### Item type 2: SPARK

#### Methods definition

* Description:

The purpose of this activity is to define guidelines to apply the chosen methods on the item.

Item

* Step 1: Inputs analysis:
  + To check inputs for applicability, consistency, and translation-able into chosen method (SPARK)
  + Report for non-verifiable requirements (e.g. performances) that should be verified at system level
  + “Entity or Object” identifications (e.g. Estimated Battery Charge Level at mission start, Estimated Battery Charge Level at mission end)
  + Dependencies between inputs/outputs and entities/objects

Outputs:

List of entities and dependencies (textual form)

Report to system spec

* Step 2: Item architecture and specification
  + Formalization of system requirements

Use of SPARK to dfine the item requirements based on system requiremenst allocate to the item and on entities identification

“Top level contract” based on Item I/O. (assumption: System requirements can be translated into contracts based on I/O)

* + Items Architecture:
    - Identification of the component based on the “entities”
    - Define the interfaces between components
    - Real time aspects: Assumption : a single cyclic task.
      * Scheduling of components

Step 3: Formal component requirements

* + - Allocation of Top-Level contracts into components
    - Refinements of Top-Level contracts into Component requirements : Contracts (How to detect additional requirements, not traceable to Top-Level ?)
    - Verification
    - Coding:

Step 4: Integration and verification

Integration (Compilink, linking

Proofs? Tests? Coverage analysis?

DRIVERS , BSP ?

* Methods:

TBD

* Environment:

No particular environment is necessary for this activity, only textual editor.

* Responsibilities: TBD
* Inputs:

No specific inputs

* Outputs

SPARK guidelines (requirements and code)

Formal analysis description

#### Item requirement development

* Description:

The purpose of this activity is to develop the item requirements (in SPARK) to implement the system requirements allocated to the item.

* Methods:

SPARK

* Environment:

TBD

* Responsibilities: TBD
* Inputs:

System specification allocated to the item

Assumptions: Modelica model, textual requirements

System Architecture: SysMl.

* Outputs

Item requirements

#### Item requirement verification

* Description:

The purpose of this activity is to verify the compliance of the item requirements to the system specification allocated to the item

* Methods:

Review?

* Environment:

TBD

* Responsibilities: TBD
* Data under verification
* Inputs used for verification

System specification

Item requirements

* Outputs

TBD

#### Item implementation

* Description:

The purpose of this activity is to implement the item requirements into source code, and to produce the executable object code

* Methods:

Ada

* Environment:

Gnat Ada environment

* Responsibilities: TBD
* Inputs:

Items requirements

* Outputs

Source code

Executable object code

#### Item verification

* Description:

The purpose of this activity is to verify the compliance of the item implementation to the item requirements

* Methods:

The activity consists of running GNATProve. The tool detects all cases where the contracts are not satisfied.

* Environment:

GnatProve

* Responsibilities: TBD
* Data under verification
* Inputs used for verification:

Item requirements

Source code

* Outputs

Analysis report