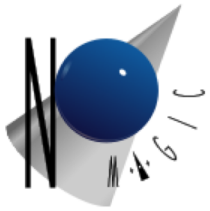


No Magic
EUROPEAN
CONFERENCE
5-6 JUNE 2018 TECHNIK MUSEUM SPEYER

BUILDING GOOD-QUALITY FUNCTIONAL SPECIFICATION MODEL

SPONSORS

A few words on Samares Engineering

SAMARES ENGINEERING
Accelerate Systems Design

- **Research and Consultancy on Systems Engineering**
  - Requirement engineering
  - Model-Based Systems Engineering
  - Co-simulation

INCOSE

AFIS Association Française d'Ingénierie Système

- **Mainly involved in avionics domain (but not limited to)**

AIRBUS

ZODIAC AEROSPACE

COMAC 中国商飞

Rockwell Collins

- **Strong links with high schools and research institutes**

GROUPE Isae
World leader in aerospace engineering higher education and research

INP ENSEEIHT

IRT SAINT EXUPERY

Agenda

SAMARES ENGINEERING
Accelerate Systems Design

- Challenges of « Good functional specification »
- MBSE approach to reach those challenges
- Demonstration

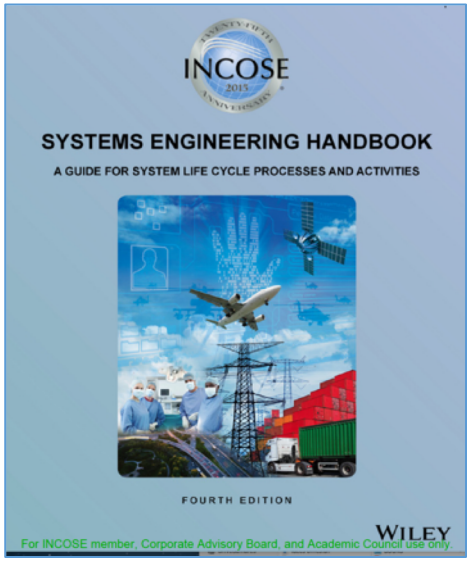
What is a « Good-Quality » specification ?

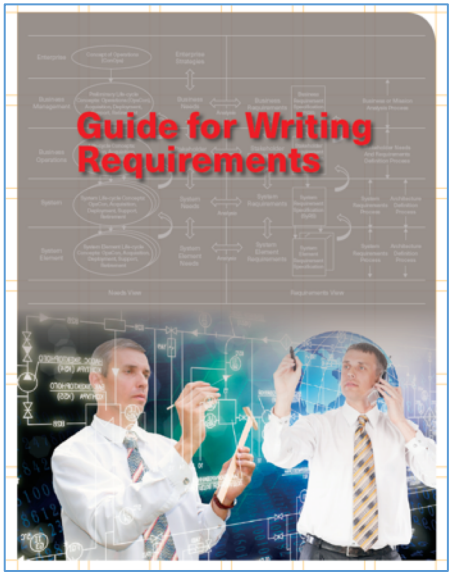
SAMARES ENGINEERING
Accelerate Systems Design

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*





Consistency is the strongest challenge

SAMARES ENGINEERING
Accelerate Systems Design

- **Can you ensure there is no conflict in 200 pages spec?**
- **Can you afford to review the total combinatory of req?**
  - Example: for 200 requirements it would mean 40 000 checks…
- **With rising number of requirements we need help !**
  - Models can help => A diagram provides "local consistency"
  - But it is not enough… we need to address also global consistency
- **Ultimate goal: reach "consistent-by-construction"**

Goal: define a MBSE methodology able to formalize requirements as connected model elements that make a consistent specification

Key principles of proposed MBSE approach

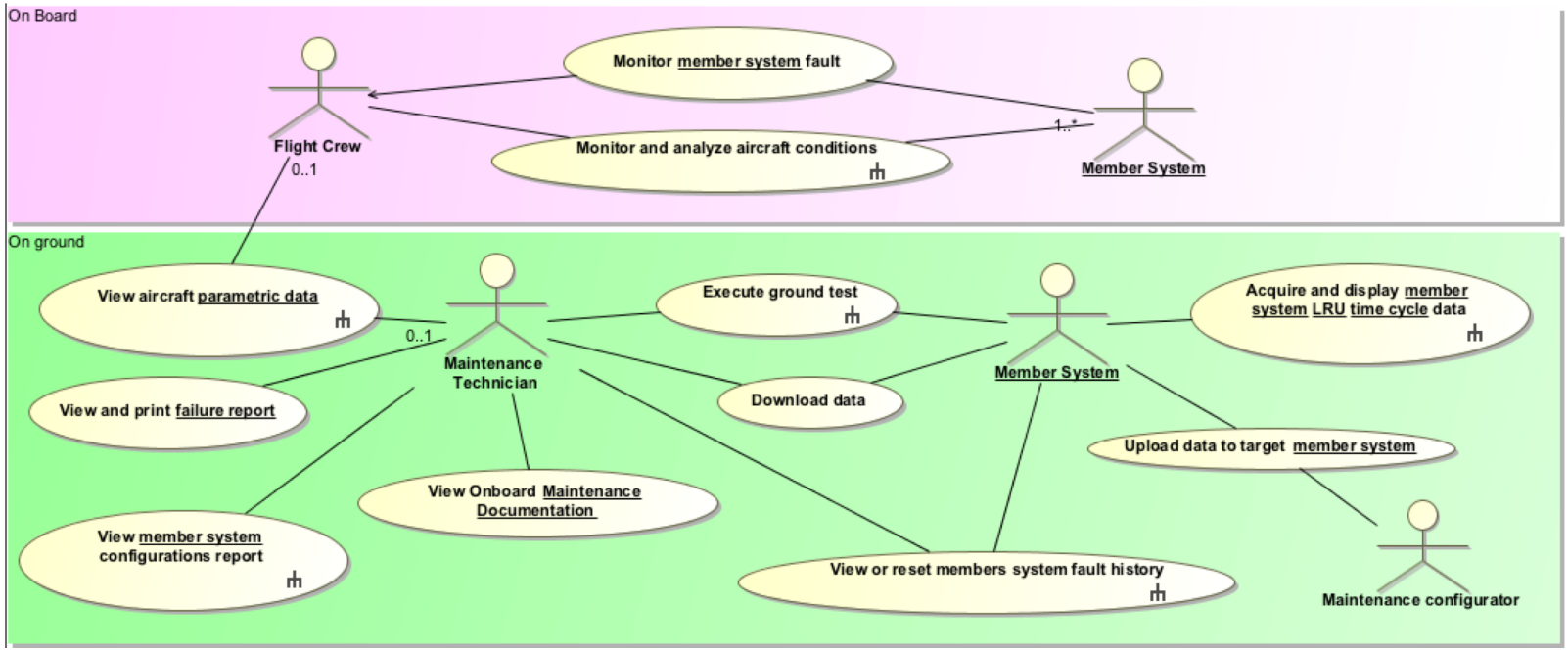
SAMARES ENGINEERING
Accelerate Systems Design

1. **Use of standard System Modeling Language**
2. **Function based definition (prescribed by ARP4754A) with support of recursive refinement (different levels)**
3. **Support of simulation to ease early validation**
   - Ability to run specification model in its operating context
4. **Support of bidirectional traceability**
   - Prescribed to reach avionics system certification
   - Useful for change management (key for long term sustainability)
5. **All elements connected (consistent-by-construction)**
6. **Agile approach (late new or changed requirements)**
7. **And obviously a Modeling Tool conformant to SysML**

Complete and correct requirements (1)

SAMARES ENGINEERING
Accelerate Systems Design

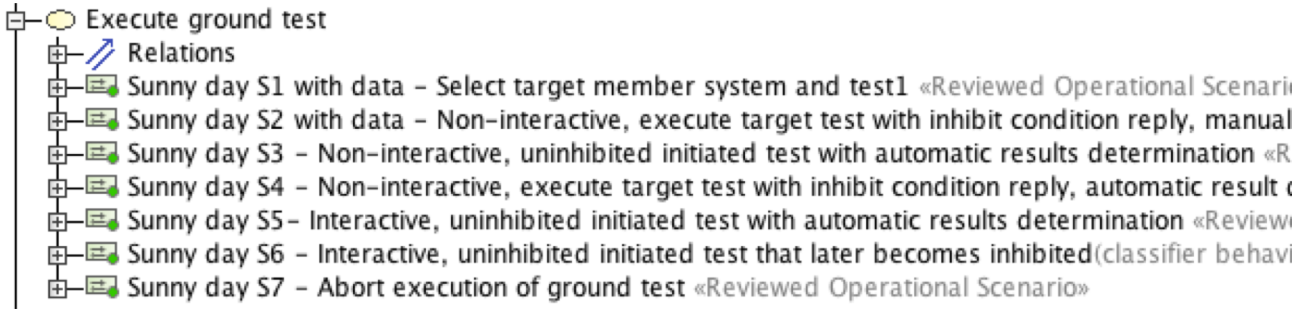
- **Suggestion #1: structure inputs into UC and actors**
  - Motivation 1: a UC provides goal for users (actors) and then ensures completeness of functionality. UC is the right container to organize future validation scenarios
  - Motivation 2: actors provide functional boundaries and then help ensuring that functional scope for system is correctly understood

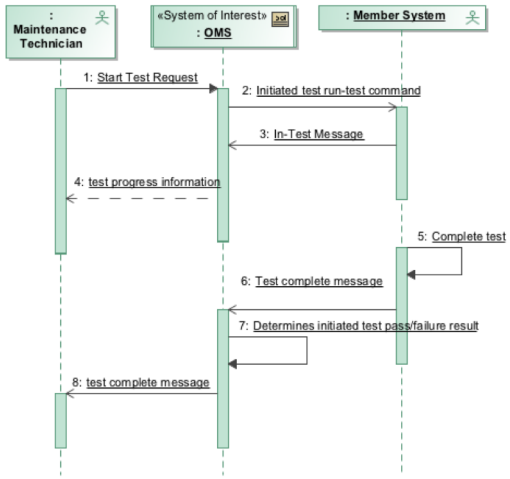


Complete and correct requirements (2)

SAMARES ENGINEERING
Accelerate Systems Design

- **Suggestion #2: use black box scenario-based approach**
  - Motivation 1: capture all intended normal and non-normal behaviors (completeness) with special focus on interactions ➔ can check ICD (necessary and sufficient functional interfaces)
  - Motivation 2: Capture abnormal behaviors (address safety)
  - Motivation 3: Scenarios are easy to review and validate
  - Motivation 4: straightforward derived into validation scenarios
- **UC is scenario umbrella and provides guidance**
  - Same scope, start, end, actors
  - Can detect inconsistencies early

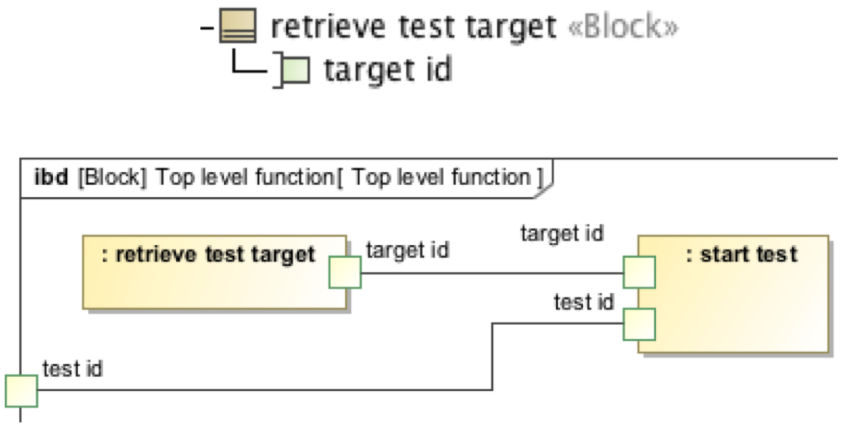


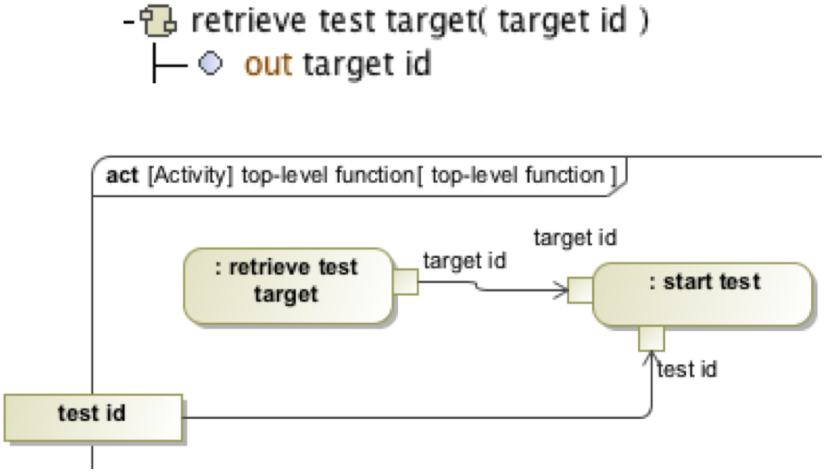


Which SysML concept for function?

SAMARES ENGINEERING
Accelerate Systems Design

- **Common SysML concepts to formalize a function**
  - *Block* or *Activity* for function definition
  - Respectively *Port* or *Parameter* for functional interface
  - Respectively *Part* or *Call Behavior Action* for function call (usage)
  - Respectively *Connector* or *Object Flow* for functional flow

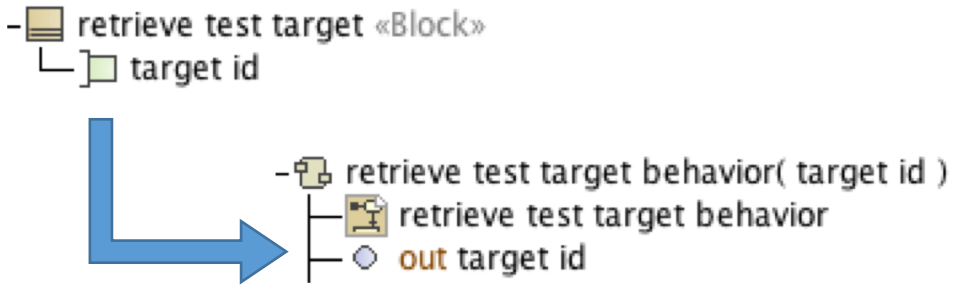




Function behavior (for simulation)

SAMARES ENGINEERING
Accelerate Systems Design

- **Function behavior = Activity or State machine (SM)**
  - If function is represented by *Block* and behavior is represented by *Activity* ➔ have to map *ports* and *parameters* at each level



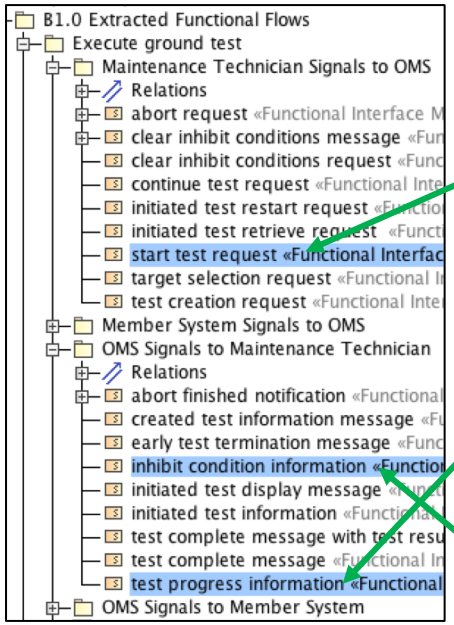
  - If function as *Block* and behavior as *State* machine, cannot see sub-functions in the behavior (less intuitive)

- **We choose to represent function as *Activity* as it can be completed with behavior consistently**

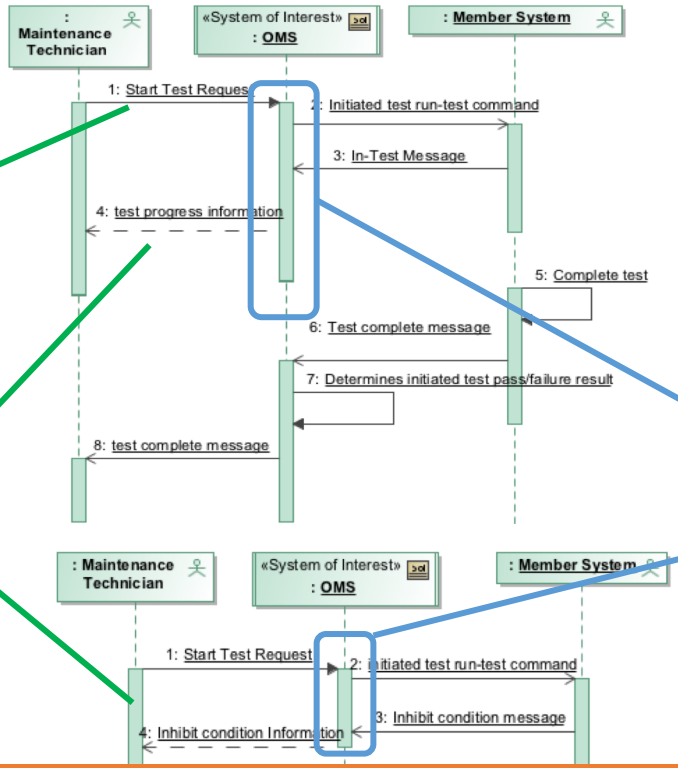
How to combine usages into 1 definition?

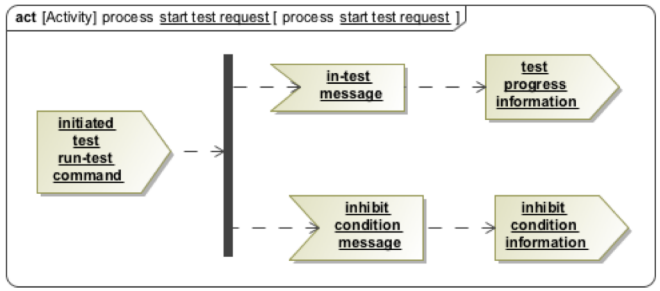
SAMARES ENGINEERING
Accelerate Systems Design

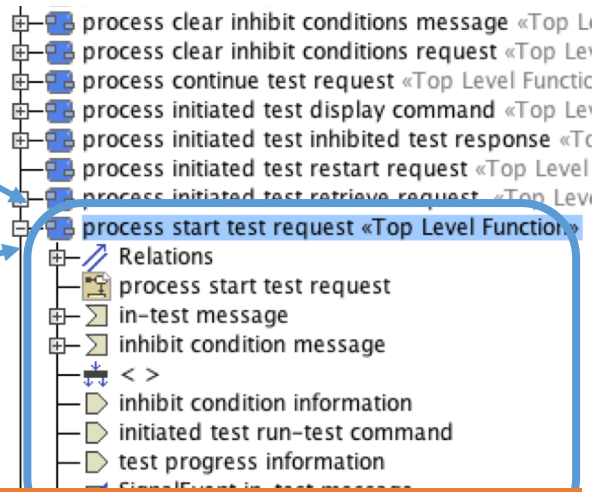
- Pattern to identify top-level functions and system functional interfaces from intended behaviors (usages)



SIGNALS







Scenario is focused on capture of top level functions and interactions, not on function logics
Idea is to ensure it remains simple enough to be validated and to leave logics for further stage

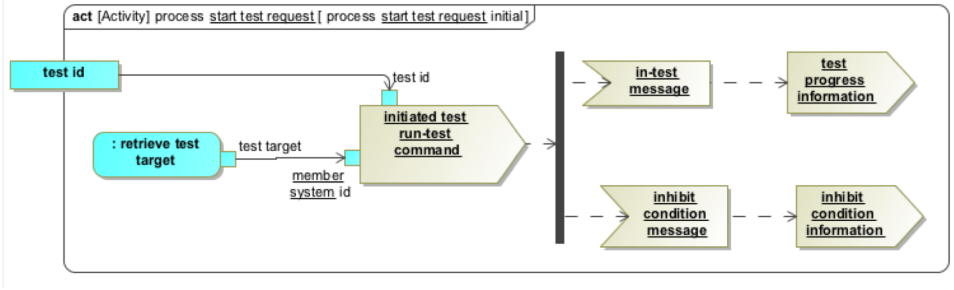
Then we use tool (plugin) to combine scenarios and define function required logics iteratively

Complete top-level functions and interfaces

SAMARES ENGINEERING
Accelerate Systems Design

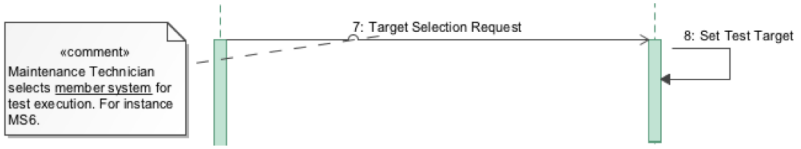
- **Once identified, top-level functions are completed**
  - Definition of their inputs and outputs
  - Functional flows between elements

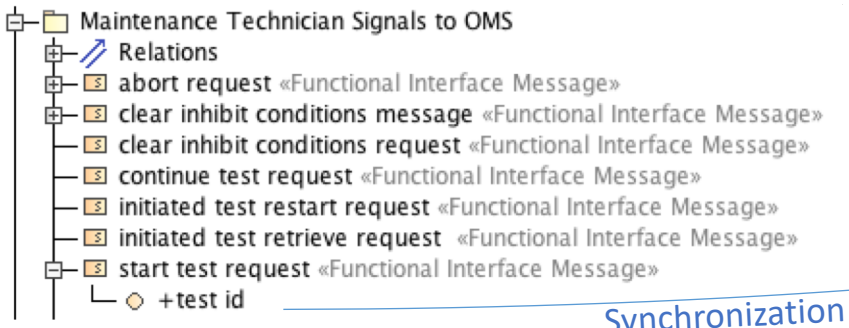
Data continuity guidance principle
- Each function input either comes from parent function input or from another function output
- For top-level function, inputs may come from input signal that triggered function => lead to update interface

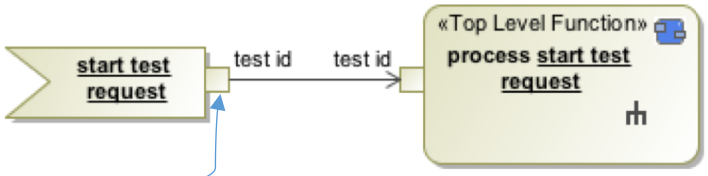


May lead to new functions

May lead to complete scenarios ➔ back to previous step





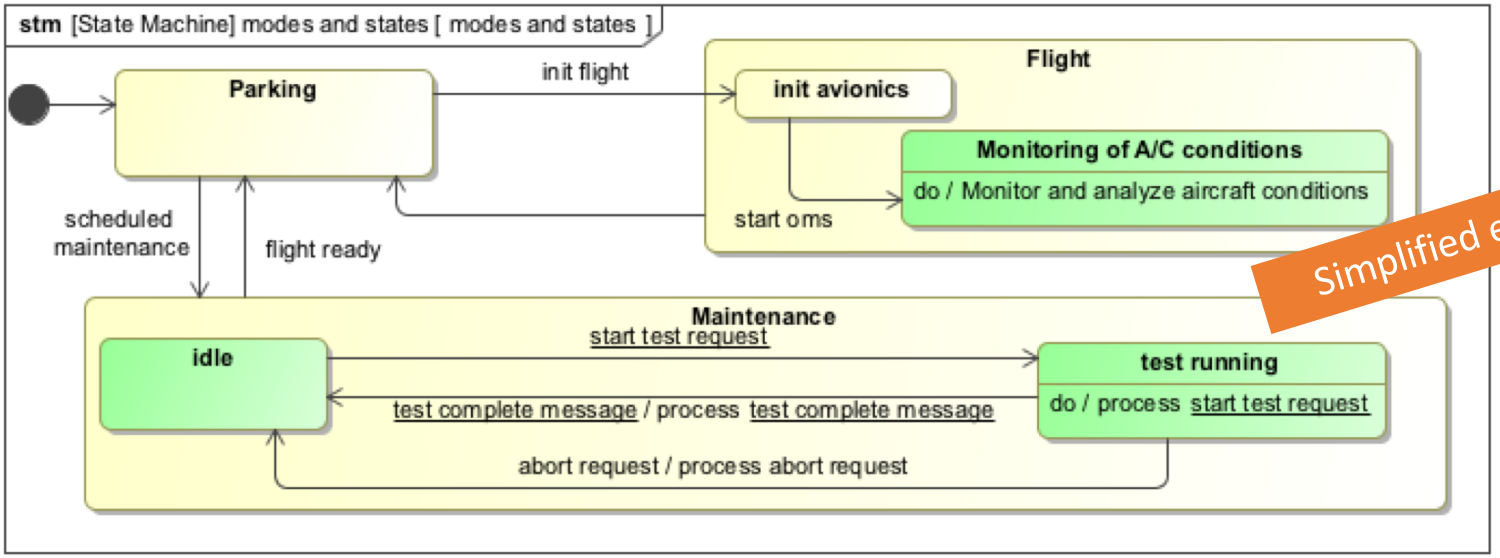


Synchronization ensured by Cameo

Specify function validity conditions

SAMARES ENGINEERING
Accelerate Systems Design

- **Functions are not valid at any time**
  - Have to specify conditions in which their activation is valid
- **We use state machine to represent mission states**
  - Input signals are put on transitions
  - Top-level functions set in states (doActivity) or on transition effect



Refine functions down to allocation

- **Each function is refined (realized with lower-level functions) down to the level where :**
  - Either it can be allocated to existing products
  - Or it is fully understood from its specification (no realization risk)

Description of scenarios (operations, acquisition, maintenance, deployment...)

A. Identification of functions from needs and scenarios

Top-level Required functions

Top down — *Refinement / Flow down*

B. Identification of functions from Domain knowledge

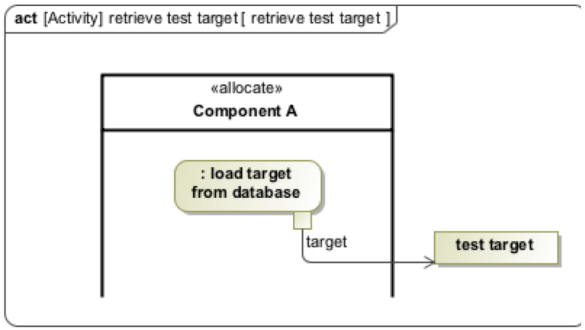
Technical functions

Bottom up — *Reuse / integration*

products

Product functions

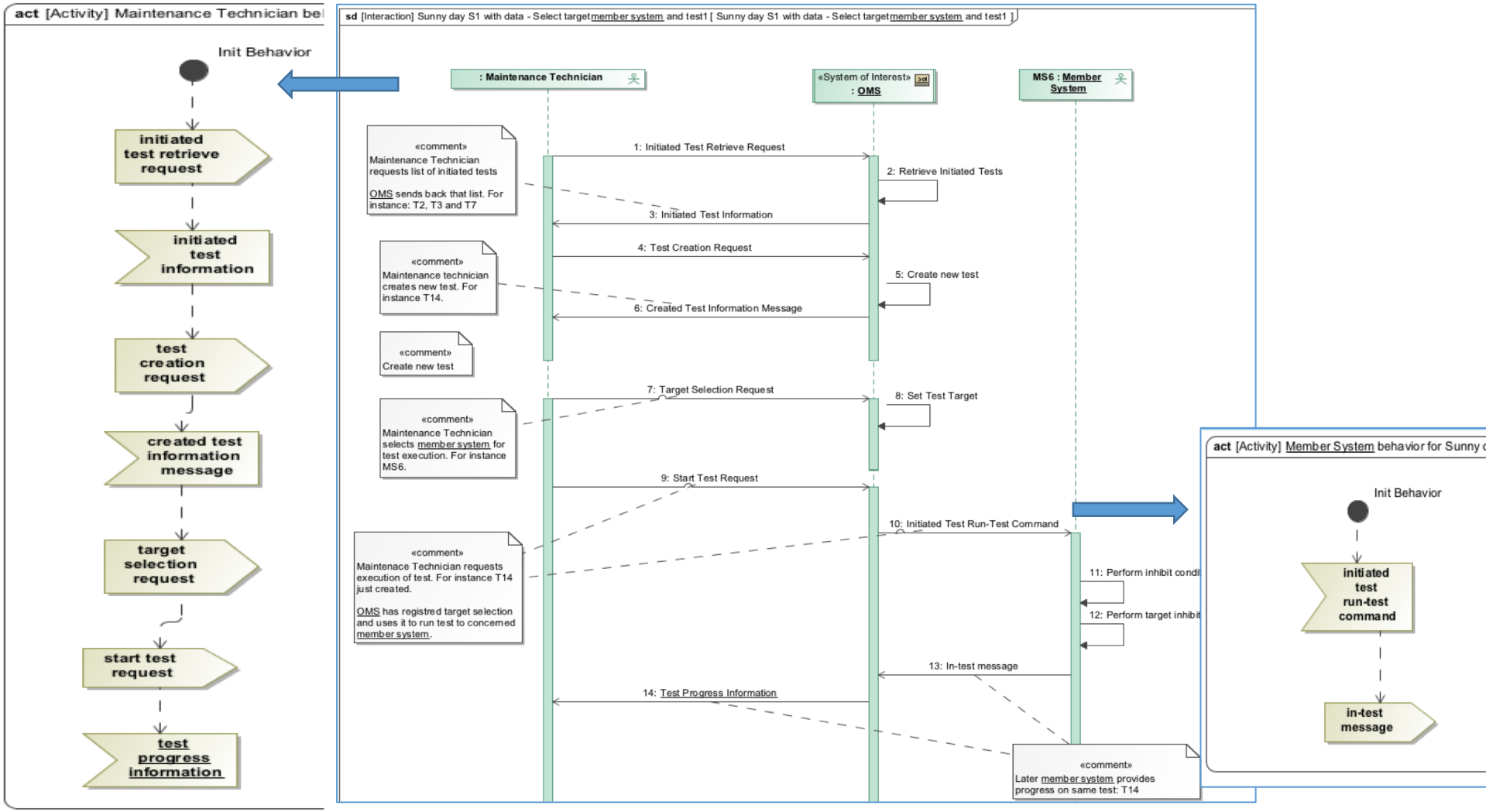
C. Identification of functions from products data sheets



Functional breakdown (calculated by Cameo)

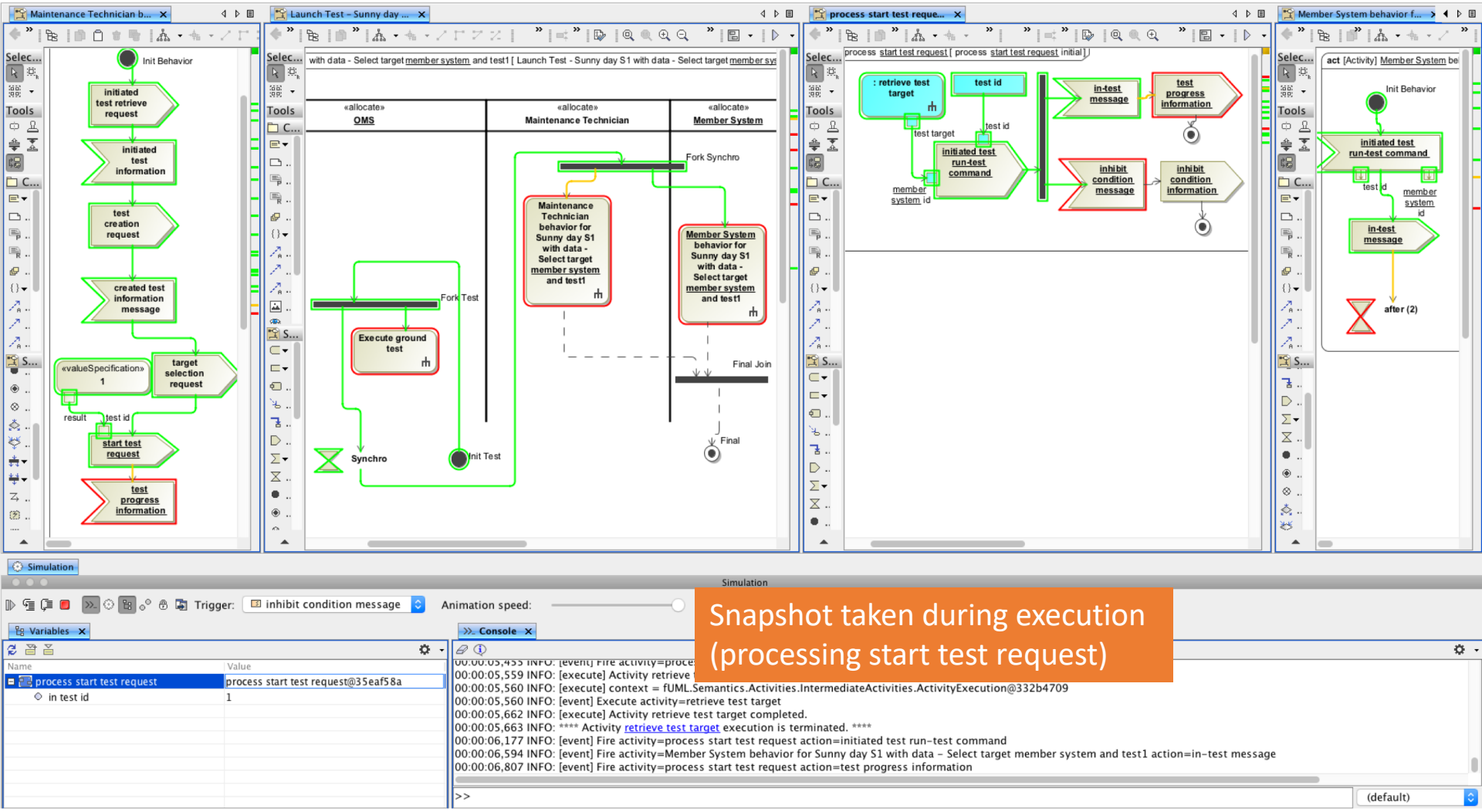
At any time can simulate a scenario (1)

SAMARES ENGINEERING
Accelerate Systems Design



At any time can simulate a scenario (2)

SAMARES ENGINEERING
Accelerate Systems Design

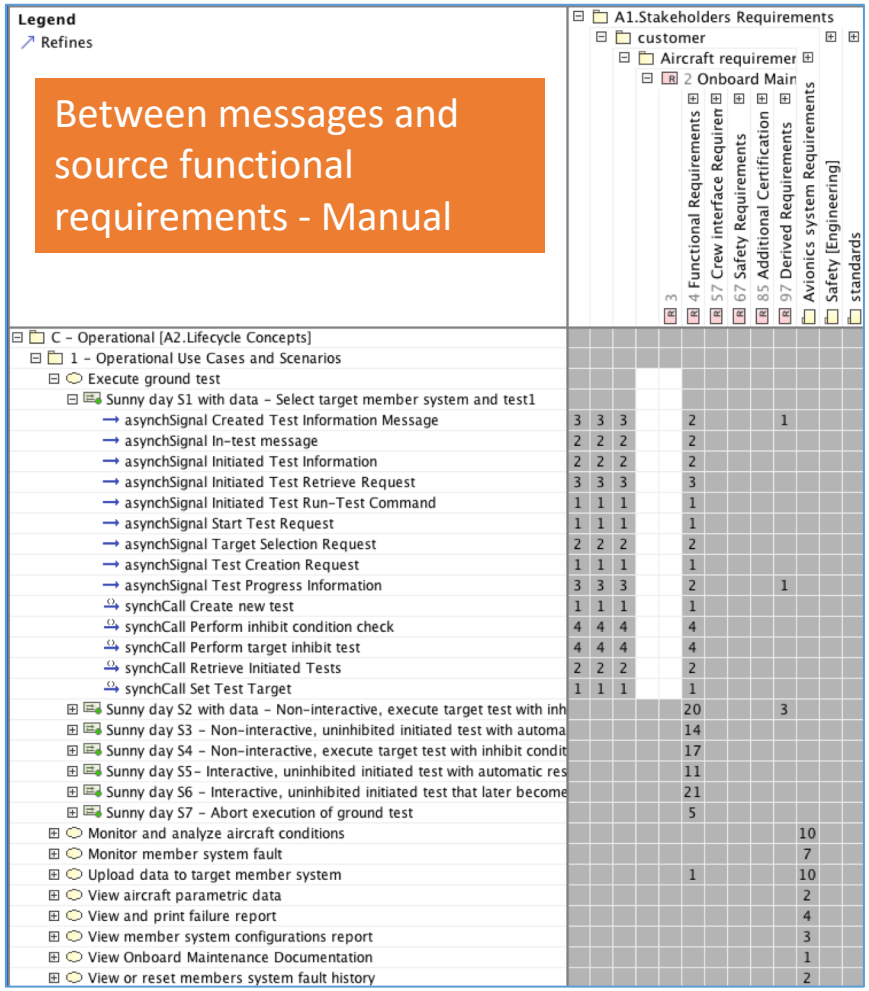


Snapshot taken during execution (processing start test request)

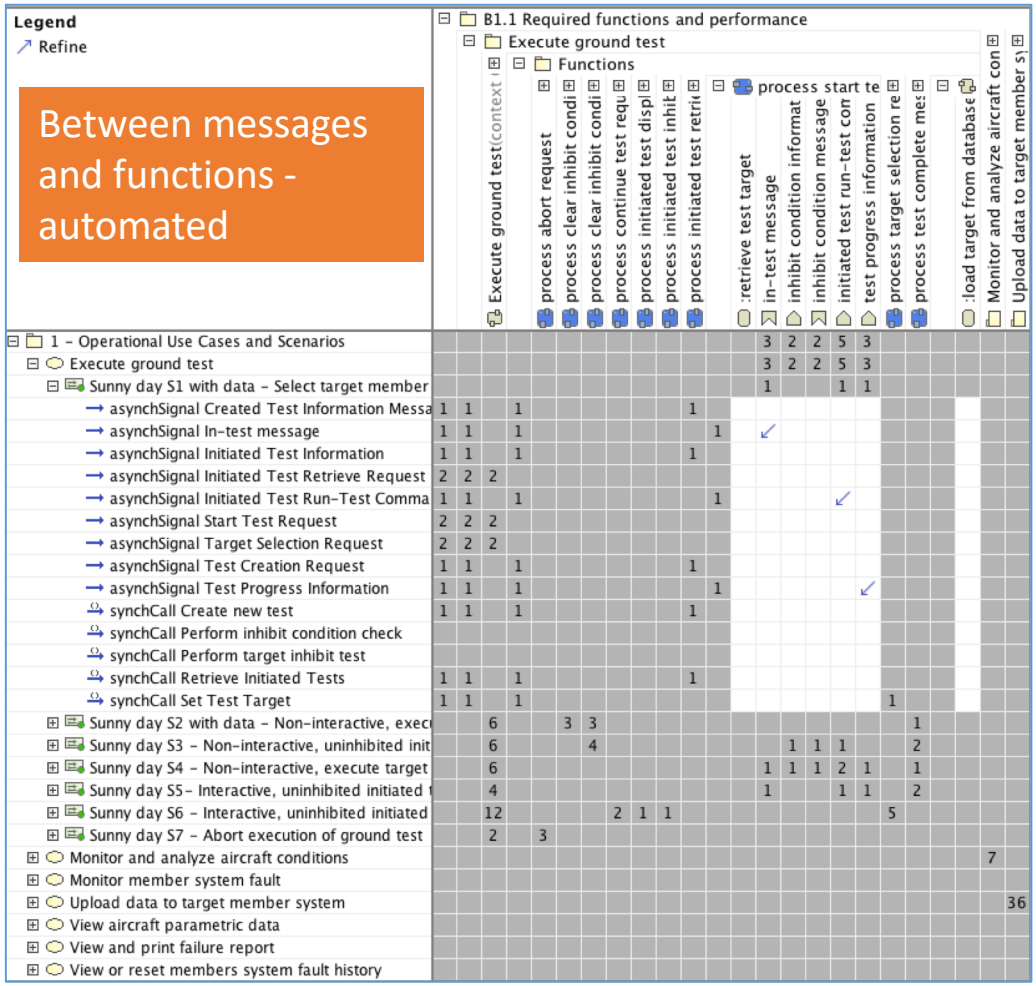
Traceability matrix

SAMARES ENGINEERING
Accelerate Systems Design

Between messages and source functional requirements - Manual



Between messages and functions - automated



End to end traceability

SAMARES ENGINEERING
Accelerate Systems Design

This representation is only for pedagogical purpose. Need other representation for whole System!!!

System functional requirements?

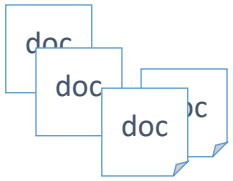
SAMARES ENGINEERING
Accelerate Systems Design

- **Where is system functional specification ? Where are system functional requirements?**
- **They live in the model ! They can be derived from all functions and their definitions, starting from top-level functions down to leaf functions**
- **Functional requirements shall take into account**
  - Activity parameters
  - States that restrict function validity
  - Activation condition (end of other functions, signal event)
  - Specification of actions to perform if any (design excluded)

Big picture (work presented in orange)

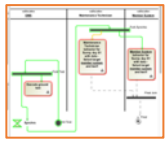
SAMARES ENGINEERING
Accelerate Systems Design

Collect stakeholder needs and constraints

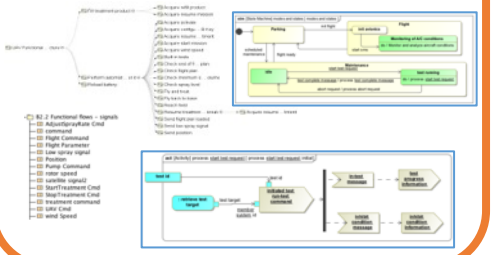


Structure functional needs into scenarios

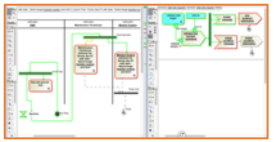
Requirements capture and definition of top level functions



Define top level system functions and flows



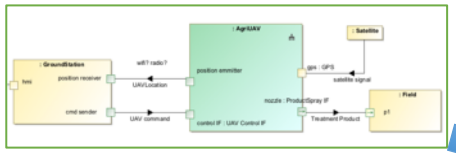
Architecture definition (functional and physical)



Define functional architecture

Define physical architecture and system design

Formalize physical interfaces



System level requirements

Full set of System requirements

Demonstration (if remaining time)

SAMARES ENGINEERING
Accelerate Systems Design

- **UAV for agriculture**
  - Treat field against pathogenic agents




- **Iteration 1**
  - Structure input requirements into UC and scenarios
  - Identification of top-level functions
  - Refinement of functions and identification of missing behavior…
- **Iteration 2**
  - Go back to scenarios and updates
  - Identification/update of top-level functions
  - Refinement of functions
  - Simulation

Future work

- **Complete formalization of requirements**
  - Design and Physical constraints
  - Complete function definition with performance and safety concerns
- **Connection of operational context with 3D animation framework**
- **Generate / update textual requirements from pattern**
- **Automated impact analysis (through traceability)**
- **Functional design and architecture trade-offs**
  - Ability to represent different function realizations
  - Ability to select a given set of realizations for simulation

Thank You for your attention

SAMARES ENGINEERING
Accelerate Systems Design

- Any question ?

Appendix - Import/synchronization of requirements