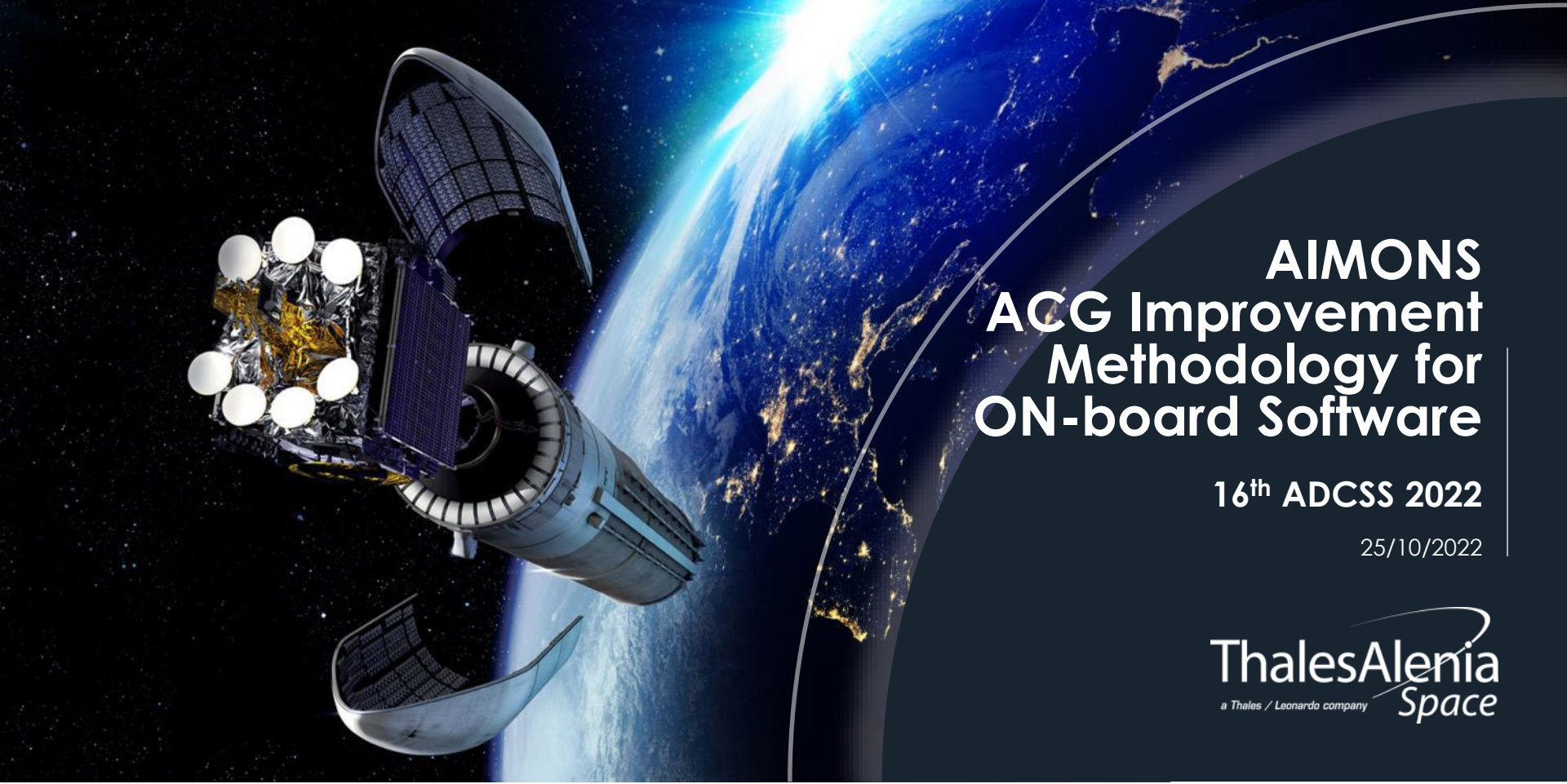


AIMONS ACG Improvement Methodology for ON-board Software

16th ADCSS 2022

25/10/2022

ThalesAlenia Space
a Thales / Leonardo company

Outline

Introduction
Study context and objectives

Study status
Task 1 main conclusions

Task 2: focus on Simulink Check

Current conclusions

Introduction: study context & objectives

CONTEXT:

- Autocode is a now standard for AOCS OBSW development (and FES to SVF simulator)
- Autocode introduces 1 new step: **Model** / Source code / Object code
- SAVOIR autocode handbook issue 01 released June 2021
- How to efficiently integrate the guidelines on a V&V AOCS OBSW autocode process & framework ?

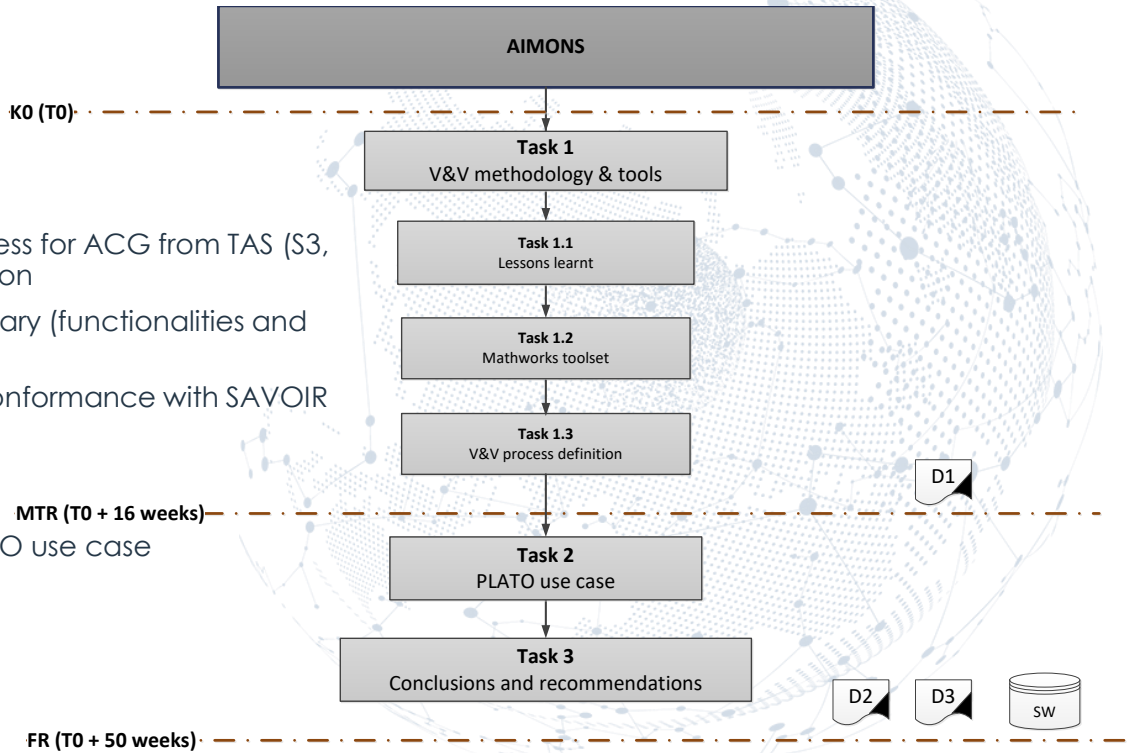
PURPOSE of STUDY

- Lesson learnt on numerous TAS programs (with autocode) in terms of:
  - V&V Process
  - Toolbox usage
- Based on updated framework (toolboxes evaluation), propose a subsequent V&V process
- Experimentation on specific use case (PLATO)
- Conclusions and final recommendations on the process and framework for V&V AOCS OBSW development

Introduction

Work logic

- **Task** 1: closed
  - **Task 1.1**: Lessons learnt on V&V process for ACG from TAS (S3, SBNEO, PLATINO…), Toolboxes selection
  - **Task 1.2**: Mathworks toolboxes summary (functionalities and efficiency)
  - **Task 1.3:** V&V process definition in conformance with SAVOIR handbook
- **Task 2**: in progress
  - Application of Task 1 process to PLATO use case
- **Task 3**:
  - Conclusions and Recommendations



Task 1 main conclusions

Task 1.2: Mathworks toolboxes summary (functionalities and efficiency)

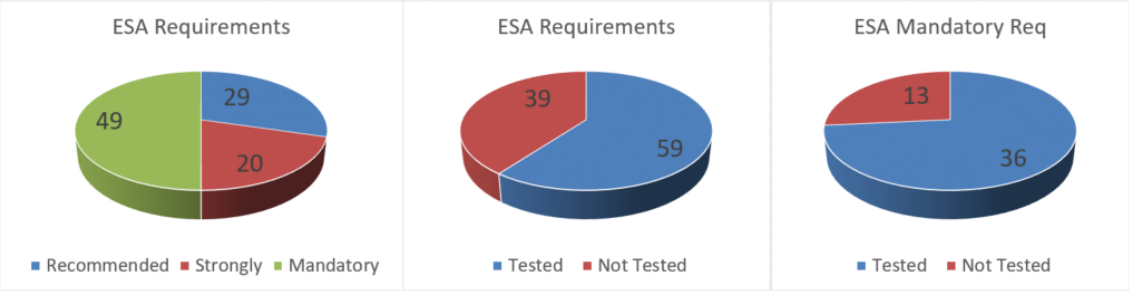
- Recall of Mandatory or highly recommended Mathworks toolboxes:
  - ***ML/SL/Embedded coder*** for code generation (lessons learnt)
  - ***Simulink check*** recommendation for guidelines automatic verification
  - ***Simulink coverage*** recommendation pending SW unit process selection (MIL/SIL level)
    - Action to derisk via proof of equivalence between MIL and SIL
- Other toolboxes selection are pending process and not identified as key for the V&V process
  - ***Simulink Design Verifier:*** pending SW unit verification process selection (MIL/SIL level)

Task 1.3: V&V process definition in conformance with SAVOIR handbook

Task 2 status: Simulink Check experimentation on PLATO use case

- Implementation of most ***mandatory*** rules verification on Simulink check (2019a and 2022a) from ESA handbook: **98** requirements
  - 14 covered by dedicated Custom Checks
  - 45 covered by Native Simulink Checks.

:



Nota: implementation of internal TAS guidelines also performed

- Main conclusions
  - Efficient and user-friendly tool (ready for continuous integration) but needs refinement notably for native checks limitation & warnings treatment & exceptions management (nota: enhancement in the last release)
  - Preference for custom checks

Task 2 status: Simulink Check experimentation on PLATO use case

TOOL

- Most efficient framework to assess the adherence of a model to a guideline (ESA Handbook or internal)
- Tools maturation needed to have a fully efficient process

PROCESS

- Recommendation to use the tool at the **early steps of development** and to consider it as a mandatory verification step for each delivery from AOCS to SW team.
- Ready for SW integration process, to reduce manual work and log delta between SW releases
- Minor rework of the guidelines to update rules so that it can be automatically verifiable
- Some rules from the SAVOIR Guidelines cannot be verified with model tools such as Simulink Check
  - Minor specific adaptation of the process for these few rules for which the verification with the tool is not trivial (e.g; verification method => Code inspection)

Current conclusions & way forward

V&V process and framework

- V&V process is pending selected tools maturity and company heritage
- « *The sooner the better* » applicable **IF** no rework at later stages
- Rules verification is vital at model level for **building block approach**

Study termination and possible continuation

- Task 2 in progress: coverage analysis
  - Where to perform the coverage analysis: model or/and source level?
- Final conclusions & recommendations : planned end 2022
- Possible completion of the complete automatic verification of SAVOIR autocode handbook in progress.