|  |
| --- |
| UNCLASSIFIED |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | REFERENCES | ISSUE | DATE |
| logoIRT-StExupery |  |  |  |  |
|  |  |  |  |  |
| logoAirbus |  |  |  |  |
|  |  |  |  |  |
| logoONERA |  |  |  |  |
|  |  |  |  |  |
| See original image |  |  |  |  |
|  |  |  |  |  |
| DASAVIA |  |  |  |  |
| logoSAFRAN |  |  |  |  |
| logoThales |  |  |  |  |

|  |
| --- |
|  |
| Streamlining Development Assurance  µXAV systems Process Definition |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
|  |  | Page : 1 / 46 |

|  |
| --- |
| This document is the intellectual property of RESSAC members It may not be used, reproduced, modified or disclosed without its authorization.  RESSAC members Proprietary Data. |

signatures

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | REFERENCES | APPROVERS |
|  |  | Fonction 1 |
|  |  |  |
|  |  | Name 1 |
|  |  | Fonction 2 |
|  |  |  |
|  |  | Name 2 |
|  |  | Fonction 3 |
|  |  |  |
|  |  | Name 3 |
|  |  | Fonction 4 |
|  |  |  |
|  |  | Name 4 |
|  |  | Fonction 5 |
|  |  |  |
|  |  | Name 5 |

Table of contentS

HISTORY 3

1. PURPOSE AND SCOPE OF THE DOCUMENT 6

2. Glossary and terms 6

2.1 Acronyms 6

2.2 Terms 6

3. ORGANIZATION 6

4. LIFE CYCLE PROCESSES 8

4.1 Principles 8

4.1.1 Layers 8

4.1.2 Incremental development 8

4.1.3 Contract based specification 9

4.1.4 Model Simulation and scenario reuse 9

4.1.5 Virtualization 9

4.1.6 Automatic translations and verification 10

4.1.7 AV configuration adaptation 10

4.2 Methods and technics 10

4.2.1 Collective review 10

4.2.2 Reviews 11

4.2.3 System and Multi-System Simulation 11

4.3 Life cycle description 12

5. Process Activities 13

5.1 Planning process 13

5.1.1 Initial process definition 13

5.1.2 Increment definition 14

5.1.3 Processes and increments adaptations 14

5.2 µXAV Layer 0 – Multi-Systems Level 16

5.2.1 Specification Process 16

5.2.2 Early Verification and Validation Process 19

5.2.3 Implementation Verification and Validation Process 23

# HISTORY

This section records the successive releases of the document following the initial one. The initial release is produced using several iterations.

|  |  |  |  |
| --- | --- | --- | --- |
| **Release** | **Date** | **Collective Review Attendees** | **Life-cycle change** |
| Initial |  |  |  |
|  |  |  |  |

# PURPOSE AND SCOPE OF THE DOCUMENT

The purpose of this plan is to describe the development and integral life-cycle processes for the µXAV/µXAV systems as developed in the scope of the RESSAC project

# Glossary and terms

## Acronyms

**AV:** Air Vehicle, the drone and its systems.

**AFHA:** Air vehicle level Functional Hazard Analysis

**DAL:** Development Assurance Level

**FHA:** Functional Hazard Assessment

**PASA:** Preliminary Air vehicle level Safety Assessment

## Terms

**Iteration**: many definition and design tasks are mutually dependent within the same process.

**Functions:**  Behavioral specification units scoped by a definite interface and mapped on implementation resources (items or systems). It is a concept required by the safety assessment process (e.g DAL assignment, FHA).

**Contract**: set of assertions (i.e properties) formulated over the I/O variables of a function interface. These assertions (split into an ‘assume’ group and a ‘guarantee’ group) are required to be met by any implementation of the function.

**Stakeholder**: Person(s) acting as customer in the scope of the RESSAC project of the µXAV, of a system or of an item.

# ORGANIZATION

In the scope of the RESSAC project, the activities are shared between the project partners, grouped into various teams:

* *Process Definition team* (ACG Solutions, Dassault Aviation), in charge of the life cycle processes definition and improvements,
* *Specification* *team* (Dassault Aviation). In charge of all aspects of the multi-system specification and MMS system specification.
* *Implementation* *team* (Esterel Technologies, Zodiac, Dassault Aviation, AdaCore). This team is in charge of architecture definition, integration, verification and validation activities at layer 0 and for MMS system.
* *Safety Group* (Apsys, ONERA, Dassault Aviation). Manages the interactions between the safety process and the development process. It is in charge of subcontracting the external safety assessment activities, of providing their needed inputs, and of ensuring appropriate use of their results by the development process
* Other teams dedicated to EPS and HBS development will be defined in revised versions of this document, after completion of the first increment.

# LIFE CYCLE PROCESSES

## Principles

### Layers

The complete development of the µXAV systems includes several abstraction layers:

**Layer 0**: Aircraft level as defined in ARP4754 and ARP4761. All the systems of the µXAV are considered as a unique system, i.e as a multi-system (or system of systems). Layer 0 activities include the development of the AV’s operational specification including the µXAV external interfaces, the functional specification and the multi-system’s architecture. The µXAV functions are mapped to the systems.

**Layer 1**: System level. Each system is considered in isolation with the other systems. This layer is developed independently for each system. Any issue regarding two systems or more is reported to layer 0 teams. For each system, activities include the development of the system operational specification, the functional specification and the system architecture. The system functions are mapped to the items. Items integration and verification are performed progressively following availability of items

**Layer 2**: Item level . Each item is developed separately based on the functions allocated to this item. The allocated functions (ARP4754’s terminology) are synonymous of system requirements allocated to an item. The item developments may use different methods, tools and numbers of development tiers. The items are defined in layer 1 architectures. They may consist of:

* Pure software. HW/SW integration is performed at layer 1.
* One or several hardware components, complex or not. An electronic board is considered as a hardware item
* A combination of SW and HW components, HW/SW integration is performed at layer 2 level.

### Incremental development

The product life cycle is incremental, developing progressively a limited number of new functions/features/systems.

4 increments are planned. Depending of the results of one increment, next ones may be adapted as necessary.

The increment definition and the life cycle adaptations are defined during the planning process and are recorded in a dedicated document.

### Contract based specification

Contracts are systematically formulated in the functional specifications, in an informal way, and wherever possible as executable assertions for layers 0 and 1. It relies on uniform[[1]](#footnote-1) *assume-guarantee reasoning* across all layers. This approach prevents introduction of specification faults, as this method ensures:

* Separation of the What from the How in specifications, i.e the expected behavioral properties from the behaviors to be implemented,
* Separation within the properties of the assumptions (on inputs, environments and contexts) from the functional Input/Output relations to be guaranteed,
* Possibility of assumption consistency analysis throughout several layers.
* Greater accuracy, completeness and non-ambiguity of specifications

Contracts are also used for specification verification:

* By manual verification (reviews) when the contracts are textual,
* By simulation and testing when the contracts are executable assertions (all layers),
* By formal analysis when the contracts are amenable to automated deduction, model-checking, or abstract interpretation

TO ADD FEW WORDS TO DESCRIBE THE APPROACH

### Model Simulation and scenario reuse

Operational specification at layers 0 and 1 are based on scenario definition. These scenarios are translated into simulation procedures to validate the functional specification including the compliance of the functional specification to the operational specification.

These simulation procedures at layer n will be systematically reused at layer n+1.

This is intended to:

* Verify cross-layer behavioral consistency of the specifications,
* Systematically provide some validated execution contexts to perform ‘component’ verifications. ‘Component’ may be a system, a sub-system, an equipment or an item.

This method enables an “early Verification” that is another name for executable system specifications, or model-based system development with simulation capabilities.

### Virtualization

Some verification activities at different layers will be performed using virtualization of some items. While additional activities may be still necessary on final configuration, the process will claim credit on verification performed on virtual platform.

Virtualization is used for

* **Hardware platform. :** Simulated hardware will be used as substitute for actual hardware implementation
* **System environment**: Some items and system components will be simulated, including the use of
  + Model of the external environment (wind and icing conditions),
  + Models of the drone’s mechanical behavior (AV), and of the physical devices (EPS, HBS) sensing, actuating and managing energy,
  + Models of the physical architectures interconnecting the items,
  + Model of the hardware resources executing software,

Representativeness of such a virtualized multi-system integration and its bearing on implementation fault elimination is an experimentation goal of the use case. It is intended to explore, to a limited extent, the potential benefits of emerging engineering concepts like 4D functional mock-ups and digital twins, i.e simulated iron birds (fault prevention dimension).

### Automatic translations and verification

In the implementation processes, trusted automatic translation, synthesis or compilation tools are used wherever possible.

An example in the use case is the use of Scade KCG followed by CompCert compilation at layer 2 with credits on property preservation[[2]](#footnote-2) from model to binary code.

Analogous examples are possible for hardware (logical synthesis and layout tool chains).

Associated to tool qualification considerations and certification credits, the use of these tools will eliminate or reduce the need for tool output verification.

The selected processes will also promote the use of verification tools, when available, for all systematic verification activities. Reviews are allotted to expert engineering judgments of high added value that are out of reach of any mechanized verification tools.

### AV configuration adaptation

Functional spec introduced PDI ??? TO BE CONFIRM, IF YES TO DESCRIBE THE POSSIBLE ADAPATIONS, THE WAY TO DO THAT ….

## Methods and technics

This section provides description of methods and technics used in multiple activities only.

### Collective review

This activity consists of a review performed during a face to face meeting. All attendees read collectively the document under review, and update it. Consensus is required to implement the changes.

The history section of the document records the date of the review, the main changes, and attendees.

The problematic topics needing further investigations are recorded in an OPR database hosted by the collaborative workspace (Github). LC is in charge of organizing periodic meetings to ensure that the registered OPRs are being addressed by the appropriate teams or groups of teams. Progress on the OPRs is periodically recorded, until they are resolved (and then removed from the data-base). In case an OPR is not fully solvable, it is left in the data-base as “closed OPR” with status information on the unsolved part.

### Reviews

Reviews are an independent reading of data.

The verifier that is different from the author of the data under verification performs the review as following:

* When applicable, the verifier uses the trace data
* Based on these trace data, the verifier reads the data and records the comments and proposed changes in a review report. The verifier name is logged in the review report.
* When review report is completed, the data author analyzes all comments.
  + The author agrees with the comment and the proposed change: The data is updated. The modified data references the review report.
  + The author disagrees with the comment and the proposed change or need further information: Author discusses with the Verifier to find a solution with common agreement: To update the data or to reject the comment.
  + In case of disagreement between author and verifier, a collective review is held with additional attendees.
* The review report records the date of the review, the changes, the author and the verifier.

### System and Multi-System Simulation

Simulation is performed at µXAV and system level to validate the functional specification. The simulation is based on the scenario developed in the operational specification.

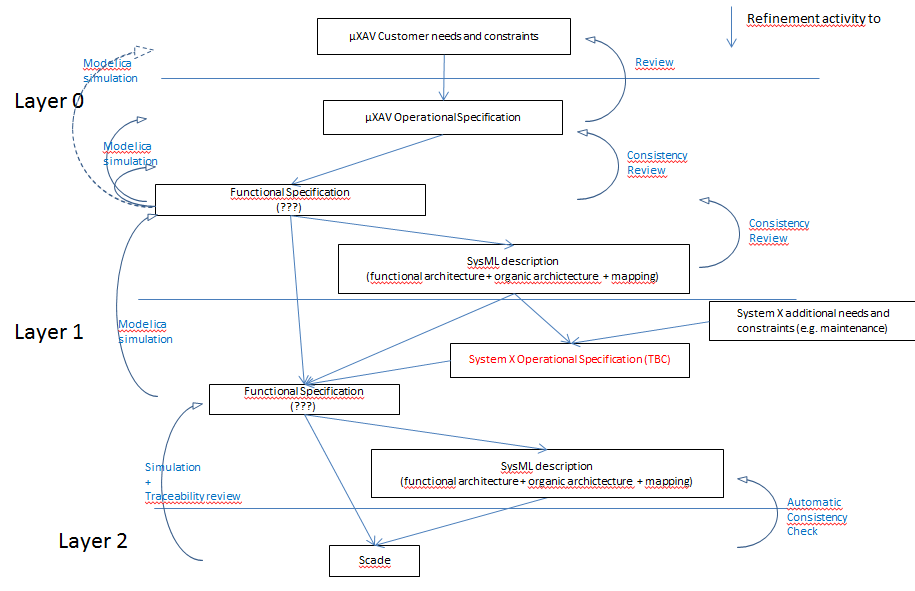
The set of simulation cases is expected to cover with reasonable confidence the combinatorial space of the input conditions that exercise µXAV’s systems or the system.

For continuous physical variables: altitude, attitudes, speed, energy levels, wind and icing profiles, there are infinitely many possible joint profiles of these variables. So discretization and coverage criteria are defined to cover:

* Continuous inputs (Weather conditions, Altitude, speed, energy levels) are covered either through
  + Selecting few regulatory ones (e./I for weather conditions, used SWC, AWC etc.)
  + Selecting three cases: maximum range value, average case and minimum range value.
  + using a grid approach combined two or more parameters representative of operational conditions
* Discrete inputs (events, to their relative ordering and to their mapping to physical time such as interactions on Control Panel, failure detection) are covered through
  + Each possible value of the discrete event is part of at least one scenario
  + Value switches in the physical time are defined to be representative of operational conditions
  + A grid approach combined two or more parameters representative of operational conditions
* Hybrid Coverage: µXAV and its system dynamics intertwine continuous time dynamics and events (internal and external ones). So a global input conditions coverage analysis has to merge the two preceding coverage analyses. It includes also some “worst case” conditions scenarios

## Life cycle description

This figure provides an overview of the life cycle development and verification processes



# Process Activities

## Planning process

This process consists of identifying the applicable life cycle and the activities to be performed. A first release of the µXAV systems process definition is provided at the beginning of the project. Then this definition may be updated iteratively as necessary. The µXAV systems process definition is accepted through a collective review by the RESSAC project partners.

### Initial process definition

* Description:

The purpose of this activity is to identify the activities, environment, methods and responsibilities for the development, verification/validation of the µXAV systems.

This activity produced a process definition document, defining the life cycle processes and activities for all layers.

Minimum development standard will be also defined. It includes rules at any layer for

* + I/O identification
  + Functions identification and decomposition (to enable mapping and traceability to lower layer)
  + Traceability rules
  + IT THERE SOME STANDARDS FOR SYSML?

Further guidelines may be provided for some systems/items to detail procedures and instructions for engineering teams

* Methods:

The process definition and the standards are textual documents. They are developed through a set of collective workshops and discussion with various partners and experts. Each collective workshop is prepared through several exchanges and documented by a designated author.

These workshops include iterations between collective reviews and document update.

* Environment: No particular environment is necessary for this activity, only textual editor.
* Transition criteria: T0 of the project
* Responsibilities: Process Definition Team
* Inputs: Background and experiments proposals from RESSAC partners
* Outputs
  + RESSAC\_Process\_Definition\_Document: The present document
  + RESSAC\_Development\_Standard

### Increment definition

* Description:

During the initial planning process, an initial definition of the increments is provided. The accuracy of this definition may decrease from the first increments to the latest ones.. Along with this identification, an impact analysis is conducted, identifying the change impact and the need for re-verification.

Any development increment may be defined on two axes:

* **Functional**: Functions, Features or behaviors to be added or modified.
* **Implementation**: Integration of items in replacement of virtual ones (e.g prototypes, mock-ups, virtualized OS or virtualized hardware).

An increment may comprise progress on the two axes at the same time. It may be apply to layer 0, layer 1 and/or layer 2

Functional description of the increments is provided in a separate document, which is submitted to Safety Group for analysis.

* Methods: A textual document is provided

New services or behaviors are decided by L0Spec team, on the basis of the desired behavior assumed to be known by this team. Increment definitions are submitted to Safety Group that gives feedback only in case of safety problem.

* Transition criteria: T0 of the project
* Environment: No particular environment is necessary for this activity, only textual editor.
* Responsibilities: Specification Team, Safety Group
* Inputs: RESSAC\_Process\_Definition\_Document
* Outputs: RESSAC\_CaseStudy\_Development\_Increments

### Processes and increments adaptations

* Description:

This activity is performed at the beginning of a new increment (except the first one). Based on the results and difficulties encountered during the last increment, the process life cycle may be modified.

The scope of the next increments are then adapted as necessary in regard of directives coming from Safety Group (To be confirmed), open problem reports and project management data.

* Methods: The retrospective of the last increment is performed in form of a collective review. Any adaptation collectively decided leads to process and increment definition changes
* Environment: No particular environment is necessary for this activity, only textual editor.
* Transition criteria: End of last increment
* Responsibilities: All teams involved in the previous increment
* Inputs:
  + Data produced during last increments
    1. Current functional definition at all layers,
    2. Current architectural definition at all layers,
  + Data produced by the safety group (Safety Group): TO CONFIRM HOW THESE DATA MAY INFLUENCES THE SCOPE OF INCREMENTS
    1. Current AFHA, SxFHAs,
    2. Current PASA, PSxSA,
  + OPR generated by the previous increments
  + Project management data: Resources, budget and planning,
* Outputs
  + RESAC\_Process\_Definition\_Document updated as necessary
  + RESSAC\_Development\_Standard updated as necessary
  + RESSAC\_CaseStudy\_Development\_Increments updated as necessary

## µXAV Layer 0 – Multi-Systems Level

The activities at layer 0 are grouped in three processes:

1. Specification Process.
2. Early Verification and Validation Process.
3. Implementation Verification and Validation Process.

### Specification Process

The following tasks are performed to produce the complete µXAV Layer 0 specification. The data produced by each activity are tightly coupled. So these tasks are performed in parallel and iteratively until global consistency is reached.

The specification Process includes the following activities

* + Operational specification.
  + Functional specification
  + Architecture definition
  + Mapping of the functions to the systems

#### Operational Specification

* Description:

Based on customer’s needs, the first step of this activity is to identify

* The operational context, defining the possible missions of the µXAV
* The external interfaces, including the man machine interaction (Control Panel, Remote Control)
* Expected performances
* Foreseeable operating conditions (environmental, human interfaces, possible failures)

Then mission scenarios are developed. The mission scenarios address how the drone is operated by its user, in particular the different operational modes, the possible degraded modes in case of failures, or abnormal environment conditions, and the expected mission performances. The scenarios are developed to address the operational context in the foreseeable operating conditions. Each scenario follows chronological order of events, and identifies allowed interactions, in following the chronological order of events, interactions and continuous time evolutions

Typically, a mission scenario includes 4 steps:

1. Preparation of the AV (loading payload, mission, power-on …)
2. Start of the mission in remote control mode or autonomous mode)
3. Take-off, cruise and landing phases, with possible additional phases in case of mission parameter updates
4. Mission termination: Payload release, power-off or start of a new mission.

These scenarios are supplemented as necessary with additional requirements and constraints. These additional requirements and constraints do not duplicate the scenarios but express characteristics and conditions that cannot be included in any scenarios.

* Methods: Textual description

This activity is performed through the capture of customer needs, either by direct collaboration of the customer (through discussion or data) or through the knowledge and background of activity responsible.

* Transition criteria: End of initial planning process
* Environments: Textual editor
* Responsibilities: Specification Team
* Inputs
  + Knowledge of customer’s needs.
* Outputs
  + µXAV layer 0 operational specification

#### Functional Specification

* Description:

The activity consists in analyzing the operational specification to identify the main functions of the µXAV. Depending of the complexity, a function may be decomped into sub-functions. Each function or sub-function (TO BE CONFIRMED: FOR A FUNCTION DECOMPOSED INTO SUB FUNCTION, IS THERE FONCTION DESCRIPTION **AND** SUB-FUNCTION OR ONLY SUB-FUNCTIONS?). is described by:

* + interfaces: inputs and outputs of the function
  + a set of contracts including a set of assumptions and guarantees of the function
  + a behavioral specification that supplement the contracts. This specification should not duplicate the contracts (TO BE CONFIRMED)

The contracts and the behavioral specification together fully describe the expected behavior of the function or sub-function (TO BE CONFIRMED)

TO BE COMPLETED AS NECESSARY

* Methods: Textual description.

Functional specification is a contract based specification.

* Transition criteria: End of initial planning process
* Environments: Textual editor
* Responsibilities: Specification Team. The functions’ perimeters are defined in collaboration with Safety Group team
* Inputs
  + RESSAC\_Development\_Standard
  + µXAV layer 0 operational specification
* Outputs
  + µXAV layer 0 functional specification

#### Multi-system’s Architecture

* Description

This activity consists in developing the model of Layer 0 architecture. The architecture defines

* External interfaces: communications between µXAV and the ground station (GS).
* Inter-systems interfaces: physical, analog and digital communication links between the systems,

The architecture definition is based on (OPERATIONAL SPEC ? FUNCTIONAL SPEC ?) … TO BE COMPLETED: HOW INPUTS ARE USED, AND FEW WORDS ON ARCHITECTURE ELABORATION

TO EXPLAIN THESE ASPECTS:

“Based on PASA, explain the impact of PASA on the architecture

…probability budgets on the primary events related to the inter-system interaction resources,

data-sheets of the candidate components to implement the inter-system interactions (e.g power supplies and communication links).”

* Methods: SysML modeling

TO ADD FEW WORDS ON THE SYSML MODEL PRODUCTION, SUCH AS:

Constraints, assumptions when necessary are included in the model in form of comments and attributes.

* Environments: SCADE Architect
* Transition criteria: End of initial planning process
* Responsibilities: Implementation Team
* Inputs
  + µXAV operational specification
  + µXAV functional specification
  + Safety Analysis (PASA ..) ?
  + STANDARDS ???
* Outputs
  + µXAV layer0 SysML model – Architecture part

#### Mapping of Functions to Systems

* Description

The initial step is to analyze and include the functional decomposition defined in the Functional Specification in the µXAV layer0 SysML model.

Then the activity consists in

* + mapping of the leaf-functions (bottom level of layer 0 functional decomposition) to systems or physical devices defined in the architecture
  + allocating the inter-system information flows to physical communication links.
  + TO BE COMPLETED ?
* Methods: SysML model

Mapping allocation consists in supplemented the architecture model with the functions description. These descriptions are included in attributes blocs (TO BE CONFIRMED) in the model.

Iterations with Safety Group are performed to consolidate and get a common agreement of the mapping

Paper-pencil for solving of the mapping constraints WHAT IS IT ???

* Environments: SCADE Architect.
* Transition criteria: End of initial planning process
* Responsibilities: Implementation Team and Safety Group
* Inputs
  + µXAV operational specification
  + µXAV functional specification
  + µXAV layer0 SysML model - Architecture part
* Outputs
  + µXAV layer0 SysML model – Functional part

### Early Verification and Validation Process

The early Verification and Validation Process includes the following activities

* + Operational specification review
  + Functional specification review
  + Functional specification simulation
  + SysML model review

#### Operational specification review

* Description:

This activity consists in performing a review of the µXAV operational specification with the stakeholders. The purpose of this review is to verify that the operational specification is a correct and complete capture of the customer needs.

* Methods: Collective review. INSTEAD OF REVIEW, IS IT POSSIBLE TO USE SCENARIO EXECUTION ?
* Environment: No particular environment
* Transition criteria: Initial or update of the operational specification considered as mature enough by its author
* Responsibilities: Specification team and stakeholders
* Data under validation: µXAV operational specification
* Data used as input for the activity: Customer needs and constraints
* Outputs: µXAV operational specification updated as necessary

#### Functional specification review

* Description:

This activity consists in performing a review of the µXAV functional specification. The purposes of this review are:

* + To verify the compliance to the operational verification. It includes the correctness and completeness of contracts, assumptions and behavioral specification
  + To identify the contracts, assumptions and behavioral specification features those are not directly to the implementation of any part of the operational specification. These parts are provided to stakeholders and safety group for analysis. Corrective actions may be identified as necessary
  + To assess the correct understanding and the usability for people in charge of using this document for further refinements at next layer.
  + To check the conformance to development standard
* Methods: Collective review and discussion with stakeholder
* Environment: No particular environment
* Transition criteria: Initial or update of the functional specification considered as mature enough by its author
* Responsibilities: Specification team, implementation team, safety group and stakeholders
* Data under validation: µXAV functional specification
* Data used as input for the activity:
  + µXAV operational specification
  + RESSAC\_Development\_Standard
* Outputs:
  + µXAV functional specification updated as necessary
  + Feedback from stakeholder and safety group
  + Corrective actions

#### Functional specification simulation

* Description:

One of the main innovative aspects of this process is to introduce executable specification. So, this activity consists in

* + Developing a modelica model based on functional specification
  + Translating scenarios defined in the operational specification into simulation procedures.
  + To exercise the simulation implementation in the simulation environment
  + To analyze with the stakeholders the simulation results
* Methods: System and Multi-System Simulation

TO ADD FEW WORD ON MODELICA DEVELOPMENT AND SCENARIO EXECUTION

* Environment: Modelica based simulation environment
* Transition criteria: Initial or update of the functional specification considered as mature enough by its author
* Responsibilities: Implementation team and stakeholders
* Data under validation: µXAV functional specification
* Data used as input for the activity: µXAV operational specification
* Outputs
  + Modelica Model
  + Simulation procedures and results
  + Simulation results review report

#### SIMULATION CASES REVIEW ???

SOIT LES SCENARIOS SONT COMPLETS ET PRECIS ET IL FAUT UNIQUEMENT S’ASSURER QUE LA TRADUCTION DES SCENARIOS EN PROC EST COMPLETE ET CORRECTE.

SOIT (COMME C’EST LE CAS AUJOURD’HUI, LES SCENARIOS SONT “INTERPRETES” EN MULTIPLE SIMULATION CASES, ET FAUT PREVOIR UNE VERIFICATION DES SIMULATION CASES BASES SUR LES CRITERES DE DEFINITION DE CES CAS (COUVERTURES DES ENTREES ….)

#### SysML Model review

* Description

This activity consists in performing the review of the SysMl Model, both the architecture part and the functions mapping. The key points are

* + The external interfaces are completely and correctly identified based on µXAV operational specification
  + Inter-systems interfaces are described and are consistent
  + All functions of the functional specification are allocated to a system
  + For functions allocated to more than one system, it is verified that this mapping is relecvant and ensure the completeness of the function implementation
  + Inter-system information allocation to physical communication links is consistent.
  + CONFORMITY AU STANDARD ?
  + TO BE COMPLETED: QUELS TYPES D’EREUIRS ON POURRAIT AV OIR DANS EL SYSML Model?
* Methods: Review
* Transition criteria: Initial or update of the SysMl Model considered as mature enough by its author
* Responsibilities: Implementation team
* Data under validation
  + µXAV layer0 SysML model
* Data used as input for the activity
  + µXAV operational specification
  + µXAV functional specification
  + RESSAC\_Development\_Standard. TO BE CONFIRMED
* Outputs
  + Review report

### Implementation Verification and Validation Process

This process consists in integrating progressively the systems and verifying that implementation meets the specification (operational, functional and architectural).

1. i.e cross-domain, the domains being system, hardware, software [↑](#footnote-ref-1)
2. Either functional or non functional (Run-Time Errors, structural coverage, etc.) [↑](#footnote-ref-2)