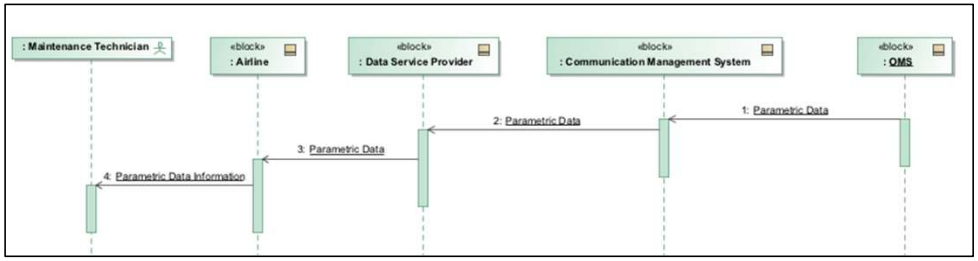
Use Cases are “user oriented” and contain exchanges with actors (outside of the system by definition) – And they are independent by definition

SAMARES ENGINEERING
Accelerate Systems Design

2. Use actors instead of real systems (more flexible)

- It was not always easy to identify roles instead of routes





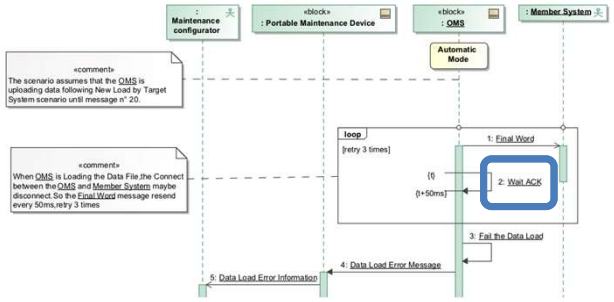
For capture of functional messages, intermediate route points are not useful (redundant messages) ➔ need to abstract from existing routes

SAMARES ENGINEERING
Accelerate Systems Design

3. Keep scenarii at functional level and simple

1. Avoid describing many cases into one Sequence Diagram
   - Hard to review and validate

2. Do not introduce non-functional requirements at this stage
   - Introduces design solution and brings lot of useless debates



SAMARES ENGINEERING
Accelerate Systems Design

4. Teamwork support is not an option for collaborative work

- UC are good means to isolate functional analysis into independent streams
- But after some time, technical functions are shared and require ability to work on SAME model
  - Centralized unique model is key
  - Use of collaborative tool becomes mandatory
- Team completed the use of Cameo Systems Modeler with Teamwork Cloud solution
  - Provides shared access (centralized database with locking)
  - Provides version control (commit, update…)
  - Supports configuration management (trunk, branches, revisions…)

Main captured benefits in applying (this) MBSE approach

- helped structuring textual upstream requirements and raised a lot of questions about clarity, completeness and consistency
  - Some of those issues would have been missed by pure textual analysis (document-based approach)
- Agility in the management of changes
  - Could add new scenarios at any time and deduce new functions or changes in some functions
- Ability to support early functional validation
  - When functional data are connected, simulation is possible

Main captured drawbacks in applying (this) MBSE approach

- Learning curve was not trivial
  - Team had to learn modelling language while understanding and following MBSE methodology and learning the tool.
- Use of models for specification means additional efforts to manage traceability
  - Must manage traceability from upstream textual requirements to model elements
  - And then manage traceability from those model elements to lower-level textual requirements

From MBSE learning to adoption - challenges

- Significant efforts to align team
  - Align skills on notation (language), methodology, and tool
  - Practice on real cases to face modeling challenges
- Invest on a collaborative modeling solution
  - Team has to work on common model elements very soon
- Ensure available coaching and support by experts
  - Experts on avionics domain
  - Experts on systems modeling notation and methodology
- Model view layout may become an issue when scaling
  - Some diagrams are hard to maintain- think about automation
  - Use of matrix or other views to edit, review, check data

Thanks for your attention !

MBSE can provide very strong benefits ! But this is a long route … and many do not know the direction…

We can have fast quick wins if we know the « pain points » and use MBSE as a strategy to tackle those pain points

SAMARES ENGINEERING
Accelerate Systems Design

Q&A

Raphael.faudou@samares-engineering.com